doc. Ing. Pavel Šenovský, Ph.D.

Bezpečnostní informatika 1

skripta
10. vydání

Ostrava, 2022

Bezpečnostní informatika 1
10. rozšířené vydání
tento text neprošel jazykovou úpravou

Vysoká škola báňská - Technická univerzita Ostrava, Fakulta bezpečnostního inženýrství

Obsah

Seznam obrázků

Seznam tabulek

Úvod

Vážený studente, dostává se Vám do rukou učební text předmětu *Bezpečnostní informatika I.*

Mým cílem při psaní tohoto textu bylo, aby čitatel získal základní přehled v oblasti informačních technologií a také otázek bezpečnosti, které jsou s nimi spojené. Text samotný není proto zaměřen na *informatiky*, ale spíše na lidi, kteří budou Informační technologie (IT) používat uživatelsky. Uživatelský přístup k problematice IT je trošku jiný - v našich úvahách o jednotlivých diskutovaných problémech nebudeme muset proto zacházet příliš do hloubky. To nás však samo o sobě nezbavuje nutnosti se s těmito technologiemi seznámit, zjistit jejich možnosti, ale také omezení, která jsou spojena s jejich použitím.

Moderní technologie jsou totiž často obklopeny z hlediska principu fungování řadou mýtů, pověr a nepochopení, které znesnadňují jejich správné použití, nebo u uživatelů vytvářejí neodůvodněná očekávání, která nemohou naplnit. Naše chápání, tedy způsob, jakým vnímáme informační technologie, přímo ovlivňuje způsob, jakým je budeme používat v praxi a v takovém případě za správné použití je pak zodpovědný, ten kdo je po používá - tedy uživatel, nikoliv nutně IT specialista. S tím jak se zvyšuje penetrace stále pokročilejších technologií od počítačů až po chytré mobilní telefony a tablety, tím se také zvyšují nároky na jejich uživatele a to zejména z pohledu bezpečnosti, ochrany osobních údajů nebo citlivých dat uchovávaných na těchto zařízeních obecně.

Tento text vychází těmto požadavkům vstříc.

Organizace textu

Pro zpříjemnění čtení jsem se také rozhodl zpracovat tento text formou vhodnou pro „distanční vzdělávání“, tak aby práce s ním byla co možná nejjednodušší. Z tohoto důvodu je text jednotlivých kapitol segmentován do bloků.

Každá kapitola začíná náhledem kapitoly, ve kterém se dozvíte, o čem budeme v kapitole mluvit a proč. V bodech se pokusím shrnout, co byste po prostudování kapitoly měli znát a kolik času by Vám studium mělo zabrat. Mějte Prosím na paměti, že tento časový údaj je pouze orientační, nebuďte proto prosím smutní nebo naštvaní, když ve skutečnosti budete kapitole věnovat o něco méně nebo více času.

Za kapitolou následuje shrnutí, ve kterém budou zdůrazněny informace, které byste si rozhodně měli zapamatovat (určitě Vám ale neuškodí, pokud si jich zapamatujete více).

To, že jste správně pochopili probíranou látku, si budete moci ověřit pomocí kontrolních otázek a testů, které by Vám měly poskytnout dostatečnou zpětnou vazbu k rozhodnutí, zdali jít dále nebo si vyhradit delší čas na opakování.

Pokud studujete Bezpečnostní informatiku 1 v rámci celoživotního vzdělávání, tak v průběhu studia narazíte také na tzv. *korespondenční úkoly*. Tyto úkoly je potřeba vypracovat a v termínech daných Vaším studijním harmonogramem je odevzdat. Tyto korespondenční úkoly poslouží k Vašemu závěrečnému hodnocení.

Pokud jste studenty řádného studia v denní nebo kombinované studijní formě, pak i Vy narazíte na korespondenční úkoly, ale můžete je v klidu ignorovat – Vaše hodnocení bude provedeno na základě písemné zkoušky.

Pro zjednodušení orientace v textu jsem zavedl systém ikon:

V novém (už šestém!) vydání skript jsem se rozhodl pro trošičku jiný způsob přípravy skript a celá jsem je přepsal v Desktop Publishing (DTP) systému LaTeX. Důvodem jsou některé schopnosti, které je s běžnými textovými procesory je možné dosáhnout pouze stěží a také to, že řada z vás bude studovat tento text přímo v počítači (tabletu, čtečce elektronických knih nebo mobilním telefonu) a v takovém případě budete chtít využít nejspíše všech schopností, která Vám tato zařízení poskytují.

Kolikrát jste si pomysleli - „jaké by to třeba bylo, kdybych mohl klepnout na jednu z těch divných

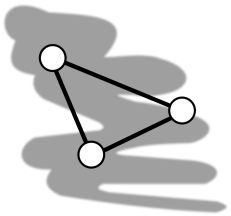
Průvodce studiem
Slouží pro seznámení studentů s látkou, která bude v kapitole probírána.

Čas nutný ke studiu
Představuje odhad doby, který budete potřebovat k prostudování celé kapitoly. Jedná se pouze o orientační odhad, neznepokojujte se proto, pokud Vám studium bude trvat o něco déle nebo budete hotovi rychleji.

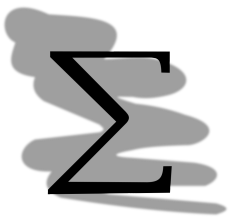
Vysvětlení, definice, poznámka
U této ikony najdete vysvětlující text, poznámku k probíranému tématu, která problém uvede do širších souvislostí, popřípadě důležitou definice.

Kontrolní otázky
Na závěr každé kapitoly je zařazeno několik otázek, které prověří, zda jste problematice kapitoly dostatečně porozuměli. Pokud nebudete vědět odpověď na některou otázku, je to signál pro Vás, abyste se ke kapitole vrátili.

Příklad
Příklady obsahují praktické demonstrace diskutovaného problému.

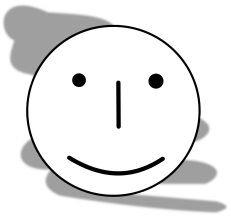


Návaznosti
V tomto segmentu budou zmíněny další návaznosti probíraného tématu na další témata tohoto předmětu, ale také dalších předmětů.



Shrnutí
Obsahuje základní myšlenky kapitoly, kterým by měl být věnována zvláštní pozornost během studia.

zkratek (které informatici tak milují) a ona by mě přesměrovala automaticky na seznam zkratek“? Nebylo by lepší kdyby na daný literární pramen bylo možné se dostat přímo klepnutím na jeho číslo v textu, nebo aby jste nemuseli vybranou pasáž hledat přes čísla stránek, ale postačovalo by kliknout



Přestávka
Po obtížné části textu, nebo prostě občas jenom tak je nutné si udělat krátkou přestávku, načerpat síly k novému studiu.

na jméno kapitoly v obsahu?

Mě jako studentovy by se to líbilo a proto doufám, že je oceníte i Vy, protože všechny výše uvedené možnosti skripta ve formátu Portable Document Format (PDF) obsahují. Aktivní odkazy jsou v textu zvýrazněny červenou (a v případě odkazů na literaturu zelenou) barvou.

Na konec skript byl přidán také rejstřík pojmů. Doporučuji, abyste jej v rámci přípravy na zkoušku prošli - zamyslete se nad tím, zda všechny pojmy, které jsem do něj zařadil, chápete a jste je schopni dát do souvislostí. Pokud ne je vedle pojmu odkaz na číslo stránky, kde je pojem probrán a Vy můžete rychle zaplnit případné mezery ve svých znalostech problematiky informačních systémů.

Přeji Vám, aby čas, který strávíte s tímto textem, byl co možná nejpříjemnější a abyste jej nepovažovali za ztracený.

doc. Ing. Pavel Šenovský, Ph.D.

Poznámka autora:
Právě držíte v rukou desáté rozšířené vydání skript. Je možné, že právě studujete na zkoušku, nebo jste se ke skriptům dostali pouze náhodou po delší době. Z tohoto důvodu by se Vám mohlo hodit stručné shrnutí změn mezi jednotlivými vydáními těchto skript.

Novinky v 5. vydání skript
1. Doplněna teorie informace o kódy, další drobné změny
2. Kapitola o šifrování byla doplněna o informace k možnosti nasazování algoritmů Secure Hash Algorithm (bezpečný hašovací algoritmus) (SHA) v čase pro generování certifikátů a základní informace o SHA-3.
3. Kapitola věnována peer to peer sítím byla podstatně přepracována (obecný úvod, architektura Berkeley Open Infrastructure for Network Computing (BOINC), bezpečnostní aplikace).
4. Kapitola rychlých informací doplněna o základy značení dle evropské legislativy Classification, Labelling and Packaging (klasifikace, označování a balení) (CLP).
5. Kapitola o Internetu – doplněny základní informace o IPv6

Novinky v 6. vydání:
1. sazba v LaTeX
2. Drobné opravy a aktualizace v textu
3. Přepsána kapitola moderního symetrického a asymetrického šifrování, aby pokrývala celé spektrum použití

Novinky v 7. vydání:
1. změny v souvislosti se změnou koncepce předmětu Bezpečnostní informatika 1
2. doplněny kapitoly

   (a) Úvod do počítačových sítí
   (b) E-government
   (c) Informační systémy veřejné správy (ISVS)
   (d) Kybernetická bezpečnost v ČR
3. některé kapitoly byly naopak odstraněny

Novinky v 8. vydání:
1. do kapitoly o škodlivém kódu byly doplněny některé informace o bezpečnosti mobilních telefonů/tabletů a zařízení Internet of Things (IoT)
2. provedeny změny v kapitole o šifrování za účelem modernizace textu a lepšího vysvětlení používaných postupů
3. doplněny informace o změnách v legislativě elektronického podpisu související s transpozicí evropské směrnice eIDAS do českého právního řádu
4. oblast podpisových schémat předělána dle požadavků normy ETSI TS 102 760-1 V2.1.1 (v předchozích vydáních byla využívána norma ve verzi V2.0.0)

Novinky v 9. vydání:
1. první a dosud jediné vydání skript v angličtině (obsahuje ale také některé, byť drobnější změny)

Novinky v 10. vydání:
1. doplněna řada pojmů do indexu
2. drobné změny a opravy v celém textu skript
3. lépe rozebrána sekce kódování, znakových sad apod.
4. velká úprava části věnované škodlivému kódu. Text by měl být jasnější a poskytovat více „akčních“ informací, které můžete použít ke zvýšení bezpečnosti Vašich zařízení, doplněna také sekce věnovaná kryptoměnám a technologii block chain
5. přepracována sekce věnovaná podpisovým schématům podle normy ETSI 119 312-1.4.1 (2021-08)
6. překreslena řada obrázků
7. TBD

Kapitola 1

Základní pojmy informatiky

Náhled kapitoly
Informace jsou základní hybnou silou dnešní společnosti, proto ji také někdy říkáme společnost informační. Z tohoto důvodu je nutné plně porozumět pojmům, jako je informace, informační technologie apod.

Po přečtení této kapitoly budete
vědět
1. co je to informace, informační technologie ...
2. jak probíhají komunikační procesy

umět
1. rozlišit informace a data

Čas pro studium
Pro prostudování této kapitoly budete potřebovat přibližně 45 minut.

1.1 Informace

Zamysleme se nad samotným pojmem informace, jelikož se tento pojem v běžném jazyce často používá, většina lidí si přibližně dokáže představit, co znamená. Pro naše účely však je nutné si tento pojem vymezit mnohem přesněji - což vyžaduje formální definici. Pojem informace můžeme definovat například takto:

Zapamatujte si
Informace je objekt nehmotné povahy, sdělení (zprávy), jehož základní vlastností je to, že u příjemce informace snižuje neurčitost.

Definice informace zmiňuje neurčitost, pokusme se ji tedy nějak definovat. Neurčitost neboli entropie, česky míra neznalosti (1.1) byla odvozena z počtu pravděpodobnosti C. Shanonnem [71] obecně takto:

$$H = -\sum_{i=1}^{n} p_i \log_2 p_i \tag{1.1}$$

kde:
H ... entropie
p_i ... pravděpodobnost výskytu i-tého jevu

Takto definovaná entropie H znamená množství informací, které jsou nutné k jejímu úplnému odstranění, tedy úplnému odstranění neurčitosti u posuzovaného jevu.

Nejjednodušší informace je typu ANO-NE, TRUE-FALSE, 0/1. Taková informace nám zároveň může posloužit pro odvození jednotky informace – jeden bit. Bit jako jednotka je tedy odvozena z míry neurčitosti dvou stejně pravděpodobných jevů.

Toto si můžeme ověřit tak, že do vzorce (1.1) dosadíme hodnoty například pro hod mincí (1.2). Pravděpodobnost p_i, že padne určitá strana mince je pro obě dvě strany stejná, tedy 0,5, takže:

$$H = -\sum_{i=1}^{2} 0,5 \log_2 0,5 = 1b \tag{1.2}$$

Ze vzorce vyplývá, že neurčitost je tím větší, čím větší je množina pravděpodobných výsledků. Na problém se můžeme podívat i z opačné strany - čím je problém složitější, tím větší množství informací je potřeba k tomu, aby byly odstraněny veškeré nejistoty (neurčitosti), které jsou s ním spojené. Informační entropie jako veličina má také širší použití - používají ji např. některé metody datamingu jako jsou rozhodovací pravidla nebo stromy pro identifikaci veličiny, která nejvíce přispívá k vysvětlení řešeného problému (a má tedy nejnižší entropii). Problematika dataminingu výrazně přesahuje možnosti těchto skript, takže, pokud Vás problematika zaujala budete si muset počkat na předmět Bezpečnostní informatika 3 (BI3) (Informatika v bezpečnosti), který je vyučován v prvním ročníku navazujícího studia.

Entropie je také extenzivně využívána např. v šifrování, kdy jedním ze základních předpokladů bezpečnosti je dobrý zdroj entropie jako nutný vstup generátoru náhodných čísel. Bez takového zdroje je možno narušit bezpečnost prakticky každého šifrovacího schématu a to bez ohledu na to, jak je jinak kvalitní.

Pro další studium je nutné si uvědomit rozdíl mezi **informacemi a daty** (údaji). *Informace* se nějaké sdělení, které u příjemce snižuje neurčitost – tuto vlastnost jsme už zmínili, pro rozlišení je ale nesmírně důležitá. Data, jako pojem, jsou totiž mnohem obecnější, jedná se také o sdělení. Tato sdělení však mohou, ale nemusí snižovat neurčitost. Data tedy mohou, ale nemusí obsahovat informace.

Informace jsou tedy podmnožinou všech dat. Například seznam všech studentů VŠB-TUO můžeme považovat za data. Výběr všech studentů, kteří studují předmět Bezpečnostní informatika 1 (BI1), však, pro mě jako pro vyučujícího tohoto předmětu, představují informace – snižují totiž u mě neurčitost v tom, kolik studentů budu vyučovat, kolik jich budu muset vyzkoušet, jak mám plánovat výuku apod.

Pro informaci je typická nutnost investice nějakého úsilí (energie), které je nutno vynaložit, abychom informaci získali z dostupných dat a je přitom jedno, jestli zpracování probíhá ručně nebo automatizovaně pomocí nějakého informačního systému nebo analytického nástroje.

S informacemi souvisí také další pojem - *znalost*. Tento pojem je často nesprávně významově zaměňován s informací. Znalosti jsou získávány interpretací a organizací informací a jejich dalším použitím např. pro rozhodování. Výše uvedený demonstrační příklad se studenty předmětu BI1 by znalost mohl představovat výstup analýzy odpovědí písemných prací vypracovaných při zkoušce předmětu. Výsledek by poskytl znalosti o probíraných tématech, u kterých studenti více chybují a byl by využitelný pro upravení skript/přednášek předmětu.

Dalším pojmem, se kterým budeme v tomto předmětu extenzivně pracovat je IT. Pokud hovoříme o **IT**, obvykle máme na mysli automatizované nástroje pro sběr, přenos a vyhodnocování údajů.

IT jako pojem se ovšem používají také v přeneseném významu, který se může částečně překrývat s významem pojmu informatika nebo ještě lépe pojmem aplikovaná informatika. **Informatika** jako věda se zabývá především zkoumáním informací jako takových, jejich vlastností, shromažďováním, zpracováním – těmito problémy se zabývá především v teoretické rovině. IT se proti tomu zabývají spíše praktickou stránkou těchto problémů - tedy že informace jsou zpracovávány na počítačích, pomocí softwarových nástrojů, že tyto počítače lze propojovat do sítí apod. IT se tedy zabývá v podstatě stejnou oblastí ale z praktičtějšího (aplikačního) pohledu.

Lepší vhled do rozdílů mezi může poskytnout nereprezentativní přehled disciplín informatiky a aplikované informatiky:

- informatika
  - teorie výpočtů
  - algoritmy a datové struktury
  - teorie informace a její kódování
  - teorie programování
  - formální metody
  - konkurenční, paralelní a distribuované systémy
- aplikovaná informatika
  - umělá inteligence
  - architektura počítačů
  - aplikovaná grafika a vizualizace
  - počítačová bezpečnost a šifrování
  - výpočetní vědy
  - specializované informatiky (zdraví, práva, apod.)
  - informační věda
  - softwarové inženýrství
- IT
  - aplikace počítačů a telekomunikačního zařízení pro získání, přenos a manipulaci s daty
  - často používána jako synonymum pro počítače a počítačové sítě
  - TV, chytré telefony, zařízení IoT jsou také považovány za IT

Dalším významným pojmem je **systém**, jedná se o pojem obecný v současné době často využívaný v různých významech. Systém bychom mohli obecně definovat jako souhrn prvků, které jsou vůči sobě v nějakém vztahu a vůči okolí působí jako celek.

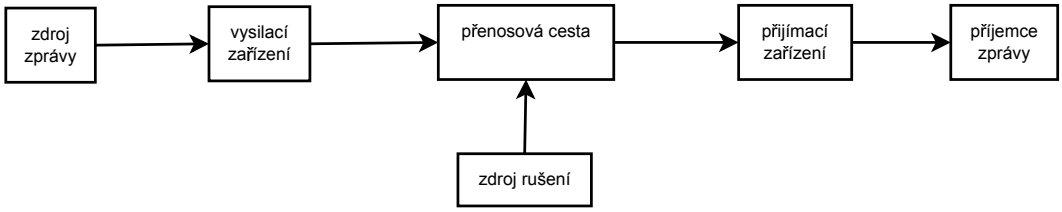
Na Informační systém (IS) pak lze nahlížet optikou výše uvedené definice systému: jako na společné působení lidí (peopleware), zařízení (hardware), programů (software) a organizačních opatření (orgware), které pracují společně na splnění vytyčených cílů (za jakým byl informační systém nasazen).

Taková definice odpovídá vymezení IS pomocí IT. IS přitom můžeme chápat i poněkud obecněji jako jakýkoliv systém, který slouží ke shromažďování, správu a vyhodnocování údajů ať již s pomocí výpočetní techniky nebo například formou kartotéky apod. Taková definice odpovídá více chápání IS jako systému pracujícího nad databázovým systémem.

Konečně pojmem **databáze** rozumíme systém pro řízení báze dat, tedy systém, který umožňuje efektivní správu dat ve smyslu jejich pořizování, údržby, výběru a to tak, aby data byla v databázi pokud možno obsažena pouze jeden krát (zamezení redundancím) a ve formě, která zaručí neustálou dostupnost a integritu dat. V češtině byly databázové systémy původně označovány jako Systém řízení báze dat (SŘBD), v současnosti se ale i v češtině používá souhrnné označení databázový systém nebo zkráceně databáze.

Ve vztahu k IS slouží databáze mimo jiné jako tzv. backend. Tedy jednotlivé IS si data, se kterými pracují, ukládají do různých databází a tím řeší všechny otázky konzistence udržovaných dat - stará se o ně databáze sama, bez nutnosti zásahu ze strany IS.

Už víme, že informace je objekt nehmotné povahy, víme také, že informační technologie nám umožňují s informacemi efektivněji pracovat – k tomuto účelu ale musí být tyto informace nějakým způsobem vyjádřeny fyzicky a přeneseny na místo určení ke zpracování. Procesu sběru, zpracování, uchovávání, přenosu a využívání informace říkáme **informační proces**. V průběhu informačního procesu může dojít ke zkreslení informace zejména v průběhu přenosu informace vlivem informačních šumů (viz obr. 1.1).



Obrázek 1.1: Obecné schéma sdělovací soustavy

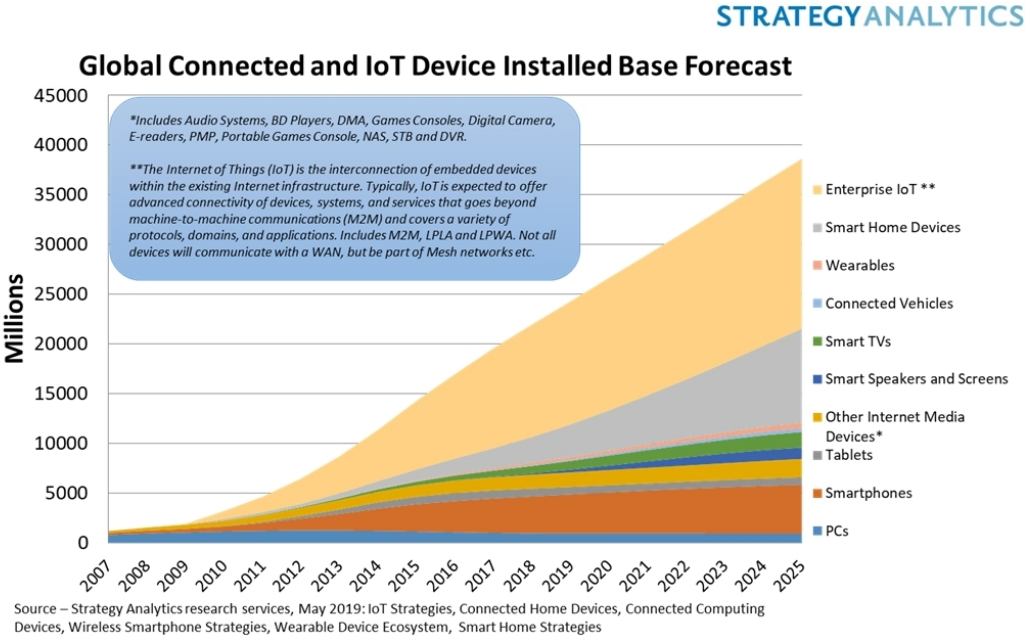
Obr. 1.1 představuje obecné schéma sdělovací soustavy, které se v různých obměnách objevuje

v řadě oborů od sociologie až po kybernetiku. *Zdroj zpráv* může představovat počítač stejně jako člověka, který produkuje zprávu a ta je zakódována ve *vysílacím zařízení* do podoby signálu vhodného pro přenos daným *sdělovacím kanálem*.

Signál se na místo určení přenáší prostřednictvím sdělovacího kanálu. V těchto kanálech může docházet k *šumům*, které informace deformují a snižují její efektivní množství. Prakticky šum působí tak, že modifikuje přenášený signál. Řada sdělovacích soustav je proti působení šumu do určité míry odolná. Pokud aplikujeme výše uvedené na běžnou konverzaci mezi lidmi, budou mít charakter vysílacího zařízení naše hlasivky, roli přijímače bude hrát náš sluch. Signál bude mít charakter vlnění šířeného vzduchem. Na tyto signály budou působit zdroje rušení ve formě zdrojů zvuku v naší blízkosti. Pokud je úroveň hluku v našem okolí nízká, nedělá nám obvykle problém porozumět podstatě sdělení, pokud však intenzita rušení přesáhne určitou mez, přestáváme postupně rozumět až do stavu kdy nejsme schopni odlišit přenášené sdělení od rušení.

V případě, komunikace dvou lidí je výhodou, že obě strany mohou vyhodnocovat průběžně kvalitu přenosu informace a reagovat, např. tak, že strana komunikace, která neporozuměla sdělení požádá o jeho zopakování nebo vysvětlení. Toto si ale můžeme dovolit pouze proto, že na obou stranách komunikace je člověk, který je inteligentní, takže je schopen takového vyhodnocení. Co ale dělat v případě, že na jedné nebo dokonce obou stranách komunikace není člověk, ale stroj.

Takový scénář je ve skutečnosti běžnější než klasická komunikace, jelikož různých zařízení a senzorů, které jsou připojeny k internetu je v důsledku masivního nástupu IoT mnohem větší množství než je lidí. Vzhledem k tomu, že tato zařízení jsou často určena pro monitoring popř. řízení různých technologií nebo procesů v reálném čase, jejich nároky na komunikaci po síti jsou velmi vysoké. Předpokládá se také, že počet takových zařízení v příštích letech bude dále masivně růst, viz obr. 1.2.



Obrázek 1.2: Předpokládány vývoj počtu zařízení IoT (převzato z [46])

Počítače, senzory a obdobná zařízení dnes nejsou (a vlastně nikdy nebyla) inteligentní. Jak tedy je možno zajistit kvalitu datových přenosů mezi takovými zařízeními? V historii se objevila celá řada algoritmů a postupů, které tento problém více či méně úspěšně řeší. Jedním z prvních bylo použití CRC algoritmů (Cyclic redundancy check (kontrolní součty) (CRC)). CRC algoritmy pracovaly tak, že pro bloky přenášených dat vypočítávaly číslo. Toto číslo pak bylo odesláno společně s daty. Po příjmu program/systém provede výpočet CRC z obdržených dat a porovná vypočtené číslo s obdrženým CRC. Pokud se oba kontrolní součty shodují, předpokládalo se, že datový přenos byl dokončen v pořádku.

Hlavní nevýhodou CRC algoritmů je jejich jednoduchost. Přece jenom tyto algoritmy byly poprvé navrženy v roce 1961, kdy ale možnosti výpočetní techniky byly totálně odlišné než jsou dnes. Většina počítačů nebyla vůbec připojena do sítě (masivní nástup Internetu nastal až v 90. letech). Jednoduchost výpočtu byla také vyžadována nízkým výkonem počítačů té doby. Toto omezení ale dnes již

neplatí, je tedy možné je nadále považovat za bezpečné?

CRC umožňují snadno identifikovat náhodné narušení komunikačního procesu, v případě, že ale je proces komunikace narušen motivovaným útočníkem, např. hackerem, CRC přestávají plnit ochrannou úlohu, přenášená data je totiž možné poměrně jednoduše pozměnit tak, aby změněná data po přepočítání vedla na stejný kontrolní součet. Proto se pro účely ověření dnes používají spíše bezpečné hašovací algoritmy (SHA) nebo na nich založené algoritmy jako např. algoritmy elektronického podpisu. Tyto algoritmy již využívají některých postupů kryptografie, což činí jejich narušení značně obtížnější.

SHA, šifrováním a elektronickým podpisem se budeme zabývat v pozdějších kapitolách, nyní se vraťme k podstatě signálu a jeho vyjádření a také otázce, co to vlastně signál je? *Signál* je stav popřípadě proces látkového nebo energetického média. Signál je tedy tím kýženým fyzickým vyjádřením nehmotné informace. Aby nám signály dávaly nějaký význam, musíme je používat podle určitých pravidel, která jim tento význam přiřadí. Takové soustavě pravidel říkáme **kód**.

Každý kód se skládá z jednotlivých symbolů, kterými pokud je určitým způsobem zřetězíme za sebou můžeme vyjádřit zprávu. Seznamu přípustných symbolů kódu říkáme *abeceda*.

Kód je obvykle navrhován s ohledem na charakter informací, které budou přenášeny. Toto můžeme demonstrovat jednoduše porovnáním abeced různých jazyků. Vezměme si třeba českou a anglickou abecedu. Pro přehlednost se omezíme pouze na velká písmena.

- anglická: ABCDEFGHIJKLMNOPQRSTUVWXYZ
- česká: AÁBCČDĎEÉĚFGHIÍJKLMNŇOÓPQRŘSŠTUÚŮVWXYÝZŽ

Českou abecedu můžeme použít pro zakódování jakéhokoliv textu v angličtině, pokud ale chceme použít interpunkci, což je v českém jazyce běžné, neposkytuje anglická abeceda dostatek symbolů pro zachycení českého textu abecedou anglickou.

Teoreticky můžeme hovořit o tzv. *optimálním kódu* – tedy takovém kódu, který právě postačuje pro přenesení dané informace. Takový kód ovšem není právě praktický, protože není univerzální. Z tohoto důvodu v běžně používaných kódech preferujeme určitou míru redundance. Jak si to představit? Použijme běžnou abecedu, kterou používáme každý den. Představme si situaci, že píšeme e-mail. Optimální kód bude takový, který bude obsahovat pouze ta písmena, která jsme v mailu potřebovali použít a žádná jiná. Co když ale v jiném mailu bude potřeba použít právě tato chybějící písmena? Pro takový mail by proto bylo potřeba použít jiný kód, složený z jiných písmen.

S takovým použitím kódů je tedy spojená jistá režie, protože musíme zajistit schopnost výpočetní techniky takovéto zprávy zpracovat. Použitím optimálního kódu se nám sice snížila náročnost z hlediska potřebného datového přenosu pro zprávu, ale zároveň se celkově výrazně zvýšila režie celého procesu přípravy kódů.

Ve výpočetní technice se tento problém řeší použitím do určité míry univerzálními systémy kódování, které často označujeme jako znakové sady (např. American Standard Code for Information Interchange (ASCII), UCS Transformation Format (UTF-8) a další). Obvzláště v minulosti byly značně nekompatibilní. Např. v minulosti se pro kódování češtiny používaly následující znakové sady: ISO 8859-2 (ISO Latin 2), Windows-1250, CP852 (PC Latin2), kód Kamenických a to se nejednalo o vyčerpávající seznam.

Naštěstí v současnosti ji povětšinou těmito problémy nejsme tak zatíženi. Standard UTF podporuje více než 120 000 různých znaků v 129 moderních a historických znakových sadách a symbolech. Nejpopulárnější UTF znakovou jsou UTF-8 a UTF-16. UTF-8 používá jeden bajt (8 bitů) pro zakódování jednotlivých znaků. UTF-16 proti tomu používá dva bajty k témuž, čímž umožňuje použití rozsáhlejších sad symbolů Unikódu. To je logické, jelikož UTF-8 podporuje pouze 256 znaků zatímco UTF-16 65 536 znaků. Je však potřeba říci, že ani UTF-16 nepokrývá všechny existující znaky ve všech abecedách - to dělá pouze UTF-32.

UTF-8 je populární především ve státech používajících různé deriváty latinky, zatímco UTF-16 je primárně využíváno v Asii. Řada jazyků v zejména v jihovýchodní Asii totiž nemá samostatné symboly pro jednotlivá písmena, ale třeba slabiky, nebo celá slova (Čínština, Korejština) nebo dokonce používá kombinace obou přístupů (Japonština). Pro pokrytí takových jazyků jsou pak potřeba tisíce znaků.

Z praktického pohledu tedy obětujeme část efektivity kódu a na oplátku získáme kód který je univerzálněji použitelný pro kódování všech zpráv. Takový kód již lze efektivně implementovat na úrovni operačního systému.

Vraťme se ke problematice kódování a abeced ještě obecně. Na základě entropie lze odvodit některé důležité vlastnosti použité abecedy a systému kódování. Konkrétně lze, za předpokladu, že pravděpodobnost výskytu každého symbolu abecedy je stejná, vypočítat maximální entropii abecedy H_{max}

podle vzorce (1.1) a tuto veličinu pak použít pro určení *efektivity kódování*.

Efektivitu můžeme měřit pomocí relativní entropie h (1.3) nebo pomocí tzv. redundance kódu r (1.4). Relativní entropií rozumíme poměr entropie kódu použitého pro zakódování zprávy k maximální entropii celé abecedy. Výpočet relativní entropie provedeme podle vzorce (1.3).

$$h = \frac{H}{H_{max}} \tag{1.3}$$

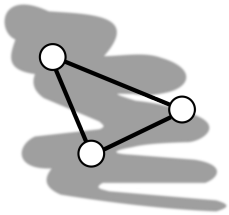
Kde
h ... relativní entropie
H ... entropie reálně použité abecedy
H_{max} ... maximální entropie celé abecedy

Optimální kód by se logicky měl mít hodnoty H a H_{max} velmi podobné, proto by se relativní entropie měla blížit 1. Pokud relativní entropii odečteme od 1, získáme redundanci (nadbytečnost) kódu.

$$r = 1 - h = 1 - \frac{H}{H_{max}} \tag{1.4}$$

Kde
r ... redundance kódu
h ... relativní entropie
H ... entropie reálně použité abecedy
H_{max} ... maximální entropie celé abecedy

Pro signál platí, že jedna informace je vyjádřena minimálně jedním signálem (tedy jedním a více signály), zatímco jeden signál obsahuje maximálně jednu informaci.



Návaznosti
Redundance je základním stavebním kamenem ochrany dat. Redundance je využívána např. v šifrování viz kapitoly věnované symetrickému a asymetrickému šifrování v těchto skriptech, popř. předmětu *Počítačové sítě a ochrana dat*.

Z historického hlediska můžeme uvažovat o celkovém množství informací, které jsou v daném okamžiku aktivně využívány. Intuitivně cítíme, že toto množství se neustále zvyšuje. To souvisí s rostoucím množstvím informací, které jsme použili pro zlepšení poznávacích procesů (citlivější přístroje, výkonné počítače schopné zpracovávat velké objemy dat apod.).

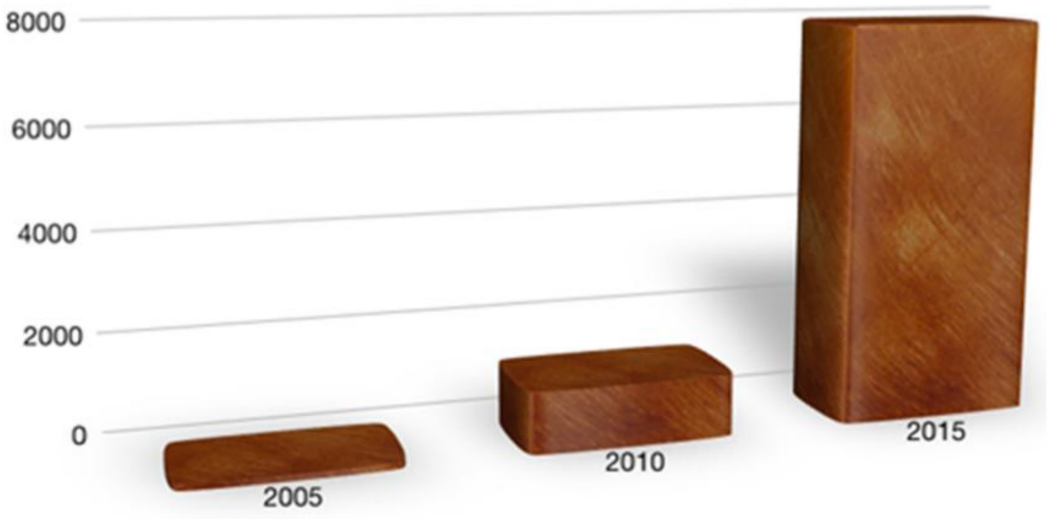
Prakticky se to ale projevuje také ve způsobu jakým data zpracováváme nebo dokonce konzumujeme např. formou sledování videa ve vysokém rozlišení.

M. Mertal na kongresu leteckého průmyslu v roce 1949 předpokládal, že nárůst informací v čase má exponenciální charakter. Tento předpoklad experimentálně dokázal roku 1955 D. S. Price. Graficky je informační nárůst zobrazen na obr. 1.3. V tomto případě je informační nárůst demonstrován úložnou kapacitou (stávající a předpokládanou) nutnou pro jeho pokrytí.

Je zřejmé, že exponenciální charakter informační nárůstu nemůže pokračovat neomezeně dlouhou dobu, bude vždy omezen hranicí technických možností dané doby. S tím, jak se blížíme této hranici, dojde ke změně charakteru křivky informačního nárůstu. Ta nejprve ztratí svůj exponenciální charakter a bude růst dále již jen lineárně se stále zmenšujícím se sklonem, až se stabilizuje na určité úrovni a na této úrovni zůstane do doby, než dojde k průlomovému objevu, který znovu nastartuje informační nárůst. Charakter průlomu určí, jestli další nárůst bude spíše lineární nebo exponenciální.

Pohledem do minulosti lze vysledovat několik období prudkého informačního nárůstu následovaného z hlediska informací stabilním obdobím, jmenujme například antiku, renesanci a období průmyslové revoluce a v moderní době masivní nástup výpočetní techniky.

Z dnešního pohledu se jako limitující jeví proces miniaturizace tranzistorů jako základních stavebních bloků moderních procesorů. Přechod na další úroveň miniaturizace je totiž v současnosti natolik náročný, že si jej nemůže dovolit každý výrobce procesorů nebo dokonce nový výrobce procesorů.To vedlo ke konsolidaci na trhu, kdy nejmodernější procesory je schopna vyrábět pouze relativně malá



Obrázek 1.3: Informační nárůst demonstrovaný na úložných kapacitách nutných pro jeho pokrytí (převzato z: [61])

skupina výrobců. Při omezených výrobních kapacitách pak každé narušení výroby může vést k celosvětovým problémům v dodávkách, jak jsme byli v minulých letech svědky.

1.2 Další vlastnosti informace

Další podstatnou vlastností informace, je že její schopnost odstraňovat entropii v čase klesá. To znamená, že informace je užitečná pouze po omezenou dobu. Po jejímž uplynutí se informace stává nadbytečnou, jelikož už svému příjemci nepřináší signifikantní užitek. Životnost informace je tedy časově omezená. V rámci zkoumání charakteru stárnutí informací se zavádí pojem *poločas stárnutí*.

Poločas stárnutí informace lze definovat jako čas od zveřejnění informace do okamžiku, kdy počet nových citací na tuto informaci odkazujících poklesne na jednu polovinu ve srovnání s okamžikem maximální aktivity (užitečnosti) informace.

Tento čas není možné zjistit přesně a bude se tak výrazně lišit případ od případu. Při zjišťování přibližného poločasu stárnutí dané informace bereme v úvahu obvykle tzv. *zpětný poločas stárnutí*. Hodnotíme tedy informaci, která již prošla celým svým životním cyklem. Znalosti o průběhu tohoto cyklu pak používáme pro odhad průběhu cyklu obdobných informací.

Ideální křivka stárnutí informace by mohla být vyjádřena následující rovnicí (1.5):

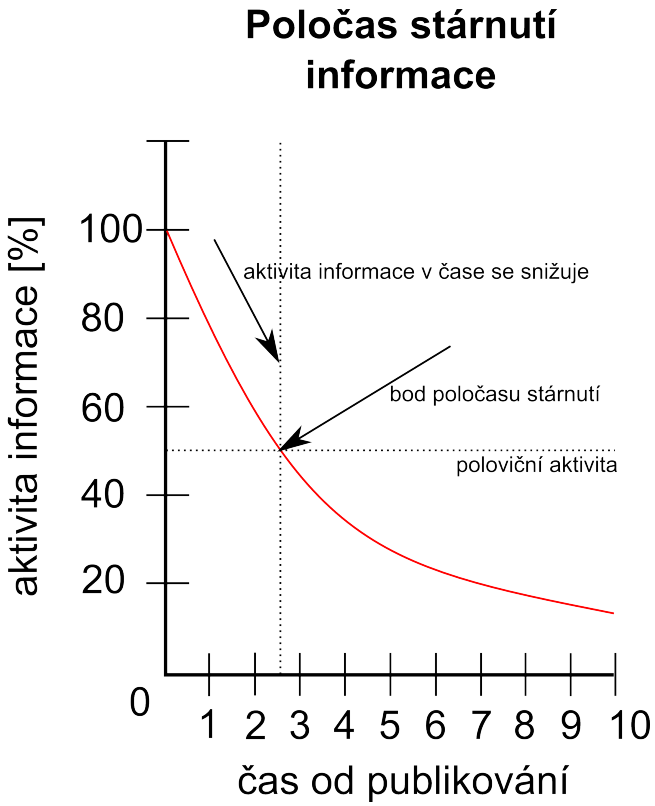
$$y = 1 - \left(\frac{a}{e^x} \cdot \frac{b}{e^{2x}} \right) \tag{1.5}$$

kde
$a + b = 1$
a, b ... jsou koeficienty, které určují progresivitu stárnutí
y ... hodnota kumulovaného procenta publikací v jednotlivých letech
x ... čas v dekádách

Jak by mohlo vypadat grafické znázornění stárnutí informací, je patrné z obrázku 1.4.

Obrázek 1.4 ukazuje stárnutí informace z nějakého vrcholu až takřka k nule. Je očividné, že tento obrázek neuvažuje tzv. *okrajové podmínky*. Informace po svém zveřejnění totiž není okamžitě na svém „vrcholu“, trvá nějakou dobu, než se dostane do širokého podvědomí a začne být aktivně využívána a projeví se tedy měřitelným způsobem v citacích, odkazech apod. Dále můžeme říci, že informace bez ohledu na její charakter se nerozšíří nikdy úplně všude - tedy aktivita informací v reálném světě nebude nikdy 100 %.

Reálná informace proto bude nejprve z hlediska aktivity narůstat, s tím jak se bude postupně šířit, poté dojde ke kulminaci aktivity a následovat bude úpadek aktivity. Příklad takového životního cyklu

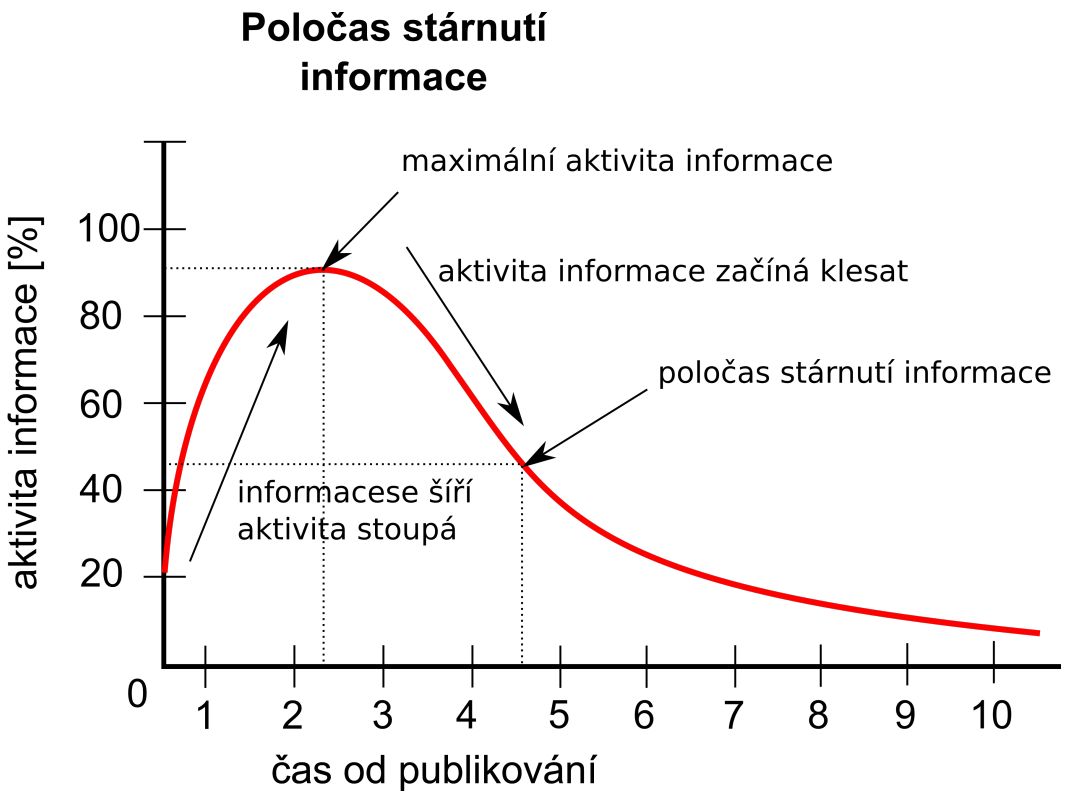


Obrázek 1.4: Křivka stárnutí ideální informace

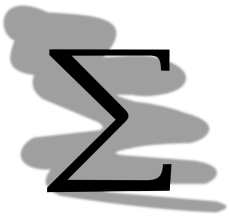
naleznete na obrázku 1.5. Informace také nedosáhne nikdy úplného rozšíření, tudíž může se pouze přinejlepším blížit hodnotě 1, nikoliv jí dosáhnout.

Parametry křivky stárnutí informace se budou lišit pro jednotlivé obory lidské činnosti.

Obecně platí, že humanitně zaměřené obory mají delší poločas stárnutí informace, vysoce inovační obory, jako např. IT, pak mají extrémně rychlý životní cyklus informace.



Obrázek 1.5: Stárnutí informací při uvažování okrajových podmínek



Shrnutí

Informace je objekt nehmotné povahy, sdělení (zprávy), jehož základní vlastností je to, že u příjemce informace snižuje neurčitost. Od *dat* se liší zejména nutností vynaložit určitou energii na získání informací.

Objem informací zpracovávaných společností prudce roste. Dynamika nárůstu souvisí s technologickým pokrokem k zejména pak omezeními, která jsou s používanými technologiemi spojena (*hranice technologických možností*).

Informace stárnou. Pro změření míry tohoto stárnutí byl zaveden pojem *poločas stárnutí informace*, jako doba od zveřejnění informace po dobu než počet nových odkazů na ni klesne na polovinu (ve srovnání s počátkem životního cyklu informace).

Kontrolní otázky

1. Definujte pojem data a srovnejte jej s pojmem informace.
2. Jak se určuje poločas stárnutí informace?
3. Jaké metody lze použít pro ověření poškození přijaté informace?
4. Proč při uvažování okrajových podmínek životního cyklu informace aktivita informace nejprve stoupá a teprve potom klesá?
5. Definujte informační entropii pomocí informace.

Správné odpovědi

1. Data jsou nadmnožinou informací. Jedná se o obecná sdělení, která u příjemce mohou, ale nemusí snižovat informační entropii. Z dat můžeme informace získat investicí energie – tedy aktivním zpracováním informací za účelem získání odpovědí na naše otázky.
2. Odhadem na základě empiricky změřených poločasů stárnutí informací podobného charakteru, které již prošly celým životním cyklem.
3. CRC, SHA, elektronický podpis.
4. Protože informace potřebuje nějaký čas pro rozšíření se a teprve potom začíná vlastně stárnout.
5. Informační entropie je množství informací, které je nutno získat pro kompletní odstranění neurčitosti určitého jevu.

Test

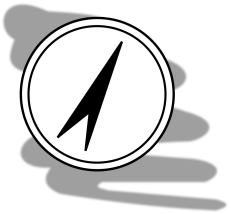
1. základní jednotkou informace je jeden
   (a) bit
   (b) kilo bit
   (c) mega bit
2. informace se obecně přenáší formou
   (a) jedniček a nul
   (b) dvojek a trojek
   (c) signálů
3. množství informací ve společnosti roste
   (a) lineárně
   (b) exponenciálně
   (c) logaritmicky
4. základním omezením budoucího zvyšování množství informací ve společnosti je
   (a) hranice technologických možností
   (b) kapacita současných výpočetních strojů
   (c) omezení není
5. IS se skládá z:
   (a) Lidí, IT a org. norem
   (b) Peopleware, software, hardware, orgware
   (c) Lidí, výpočetní techniky, programů a organizačních pravidel

Správné odpovědi

1. a), 2. c), 3. b), 4. a), 5. všechny odpovědi správně

Kapitola 2

Programové vybavení PC



Náhled kapitoly
Software je hybnou součástí každodenního života drtivé většiny ekonomicky aktivních lidí. Je to také on, který představuje určité bezpečnostní riziko. Z tohoto důvodu si povíme něco o členění software do kategorií a tyto kategorie si vysvětlíme. Zároveň se podíváme do určité (omezené) míry i na bezpečnostní aspekty užití software.

Po přečtení této kapitoly budete vědět

1. co je to software
2. jak můžeme software dělit
3. co jsou databáze
4. jak vypadá XML soubor

Čas pro studium
Pro prostudování této kapitoly budete potřebovat přibližně 30 minut.

Programové vybavení počítače tvoří rozhraní mezi počítačem (hardware) a lidskou bytostí (peopleware). Vzhledem k tomu, že se počítače staly nedílnou součástí každodenního života, je nezbytné se o něm něco málo dozvědět.

Na následujících stránkách se pokusím rozčlenit software do několika kategorií. Hranice mezi jednotlivými kategoriemi ovšem není úplně ostrá, berte prosím tedy následující stránky jako pokus začlenění problematiky SW do širšího kontextu.

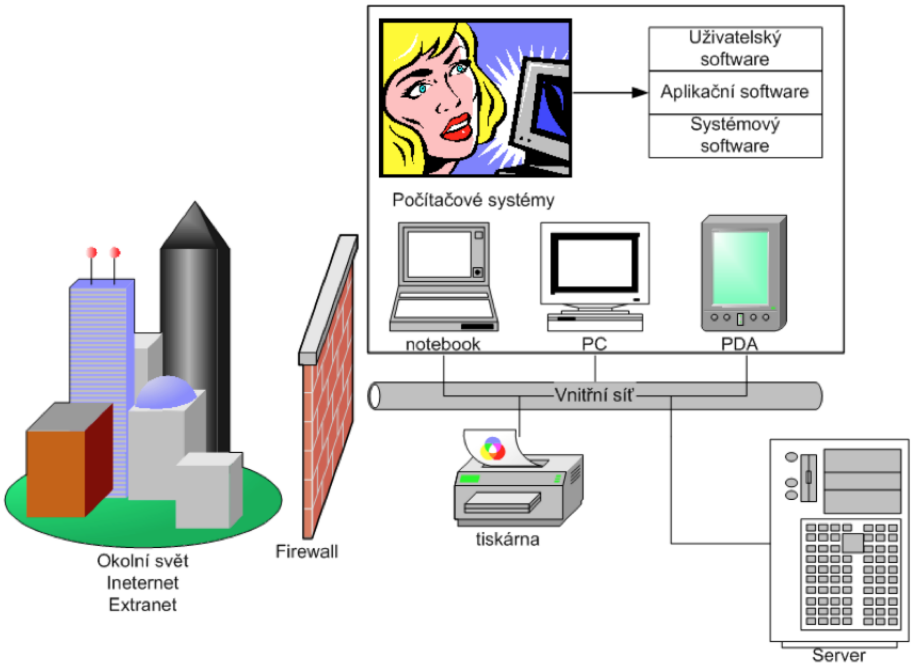
2.1 Členění software

Software lze členit podle mnoha různých charakteristik, pro základní rozlišení skupin software nám může posloužit následující členění podle účelu použití software:

1. systémové programy
2. aplikační programy
3. uživatelské programy

Základní filozofický rozdíl z hlediska bezpečnosti mezi výše uvedeným software je v tom, jakým způsobem se uživatelé a administrátoři staví k nakládání s ním.

Z hlediska administrace obvykle v podnikovém nasazení požadujeme, aby systémový software pro koncového uživatele fungoval jako černá skříňka – tedy koncový uživatel do nich nemůže zasahovat, jakýkoliv zásah může být fatální pro chod celého počítače.



Obrázek 2.1: Uživatel v informačním systému

Aplikační software vykonává „skutečnou, produktivní“ práci, za kterou je zaměstnanec placen. Možnosti konfigurace, změn tohoto typu software mohou proto být povoleny vyšší. Zároveň aplikační software funguje nad software systémovým, takže problém s jednou aplikací obvykle neohrožuje fungování systému jako celku (může ale být průvodním jevem hlubších problémů).

Konečně uživatelský software běží obvykle nad systémovou a aplikační vrstvou, škody, které je pomocí něho možno napáchat jsou tak omezené.

2.2 Systémový software

Do kategorie systémového software se řadí především:

1. operační systémy a jejich nadstavby
2. databázové systémy
3. testovací, diagnostické a antivirové programy

Operační systémy jsou specializované programy, které zabezpečují fungování samotného počítače. *Operační systémy* mají dvě základní funkce:

1. přidělování zdrojů (procesory, paměti, periferie),
2. zabezpečení komunikace člověk-počítač (hardware)

Na světě existují desítky, možná stovky různých operačních systémů, které se výrazně liší svými vlastnostmi. Pokusme se je rozčlenit do několika kategorií. Nejedná se samozřejmě o úplný výčet, při troše snahy bychom mohli nalézt další kritéria, podle kterých by bylo možné operační systémy členit jinak.

Dělení podle
druhu počítače

1. superpočítače
2. servery
3. PC
4. tablety, smartphony

5. a další

Počítače v tomto případě dělíme podle „velikosti“. Dělení je ale možné použít také odlišné např. podle počtu uživatelů, které s operačním systémem mohou zároveň pracovat:

1. jednouživatelské (Desktop Operating System (DOS), Windows95, 98)
2. víceuživatelské (Operační systém (OS) UNIXového typu (klasické UNIX systémy, LINUX (Linux is not Unix (Linux)), systémy na bázi Berkeley Software Distribution (též Berkeley Unix) (BSD) a další), Windows2000 a vyšší)

Současnou prací v tomto případě nemyslíme stav, kdy ze vzdáleného počítače spustíme nějakou aplikaci (aplikační servery), nebo využíváme nějakou službu (např. přístup na WWW stránky). Víceuživatelskou prací v tomto případě myslíme stav, kdy několik uživatelů ze vzdálených počítačových systémů pracuje s počítačem stejným způsobem jako by u něj seděli.

V této oblasti tradičně kralují operační systémy odvozené od UNIX. Windows 2000 a novější v této oblasti umožňují nějaký vzdálený přístup, je ovšem otázka zda se takovýto přístup dá považovat za víceuživatelský. Plně víceuživatelský model užití podporují až serverové verze Windows.

Operační systémy lze členit také podle počtu úloh, které je možno zpracovávat současně.

1. monoprogramový (DOS, Windows 3.11)
2. multiprogramový (UNIX, Windows9x, 2000, XP, OS/2 . . .)

Výkon procesoru lze vyjádřit pomocí počtu cyklů, které je schopen realizovat za určitou dobu, vetšinou za 1 sekundu. Právě tyto cykly přiděluje operační systém programům, podle jejich potřeb. Jednotlivé činnosti, které od počítače požadujeme se tak nevykonávají průběžně, ale po jednotlivých instrukcí, které operační systém skládá za sebou tak, aby pro koncového uživatele vznikla iluze souběžné práce velkého množství procesů v počítači. Vytváří se tedy fronty požadavků jednotlivých úloh (programů), které se postupně vykonávají.

Procesorem ve výše uvedené definici se rozumí samostatná výpočetní jednotka tedy procesor nebo jádro procesoru v případě procesorů obsahujících více jader. Vícejaderné procesory se tedy chovají jako víceprocesorové systémy a vytvářejí pro každé jádro samostatné vlákno, na kterém se jednotlivé činnosti vykonávají.

Podle použité architektury lze OS členit na:

1. klasické
2. otevřené (např. dle POSIX standardu)

Portable Operating System Interface [for Unix] (POSIX) je standardem, který by měl zajistit hladkou interoperabilitu mezi jednotlivými zařízeními pracujícími s různými UNIXovými operačními systémy. Hladkou interoperabilitou se v tomto případě rozumí především schopnost zkompilovat, bez nutnosti provést další úpravy, programy především pro různé verze UNIXových systémů, nebo systémům podobným UNIX (např. LINUX).

Nadstavby operačních systémů

Slouží ke zkvalitnění komunikace člověk – počítač. Mezi tyto nadstavby byly například často zařazovány i Windows 3.11, protože ke své práci potřebovaly operační systém DOS. V dnešní době se jedná především o programy, které usnadňují práci se soubory a složkami jako jsou například Total Commander, Servant Salamander, nástroje pro defragmentaci disku, různé editory nastavení operačního systému apod.

Do oblasti systémového software jsou také často zařazovány databázové systémy. Jedná se o systémy, které zabezpečují operace nad daty shromážděnými v tzv. bázi dat. Operacemi v tomto případě myslíme vkládání, editace a výmaz dat. Databázový systém umožňuje provádět výběry (filtrování dat) podle zadaných požadavků. Drtivá většina databázových systémů pro zabezpečení výběrů používá dotazovací jazyk Structured Query Language (SQL), tedy česky strukturovaný jazyk pro dotazování.

Vedení dat v jednotné bázi dat umožňuje uchovávat data pouze efektivně na jednom místě. Toho se dosahuje tak, že související data jsou propojena. Tím pádem v databázi nevznikají nekonzistence v důsledku duplicit.

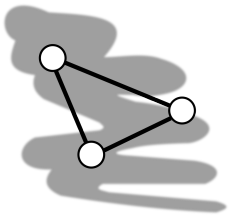
Typy

1. stromové (DBS/25)
2. síťové (IDMS)

3. relační
   (a) „velké“ - ORACLE, INFORMIX, PROGRESS, MySQL, MS SQL Server
   (b) „malé“ - dBASE, FoxPro, MS Access, Paradox, Clipper)
4. objektové (Matisse, NeoAccess . . .)
5. XML (Berkeley DB XML, Xyleme Zone Server, ...)
6. NoSQL databáze (MongoDB, CouchDB, ...)

Síťové a stromové databázové systémy ve výčtu uvádím pro úplnost, tyto systémy byly překonány v osmdesátých letech systémy relačními, které představují majoritní databázovou architekturu dneška. Přístupy využívané stromovými a síťovými databázemi se ale dosud využívají, jako metoda pro ukládání lokálních dat. Jsou tedy spíše využívány jako datové formáty.

V relačních databázích jsou data uchovávána v tabulkách s definovanou strukturou (sloupce tabulky), samotná data se pak vkládají do jednotlivých řádků tabulky. Každý řádek je v obvykle jednoznačně identifikovatelný pomocí *primárního klíče*. Tabulky samotné lze v databázi propojovat vazbami, nazývanými *relace* - odtud název relační databáze.



Relační databáze
Pro lepší pochopení funkce relačních databází je do cvičení tohoto předmětu zařazena výuka MS Access jako relativně uživatelsky přívětivého databázového systému. MS Access sice řadíme mezi „malé“ databáze, jedná se ale o databázi relační. Principy, které používá jsou tak shodné s principy databází „velkých“.

Podrobnosti o použití naleznete také ve skriptech *Bezpečnostní informatika 1 - Návody do cvičení* [88].

Objektové databázové systémy vycházejí z odlišnějšího pohledu na data - někdo by možná řekl intuitivnějšího pohledu. Filozofický přístup je následující: z reálné situace, o které potřebujeme shromažďovat data, vybereme několik objektů (například student, předmět . . .) u těchto objektů pak zkoumáme jejich vlastnosti - data, která o nich lze evidovat a také způsob jakým se mají chovat v databázovém systému - metody. Objekty jsou potom shromažďovány v databázi.

Výhodou oproti relačním databázím je mnohem širší portfolio vztahů mezi databázovými objekty, s možnostmi zachycení např. dědičnosti apod. Tímto způsobem se práce s databází filozoficky více přibližuje způsobu, jakým je navrhován software. To s sebou ale nese také problém, že tento typ databází vyžaduje ke svému nasazení poměrně hluboké znalosti systému, což představuje významnou překážku pro nasazování takových systémů v praxi.

Společně s celkovou vyspělostí relačních databází vytvořilo efektivní překážku pro rozšíření takových databází. A tak relační databáze zůstávají i v současnosti nejrozšířenější, byť s postupem času získávají některé nové schopnosti, které byly původně dostupné exkluzivně v jiných typech databází. Dobrým příkladem takového postupu jsou *XML databáze*.

Extensive Markup Language (XML) v češtině znamená rozšiřitelný značkovací jazyk. XML vychází z toho, že řadu dat, které běžně vedeme v dokumentech, lze intuitivně popsat pomocí značek. Například obchodní dopis by bylo možné zaznamenat následovně:

```
<dopis>
<adresat>
<jmeno>Jan</jmeno> <prijmeni>Nepomuk</prijmeni>
<adresa>
Ulice 15
Ostrava
702 00
</adresa>
</adresat>
<vec>Konference ABC2015</vec>
<teloDopisu> ... text dopisu ... </telo_dopisu>
</dopis>
```

Skutečný XML dokument by obsahoval ještě informaci o použitém standardu XML, kódování znaků a případně i o použitém schématu (šabloně). Pro nás je pouze podstatné, že takto strukturované dokumenty je jednodušší uchovávat a dále s nimi nějakým způsobem pracovat. Údaje v takovéto

strukturované podobě mají obrovskou výhodu v tom, že je možné je uchovávat na jediném místě - v jediném souboru, což je hlavní rozdíl proti relačním databázím, které na vyjádření složitějších vazeb v datech mohou vyžadovat i větší množství propojených tabulek.

XML databáze lze ještě dělit podle toho, zda se jedná o „čistě“ XML databáze (umí zpracovávat data pouze v XML) nebo se jedná o databáze relační s rozšířenou podporou XML, např. ve smyslu formátování výstupů, ale s vnitřním ukládáním dat do běžných propojených tabulek.

Právě přidání podpory pro XML výstupy také do značné míry omezilo potřebu nasazování čistých XML databází. A tak ani tato vlastnost neukončí ani do budoucna nadvládu relačních databází.

Konečně *NoSQL databáze* jsou databázovými prostředky, které úmyslně rezignovaly na členění ukládaných šablon do podoby tabulek. Zjednodušeně řečeno - všechna data se ukládají na „jednu hromadu“, se kterou se pak dále pracuje. Tento typ databází se hodí pro řešení úloh, na které již výkonově nepostačují databáze relační. Pro tyto problémy se vžil anglický název big data. Typickým příkladem mohou být data, na základě kterých nabízí vyhledávače, jako je např. Google Search nebo Microsoft Bing a další, výsledky svých vyhledávání. Indexace jednotlivých stránek do podoby tabulek již dávno není možná a databáze NoSQL nabízí elegantní řešení tohoto problému.

NoSQL databáze lze obecně použít všude tam, kde je nutno zpracovat obrovské množství různorodých dat. V této jedné konkrétní oblasti tak NoSQL databáze dominují nad databázemi relačními. V současnosti se objevují některé snahy nasazovat ve větší míře tento typ databází také v prostředí, kde manipulujeme s „normálními“ objemy dat. Využívá se přitom strutkturální jednoduchosti těchto databází. To umožňuje flexibilnější manipulaci s daty.

Na druhou stranu datové struktury využívané v relačních databázích umožňují ukládat data „defenzivně“ a automaticky tak zabránit celé řadě inkonzistencí, které při manipulaci s daty mohou vznikat. NoSQL databáze takové schopnosti nemají a tak případná logika bezpečné manipulace s daty musí být implementována na aplikační úrovni, což není zcela šťastné řešení.

Z tohoto důvodu lze říci, že NoSQL databáze v blízké budoucnosti relační databáze nenahradí.

Testovací a diagnostické programy

Slouží k prověřování správného fungování technických prostředků jako jsou disky, paměť apod. Patří zde např. ScanDisc, nástroje pro defragmentaci disku apod., ať už jako přímá součást operačního systému nebo jako komerční nástroje, které přinášejí oproti nástrojům vestavěným něco navíc. Příklady takových programů mohou být třeba Norton Utilities, O& O Defrag, diagnostické nástroje pro testování paměti – GoldenMemmory a další.

2.3 Aplikační programy

Programy orientované na řešení určitých tříd úloh v různých oblastech použití. Jsou méně obecné než programy systémové. Řeší třídu problémů určité třídy uživatelů. Jejich společnou vlastností je to, že jsou určeny obvykle pro velkou skupinu lidí, nezáleží přitom, zda je program šířen komerčně nebo nekomerčně.

Typy

1. Kancelářské balíky (Microsoft (MS) Office, LibreOffice . . .)
2. ediční systémy DTP (např. Adobe PageMaker, InDesign, QuarkXPress, Ventura Publisher apod.)
3. statistický software (StatGrafik, MathLab, Statistica . . .)
4. grafické systémy
   (a) editace rastrové grafiky (např. fotografie) - PhotoShop, PaintShop Pro, Gimp, Corel PhotoPaint;
   (b) editace vektorové grafiky – Corel Draw, Adobe Ilustrátor apod.
5. ekonomický software
6. (účetnictví, skladová evidence apod.)
7. řízení projektu (Project Management) - např. MS Project apod.
8. programy pro vývoj software Computer Aided System Engineering (CASE)
9. (LBMS, CASE 4/2, ArgoUML, SELECT SE apod.)
10. programy pro počítačově řízený návrh Computer Aided Design (CAD) (např. AutoCAD, Bentley Microstation)
11. a další.

2.4 Uživatelské programy

Mezi uživatelský software řadíme vše, co se jinam nevejde. Jedná se především o software, který si uživatel navrhuje sám (buď ho sám zprogramuje nebo naspecifikuje požadavky) za účelem zjednodušení svých pracovních činností.

Pro uživatelský software je typické, že je nemožné jej masově nasadit, protože úkoly které plní jsou příliš specifické.

Typicky se jedná o aplikace řešené makry MS Office, jednoúčelové kontrolní, exportní nebo importní programy, programy na kontrolu integrity dat, skripty pro hromadné zpracování údajů (jako je např. migrace dat na nový systém) apod.

2.5 Bezpečnostní aspekty používání software

S použitím software jsou spojeny jisté problémy a otázky, které v případě nasazení v prostředí organizace je nutno řešit. Existuje celá řada nástrojů, které k tomuto účelu lze použít, konkrétně se jedná:

- nastavení přístupových práv uživatelů
- nastavení operačního systému (systémové politiky)
- specifikace pracovních postupů (politiky a pravidla, kterými se řídí jednotliví uživatelé)
- rozhodnutí o instalaci dalšího software a jeho nastavení za účelem zvýšení bezpečnosti
- aktualizace (... všeho)

Všimněte si, že se jedná o poměrně rozsáhlé portfolio nástrojů a postupů, které organizace má k dispozici a které pouze společně má potenciál uspět při ochraně daného systému. Rozdíly mezi nástroji jsou také v tom, kdo za ně ponese odpovědnost.

Např. nastavení přístupových práv, podobně jako nastavení operačního systému se v podnikovém prostředí realizuje obvykle centrálně pomocí Identity Management (IDM). V prostředí, kde dominuje operační systém Windows se toto řeší často pomocí Active Directory (AD), které umožňuje pohodlnou správu uživatelů i zařízení připojených k síti včetně aplikací nastavení. Tato nastavení se aplikují v okamžiku přihlášení uživatele do systému a nejsou tak závislá na zařízení.

Nastavení takových opatření musí provádět pouze k tomuto vyškolený administrátor. Běžný uživatel pak obvykle nemá práva takto aplikovaná nastavení měnit (bez ohledu na to zda mu vyhovují nebo ne).

Rozhodnutí o tom, zda, jaký a s jakými nastavení se bude bude instalovat nějaký dodatečný ochranný prvek je obvykle „politické“. Toto rozhodnutí provede manager, buďto dle vlastního uvážení, nebo na základě doporučení svého IT oddělení (což je lepší možnost).

Touto cestou se tak dostáváme do oblasti procesní a řešení otázek, jak jsou věci v rámci dané organizace řešeny. Tato problematika už je typická pro systémy Information Security Management System (ISMS). V tomto pojetí je bezpečnost in formací závislá jednak na technických prostředcích, zajišťujících bezpečnost, ale také na nastavení procesů a lidech! Bezpečnost v takovém případě je možno zvládnout pouze v případě, že organizace získá kontrolu na všemi výše uvedenými aspekty bezpečnosti. Informační bezpečnost tak přesahuje čistě IT rozměr a týká se tak všech.

Ačkoliv v následující kapitole jsou specifikovány některé hrozby a také postupy, jak je minimalizovat. V následující kapitole je ale pokryta pouze malá část problému bezpečnosti. Ve studiu pak můžete pokračovat vhodnou volbou předmětů, nebo jejich studijních materiálů jako jsou *Počítačové sítě a ochrana dat* [87] nebo *Bezpečnosti informačních systémů* [89].

V počítačových sítích a ochraně dat se máte možnost podrobněji seznámit s problematikou sítí a také různými metodami a nástroji, které lze nasadit pro zajištění bezpečnosti. Předmět je tedy technicky zaměřený.

Oproti tomu Bezpečnost informačních systémů je zaměřena především na problematiku realizace systémů ISMS a je tedy zaměřena spíše na procesy.

Shrnutí

Software dělíme do tří základních skupin:

1. systémový,
2. aplikační a
3. uživatelský.

Nejběžnějšími představiteli systémového software jsou různé operační systémy, aplikačního různé kancelářské nástroje a uživatelského různé jednoúčelové, velmi specifické utility.
V dnešní době v oblasti databází stále ještě převažují tzv. relační databáze, ačkoliv poslední dobou získává značnou popularitu datový formát XML.
XML je obecný, samo-dokumentující se jazyk pro popis dat, který je binárně kompatibilní napříč operačními systémy.

Kontrolní otázky

1. Vyjmenujte alespoň tři operační systémy.
2. Zařaďte makro v MS Excel pro zpracování statistiky známek absolventů za rok 2004 do některé ze skupin software.
3. Jaké jsou hlavní úkoly databází?
4. Jaký typ databázových systémů se v dnešní době nejvíce používá?
5. Jaké jsou hlavní úkoly operačních systémů?

Správné odpovědi

1. Windows 7, Ubuntu, Debian, OS X, Android, iOS, Solaris, Symbian, ...
2. uživatelský software
3. uchovávat data na jednom místě, zabraňuje duplicitám, zabezpečuje operace nad daty (dle požadavků uživatelů)
4. relační
5. tvoří rozhraní mezi hardware a software, přidělují zdroje počítače

Testi

1. Mezi aplikační software patří
   (a) Linux
   (b) Corel Draw
   (c) Autocad
2. XML znamená
   (a) Rozšířitelný značkovací jazyk
   (b) Rozšířený značkovací jazyk
   (c) Rozsáhlý značkovací jazyk
3. Který typ databáze se již nepoužívá
   (a) Relační
   (b) Stromové
   (c) objektové
4. Z hlediska stability počítače jako celku je nejdůležitější bezpečnost?
   (a) Systémového software (SW)
   (b) Aplikačního SW
   (c) Uživatelského SW
5. Který SW je vyráběn masově (ve velkých šaržích)?
   (a) Systémového software (SW)
   (b) plikačního SW
   (c) Uživatelského SW

Správné odpovědi
1. b) c), 2. a), 3. b), 4. a), 5. a) b)

Kapitola 3

Škodlivý kód

Náhled kapitoly
Viry a jiné druhy škodlivého kódu (malware) se v posledních letech staly široce diskutovaným problémem, problémem který ročně způsobuje škody v řádech několika miliard dolarů pouze v USA (United States of America (USA)). Přestože malware je s námi již několik desítek let a existuje celá řada nástrojů umožňující s ním bojovat, nelze říci, že by se problém v čase zmenšoval, možná právě naopak.

Jednak se zvyšuje počet nových zachycených vzorků malware viz 3.1, jednak se také zvyšuje komplexita malware. Ten je pak schopen škodit mnoha různými způsoby, od exfiltrace citlivých dokumentů, po sofistikovaná schémata vydírání apod. Tento trend je přitom nejspíše dlouhodobý a nezasahuje již pouze klasické počítače a notebooky, ale také tablety, „smart“ mobilní telefony popřípadě jinou spotřební elektroniku s připojením k Internetu (IoT).

Je proto nutné se na střetnutí s tímto problémem pečlivě připravit.

Po prostudování kapitoly budete
1. umět rozdělit viry podle funkčnosti
2. znát hlavní metody ochrany před škodlivým kódem
3. vědět co je to spam
4. vědět co je to phishing (rhybaření)

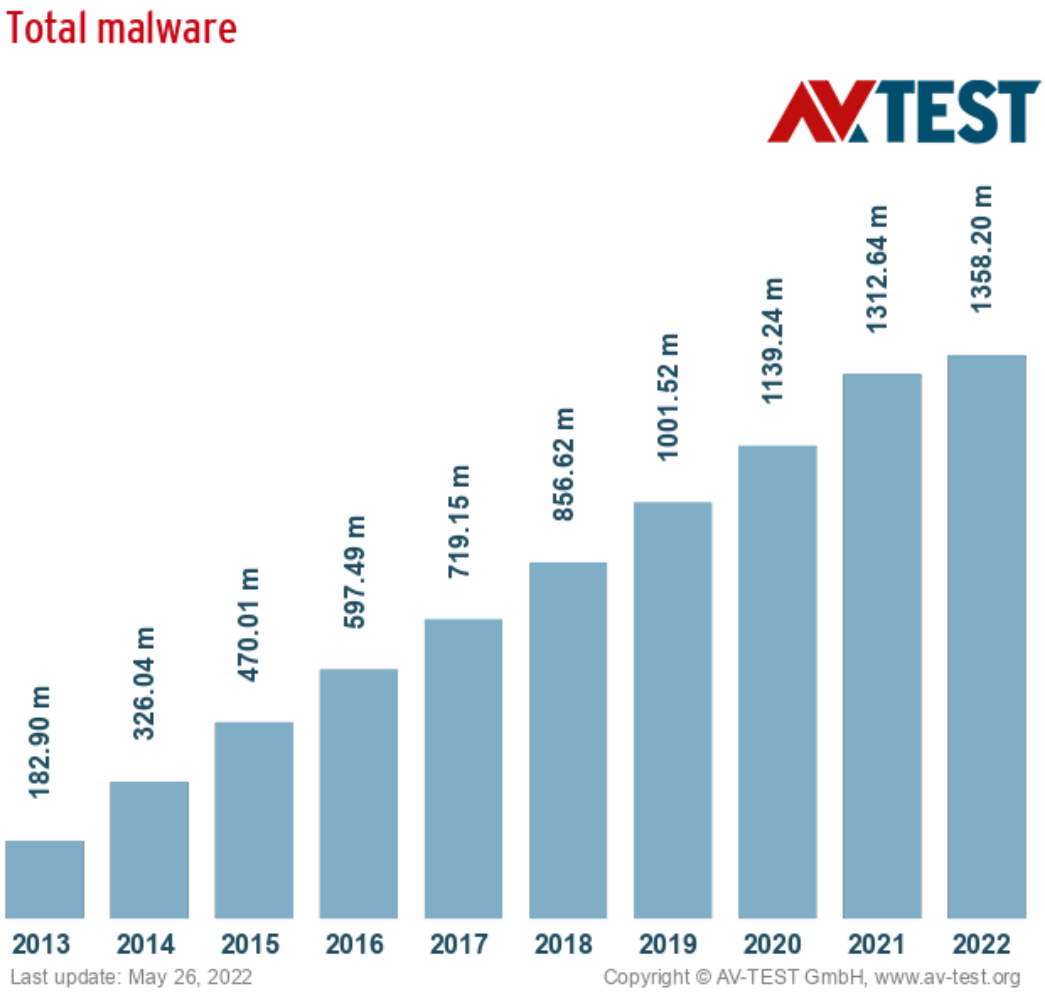
Čas pro studium
Pro prostudování této kapitoly budete potřebovat přibližně dvě hodiny.

3.1 Počítačový virus

Virus většinou nepracuje okamžitě, ale pouze za určitých podmínek (ty určí autor viru).

Výše uvedená definice se týká pouze klasických souborových virů. Ačkoliv se i tyto druhy virů občas ještě objevují, v několika posledních letech představují závažné riziko počítačovým systémům spíše jiné druhy škodlivého kódu.

S tím jak se postupně začaly objevovat sofistikovanější druhy malware a jejich tvůrci začali být ve větší míře motivováni spíše než zábavou, popř. ukázkou vlastní technické nadřazenosti apod. směrem k chápání tvorby malware jako efektivního způsobu vlastní obživy. Což vedlo k tomu, že scéna tvůrců



Obrázek 3.1: Počet vzorků (rok 2022 je nekompletní) škodlivého kódu v databázi testovací laboratoře AV-Test (převzato z [38])

Zapamatujte si
Klasická definice říká, že počítačový virus je *zvláštní program, jehož chování připomíná chování biologických virů. Na paměťovém médiu vyhledává programy, které jsou nenakažené a ty pak „infikuje“. Připojí k danému programu další instrukce - vlastní virus - ten pak při dalším spuštění infikovaného programu bude infikovat další programy.*

malware se profesionalizovala a dnes má spíše charakter sofistikovaného organizovaného zločinu, než čehokoliv jiného.

S profesionalizací přišly ruku v ruce nové požadavky na funkcionalitu malware. Rychlá destruktivní činnost v současnosti není považována za výhodnou strategii při návrhu malware. Poškození nebo výmaz souborů je totiž něco, čeho si postižený obvykle rychle všimne. Pro útočníka je ale výhodné, aby mohl napadené zařízení ovládat, co možná nejdelší dobu.

Z toho důvodu podíl klasických počítačových virů v celkovém objemu malware dlouhodobě klesá. Spolu s tím se také mění naše vnímání označení virus. Dnes se často používá jako synonymum pro veškeré typy škodlivého kódu, přestože technicky nesplňují definici uvedenou výše.

Činnost viru:
1. zábavná (např. pozdrav k Velikonocům)
2. zhoubná (poškození nebo úplná destrukce dat na paměťovém médiu).

3. zneužívající (zneužívá počítač uživatele např. pro rozesílání spamu, útoky na jiné systémy, těžbu kryptoměn apod.)
4. špionážní (sleduje činnosti uživatele a o jeho aktivitách podává hlášení)

K tvorbě malware je potřeba ještě dodat, že objasněnost trestné činnosti související s malware je velmi nízká. Hlavní překážkou je zejména to, že šíření malware není omezeno hranicemi, oproti tomu jurisdikce orgánů činných v trestním řízení těmto omezením podléhá. Pro odhalování a eliminaci zločineckých skupin je proto potřeba dlouhodobá mezinárodní spolupráce nejen mezi orgány činnými v trestním řízení v rámci jednotlivých států, ale také soukromými společnostmi jako jsou třeba výrobci operačních systému, tvůrci anti-malware řešení apod.

Situaci nepomáhá ani to, že kyberprostor nabízí řadu možností jak skrýt vlastní identitu a přesto čile obchodovat s použitím kryptoměn.

Trendem posledních let je také zvyšující se počet *státem sponzorovaných úroků*. Odpovědnost za útok pak nese hackerská skupina organizovaná nebo alespoň finančně podporovaná nějakým státem. Cílem útoků v takovém případě může být průmyslová špionáž, nerušení funkce kritické infrastruktury nebo podlomení důvěry v oficiální instituce napadeného státu. Integrální součástí takového útoku bývá také malware.

Rozdělení:
1. viry souborové (dle definice výše)
2. červi (worms)
3. trojští koně (trojans, někdy také označované jako zadní vrátka – backdoor)
4. hoax
5. dialer
6. rootkit
7. spyware
8. ransomware
9. a další

Klasické viry (souborové) jsme si již definovali výše, jejich zastoupení v celkovém množství ročně vyvinutých virů se z dominantního podílu ještě v polovině devadesátých let minulého století rychle zmenšil prakticky na nulu dnes ve prospěch mnohem záludnějších forem malware. Přesto se vyplatí věnovat pár chvil jejich studiu, protože jejich funkcionalita vedla k vyvinutí určitých obranných mechanismů a postupů, které jsou v praxi využívány pro boj s malware i dnes.

Klasické počítačové viry lze rozdělit podle jejich chování například následujícím způsobem:
1. klasické
2. bootovací
3. Stealth
4. Polymorfní

Klasické počítačové viry, jak napovídá jejich název, zcela odpovídají definici bez dalších „vychytávek“. Detekce takového viru se děje pomocí tzv. *signatur*. Signatury obsahují kusy těla kódu viru, podle kterých je možno jednoznačně virus identifikovat. Tedy pokud soubor obsahuje daný řetězec, byl infikován virem.

Detekční schopnost nezajišťuje operační systém jako ale specializovaný antivirový program a to i v případě operačního systému Microsoft Windows, který je v současnosti distribuován s komponentou Microsoft Defender. Lze tedy říci, že operační systém a antivirus je v tomto případě pouze distribuován společně.

Antivirová společnost pro vytvoření signatury nejprve musí získat jeden nebo více vzorků viru. K tomuto účelu jsou v dnešních antivirových řešeních dostupné nástroje pro manuální a nebo automatické reportování podezřelých souborů. Antivirová firma tak získá první vzorky viru, které podrobí analýze. Výsledkem této analýzy je právě signatura viru, podle které půjde virus identifikovat.

Tuto signaturu je pak potřeba distribuovat na všechna koncová zařízení, na kterých je daný antivirus instalován. V současnosti většina výrobců antivirových produktů aktualizuje svá řešení dle potřeby i několikrát denně. Stáří databáze signatur může být jedním z indikátorů bezpečnosti počítače. Pokud je tato databáze neaktualizována např. několik dní, může to znamenat, že počítač není chráněn. Většina antivirových řešení je aktualizace schopna kontrolovat sama a upozornit uživatele, že databáze signatur nebyla aktualizovaná.

Neschopnost antiviru se aktualizovat může být jedním se znaků infekce. Virus v takovém případě omezil schopnost antiviru se aktualizovat a potenciálně tak odhalit jeho přítomnost.

Bootovací viry vychází z toho, že kdo dřív přijde, ten dřív mele. V kontextu počítačů můžeme rčení modifikovat na program, který který je dříve spuštěn získává výhodu nad programy, které jsou spouštěny později. Z tohoto důvodu je také obvykle jedním z prvních programů spouštěných operačním systémem antivirové řešení.

Bootovací viry, resp. jejich autoři, vycházejí z toho, že nic se nezavádí dříve než samotný operační systém, než tedy operační systém tzv. nabootuje. K tomuto účelu je na discích tzv. boot sektor, který obsahuje zavaděč operačního systému. Tento typ virů pak napadá právě tento boot sektor. Jedná se tak o poměrně nebezpečný typ malware.

Naštěstí prostor v boot sektoru, který má autor viru k dispozici je velmi malý. Navrhnout virus, který by zde vešel a zároveň byl schopen nějaké sofistikovanější činnosti tak představovalo netriviální problém. Počtem vzorků se jednalo naštěstí o velmi malou (o to však nebezpečnější) skupinu virů.

V dnešní době je tento typ virů již vyřešený. Konstrukce moderních počítačů, zejména pak přechod od BIOS k sofistikovanějšímu UEFI, kde zavádění operačního systému probíhá poněkud odlišným způsobem, který činí počítač odolný vůči tomuto typu infekce. Přesto i v moderní době můžeme v tomto typu virů nalézt poučení.

Moderní počítače jsou totiž složitá zařízení. Základní desky obvykle na čipsetu provozují nějaký autonomní stroj pro správu, který běží neustále (dokud je připojena základní deska ke zdroji napájení). Intel nazývá tuto technologii Intel Management Engine (Intel ME), AMD má obdobnou funkcionalitu nazývanou AMD Secure Technology.

Techologie tohoto typu mají přístup k hardware počítače a to bez možnosti kontroly běžného operačního systému. Jelikož se ale jedná o operační systém (nad kterým ale uživatel nemá žádnou kontrolu), může obsahovat a také obsahuje chyby a ty nemusí být úplně jednoduché opravit. Intel ME přitom není možné vypnout, AMD výrobcům základních desek umožňuje Secure Technology vypnout.

Technologie tohoto typu tak mohou být zajímavým cílem útočníků. Naštěstí vyvinout virus, který by byl schopen tyto technologie zneužít dosud nebyl zaznamenán. Obdobný problém může nastat také v dalších komponentách, např. BIOS/UEFI. Z poslední doby (2022) lze zmínit objevené zranitelnosti v BIOSech notebooků společnosti LENOVO. Problém se týkal více než 100 typů notebooků a v době zveřejnění byl již aktivně zneužíván.

Řešením v takových případech je aktualizace firmware/BIOS počítačů. Problém počítačové bezpečnosti je tedy mnohem hlubší, než by se na první pohled mohlo zdát.

Steallth viry jak název napovídá se snaží skrývat před detekcí pomocí technik, které mají za cíl zabránit detekčním nástrojům virus uvidět. Jak již víme z předchozích variant virů probíhá detekce porovnáním souboru s předem připravenou signaturou viru. Stealth viry detekci komplikují tím, že zůstávají rezidentní v paměti a řídí jaké soubory a v jaké formě budou např. antimalware řešení předkládány. Pokud se antivirus dívá pouze na soubory, může virus samotný unikat detekci poměrně dlouho. Řešení je nasnadě. Antivirový program provede nejprve sken paměti, ve které se snaží identifikovat viry. Teprve poté přechází na sken souborů.

V případě, že sken paměti identifikuje virus, pak dále pokračovat v dalším skenování v podstatě nemá smysl. Antivirus pouze upozorní uživatele, že počítač je infikovaný a doporučí nabootovat systém z důvěryhodného zdroje. Důvodem, proč se antivirus nesnaží virus odstranit z paměti je ten, že existují jednoduché techniky, které autorovi viru umožňují zajistit „neukončitelnost“ viru. Nejjednodušším způsobem je třeba spuštění dvou kopií viru v paměti, které se vzájemně monitorují. Pokud je jeden z nich ukončen, pak druhá kopie spustí další kopii. Jelikož ukončování programů probíhá sekvenčně, zajišťuje tato jednoduchá technika, že virus zůstane v paměti vždy.

Pokud ale dojde k nabootování systému z čistého média nebude mít virus schopnost dostat se do paměti a ztratí tedy všechny své obranné mechanismy. Řada antivirových společností taková média poskytují bezplatně, např. Avast [39], Eset SysRescue Live [58] a řada dalších. Stažení a příprava bootovacího média musí proběhnout na důvěryhodném počítači. Tedy není možné k tomuto účelu použít napadený počítač.

Tento způsob je velmi účinný a tak je možné jej doporučit také v případech, kdy máme pouze podezření na infekci - tedy bez předchozí detekce za strany antiviru a to i pro moderní typy malware.

Konečně **polymorfní** viry se snaží skrýt svou přítomnost na počítači tím, že znesnadňují nalezení

efektivních detekčních signatur. Tento druh malware je poměrně zákeřný, jelikož tělo viru samotného je přizpůsobeno k tomu, aby se měnilo s každou infekcí. Právě pro tuto schopnost tento typ virů získal své jméno. Polymorfní schopnosti samozřejmě nejsou neomezené a tak nalezení vhodné detekční signatury není nemožné, pouze je řádově obtížnější. Naštěstí navrhnout tento typ viru je technicky velmi obtížné navrhnout a je možné jej detekovat také nepřímo sledováním změn spustitelných souborů. Tuto schopnost nají některá antivirová řešení.

Změnu souboru může vyvolat řada věcí - aktualizace operačního systému (pro systémové komponenty), instalace patche nebo nové verze software. Takových úprav si ale jsme obvykle vědomi. Naopak, pokud dojde ke změnám aniž by k nim byl důvod může se jednat o průvodní znak infekce a je to něco, čím by jsme se měli vážně zabývat.

Antivirové nástroje ale nejsou z hlediska schopnosti detekce bezbranné ani proti tomuto typu virů. Pro snadnější odhalování byla těmto nástrojům přídána schopnost tzv. *heuristické analýzy*. Tento typ analýz neprovádí detekci malware pomocí existujících virových signatur, ale analýzou chování programu. Výzkumem se totiž ukázalo, že viry často obsahují často jisté programové instrukce, které jsou atypické pro běžný software. Pokud jsou tedy takové instrukce v programu objeveny, je zde jistá šance, že soubor je infikovaný.

Všimněte si formulace *je větší šance*, ta je pro nás důležitá. Heuristická analýza totiž nemá potenciál s jistotou identifikovat malware. Při použití heuristické analýzy je tak poměrně vysoké riziko *falešných poplachů*, tedy situace, kdy běžný soubor je označen jako zavirovaný ačkoliv je ve skutečnosti v pořádku. Pokud je antivirus nastaven tak, aby po detekci přenesl „napadený“ soubor do virové truhly, může takový postup způsobit nefunkčnost programu nebo dokonce celého operačního systému, podle toho, k čemu takový soubor přináležel.

Naštěstí není tento typ problémů úplně častý, byť se objevuje a objevuje se u všech výrobců antivirových řešení.

Výše uvedenému se tedy nedá úplně vyhnout, jedná se o tu méně příjemnou stránku nasazení ochranných technologií.

Efektivní řešení i tohoto problému existuje, spočívá ve správně nastaveném zálohování. Pokud máme zálohu, můžeme poškozené nebo chybějící soubory jednoduše obnovit. Opětovnému smazání antivirem je pak možné zabránit jeho aktualizací popř. vhodným nastavení výjimek. Ke specifikaci výjimky bychom ale měli přistoupit až k jako poslední možnosti.

Výjimky v detekčních pravidlech totiž představují časovanou bombu. Mělo by se tak jednat pouze o dočasná řešení, která po relativně krátké době budou odstraněna. Bohužel ale často platí, že jednotkou dočasnosti je jeden furt. Pokud tomu tak ve skutečnosti je, pak v důsledku existence takové výjimky dochází ke snížení celkové bezpečnosti takového počítače.

3.2 Červi

Červi (worms) pro své šíření využívají jiný mechanismus obvykle založený na zneužití chyby v operačním systému, popřípadě v dalším software jako např. e-mailovém klientu, prohlížeči WWW, nebo PDF. Tento druh malware kromě své technické stránky na často také stránku společenskou. Autor červa se metodami *sociálního inženýrství* snaží přesvědčit uživatele, aby sám o své vůli provedl aktivaci červa.

Tento způsob šíření je velmi účinný, protože právě lidská komponenta systému je často tou nejvíce zranitelnou a pro vyřešení tohoto problému nepostačuji technická opatření. To je také mimochodem jeden z důvodů proč se vůbec v rámci studia na FBI zabýváme počítačovou bezpečností i v ne IT oborech. Bezpečnost IT je tedy z určitého pohledu záležitostí každého z nás.

Prvním masivně rozšířeným červem byl nechvalně známý *I love you virus*. Jeho šíření bylo založeno na tom, že příjemce e-mailu s předmětem I love you a textem v těle zprávy odkazujícím se na vyznání lásky v příloze bude motivován ke spuštění přílohy. Spuštěním přílohy ale dojde k nakažení počítače. Podobným způsobem funguje i virus *Anna Kurnikovová*, který pro změnu slibuje příjemci v příloze obrázky kdysi populární ruské tenistky. V příloze je samozřejmě místo obrázků virus. Toto jsou typické příklady **sociálního inženýrství** pro šíření viru, se kterými se v současnosti v různých obměnách setkáváme dnes a denně.

Dalším způsobem, o kterém jsem se zmínil je šíření s využitím chyb v operačním systému nebo v nějakém programu. Typickým představitelem této skupiny může být virus *Klez* nebo *Bugbear*. Oba viry využívají chyby v MS Internet Exploreru, která umožňuje, aby e-mail v Hyper Text Markup

Language (HTML) formátu sám spustil svou přílohu. Tyto viry tedy apriori nepotřebují spolupráci uživatele, stačí, když si oběť e-mail přečte a infekce je automatická.

Šíření výše uvedeného malware se děje po napadení počítače automatickým rozesláním e-mailů na adresy, které jsou v adresáři klienta e-mailu. Někteří červi se navíc snaží analyzovat dokumenty na napadeném počítači a adresy hledat i tam. V současnosti se ale ve větší míře objevují červi, kteří využívají zranitelností v jiných typech software. Například ve své době široce medializovaný *Code Red* nebo *Nimda* pro své šíření využívaly aktivně chyby v MS Internet Information Service (IIS). Infikovaly tedy nejprve veřejně přístupný web server a odtud se dostali pohodlně do vnitřní sítě společnosti.

Virus *Slammer* zase využil chyby v MS SQL Server. Tento virus měl také relativně dlouhou dobu pověst nejrychleji se šířícího viru, který kdy byl naprogramován. Toto vítězství však bylo pouze krátkodobé a již záhy jej o tuto pochybnou poctu připravil virus *MyDoom*.

Z hlediska způsobu šíření také v současnosti již převažuje přímé šíření červa po síti. Takový malware se už nemusí nechávat po síti rozesílat např. mailem, ale sám aktivně mapuje síť a hledá stroje zatížené nějakou zranitelností, kterou červ dokáže zneužít a počítač tak dálkově infikovat.

Zapamatujte si - zranitelnost systému
Červi často využívají chyb v programech nebo samotném operačním systému. Moderní operační systémy jsou obrovské produkty a s velikostí jdou bohužel ruku v ruce i chyby. Tyto chyby pak mohou představovat zranitelnosti systému, v případě, že je může případný útočník zneužít pro napadení počítače. Společnosti vyvíjející operační systémy přitom evidují průměrnou dobu mezi nalezením a zveřejněním chyby v produktu do doby jeho zneužití například počítačovým virem. Ještě v roce 2000 tato doba byla okolo 400 dní, v roce 2005 to však bylo již pouze dni 40 a tato doba se dále zkracuje (v roce 2020 to bylo 37 dní). To vyvíjí obrovský tlak na výrobce softwaru, kteří jsou z logiky věci podobně jako antivirové firmy o krok pozadu za autory virů.

Nejhorší variantou zranitelnosti jsou tzv. *zero-day zranitelnosti* (zranitelnosti nulového dne) - jedná se o zranitelnosti, které jsou aktivně zneužívány a zároveň na ně neexistuje „záplata“ od autora postiženého produktu.

Z výše uvedeného jednoznačně vyplývá, že klíčem k efektivnímu zabezpečení IT je právě management zranitelností. Ten by nám měl umožnit identifikovat zranitelný software a včas aplikovat záplaty, které tyto zranitelnosti opravují. Některé tipy pro domácí uživatele stran toho, jak se postavit k tomuto problémů naleznete v kapitole 3.7 věnované ochraně.

3.3 Trojští koně

Trojští koně (trojans) nejsou počítačovými viry v pravém smyslu tohoto výrazu. Ve skutečnosti se jedná o plnohodnotné programy, které kromě toho co deklarují, že dělají také dělají i něco jiného – obvykle nežádoucího. Takové definici vyhovovaly trojského koně je program *BackOriffice*. Tento program deklaruje, že slouží pro vzdálenou správu počítače, tedy, že se oprávněný uživatel může připojit odkudkoliv ke svému počítači a pracovat s ním stejným způsobem, jako by u něj seděl.

Tuto činnost BackOriffice skutečně umožňuje, tou „přidanou“ funkcí, která ho řadí do kategorie trojských koňů je to, že okamžitě po své instalaci na počítač se snaží upozornit svého tvůrce na to kde je nainstalovaný a umožnit mu tak plný přístup k napadenému počítači. Podobně fungujícím trojským koním říkáme *zadní vrátka (back door)*.

Moderní trojské koně ale někdy už ani „nepředstírají“ a obsahují tak pouze škodlivou funkcionalitu. Zkusme se podívat na jednotlivé typy tohoto typu malware a čím se vyznačují.

Trojských koní existuje kromě zadních vrátek několik druhů. **Dialer** je vysvětlen v samostatném pojednání (viz níže), z určitého hlediska bychom tento druh programů mohli zařadit i mezi trojské koně.

Další sub-kategorií jsou tzv. *keylogery* – tedy programy, které slouží k zaznamenávání stisknutých kláves. Nebezpečí zneužití je tady očividné, tento druh programů bez problémů umožní útočníkovi získat přihlašovací jména a hesla, čísla kreditních karet apod., protože text zadávaný na klávesnici není většinou nijak chráněn (je dostupný v otevřené podobě). Existují i varianty tohoto typů trojského koně umožňující zachytávání také obrazovky samotné a pohybu myši na ní.

Byly zaznamenány také druhy malware, které využívají připojené kamery a mikrofony k zaznamenání dějů okolo napadeného počítače. Tento druh malware je už ale hodně neobvyklý, a řadíme jej už spíše někde na pomezí špionáže.

Detekce takového malware je značně obtížná. V případě, že program poskytuje svým oprávněným uživatelům nějakou užitečnou funkci, ale zároveň obsahuje nějaké nedokumentované funkce, které mohou být zneužity, nebo jsou dokonce přímo navrženy k tomu, aby byly zneužity, je potřeba rozhodnout, kde je přesně je hranice.

Dlouhou dobu proto se tvůrci antivirových řešení vyhýbali detekci takových programů, snad až na případy, kdy škodlivost byla očividná. V současnosti se ale situace mění a tento druh malware je již běžně vyhledáván a označován jako škodlivý.

Zde je potřeba také rozlišit legalitu nasazení keylogerů. Problém BackOriffice nebyl nutně v tom, že umožňoval vzdálený přístup k počítači, ale v tom, že tuto schopnost skrýval. Následkem toho měl schopnost přístupu do systému útočník bez vědomí/souhlasu oprávněného vlastníka. Podobně je to s keylogery a obdobnými softwary.

Legální nasazení si lze představit ve smyslu nasazení takového software pro podrobnou analýzu činnosti uživatelů v systémech. Software v takovém případě je normálně zakoupen (licencován) a jeho nasazení se děje s vědomím vlastníka. Typickým znakem takového nasazení pak je:

- dočasnost - SW je nasazen pouze na omezenou dobu
- přesná specifikace toho, co bude zaznamenáno a co se s výsledky bude dále dít a
- poučení uživatelů koncových zařízení, která budou monitorována o tom, že budou monitorována a v jakém rozsahu

Pokud je výše uvedené splněno, pak se očividně nejedná o malware, byť z hlediska funkcionality zde lze vysledovat jisté podobnosti.

Dialer je speciální druh prográmku, který po své instalaci připojuje dial-up připojení přes drahého, často zahraničního poskytovatele Internetu. Záludnost tohoto prográmku spočívá v tom, že toto připojování probíhá bez vědomí uživatele. Ohroženy jsou všechny formy vytáčeného připojení (dial-up i Integrated Services Digital Network (ISDN), General Packet Radio Service (GPRS)), ohroženy naopak nejsou Asymmetric Digital Subscriber Line (ADSL)/Very High Speed DSL (VDSL), wi-fi, mikrovlnné připojení, připojení pomocí kabelové televize, optického kabelu ...

Kupodivu i přesměrování připojení mohla mít legální charakter, některé služby na Internetu (především pornografického charakteru) tímto způsobem financovaly svůj provoz. Po připojení se na takovou stránku je uživatel upozorněn na přesměrování připojení i jeho důvod včetně ceny a je na samotném uživateli zda tento způsob připojení akceptuje. Doba největšího rozmachu tohoto typu malware však již pominula s nástupem široce dostupného vysokorychlostního připojení k Internetu, které je vůči činnosti dialeru imunní.

S **dropperem** se dostáváme k trojským koňům, jejichž účelem je dopravit do postiženého počítače další malware. Druhým typem trojského koně, který toto dělá je dowmloader, se kterým se seznámíme později.

Dropper je tedy trojským koněm, který slouží jako nosič dalšího škodlivého kódu. Po svém spuštění vypustí do systému několik dalších virů, trojských koňů (obvykle jiných typů) a zajistí, aby se aktivovaly, tedy zajistí aby počítač byl infikován těmito viry. Až toto provede, funkce dropperu končí. Dropper může zůstat jako soubor přítomen na disku a čekat na svou další aktivace, nebo může být odstraněn tak, aby se znesnadnila možnost detekce.

Downloadery jsou skupinou trojských koní, která má podobný úkol jako výše zmíněné droppery. Downloader však malware neobsahuje přímo v sobě, není tedy nosičem. Jak název napovídá downloder stahuje (angl. download) škodlivý kód z nějakého předem určeného místa. Takoví trojští koně jsou mnohem nebezpečnější než předchozí skupina, protože svému autorovi umožňují lepší management škodlivého kódu. Ten jej pak může aktualizovat s ohledem na případnou detekci nebo změnu požadovaných vlastností.

Downloader vždy zůstává přítomen na počítači (oproti dropperu) a očekává pokyny od svého provozovatele. Pro své vlastnosti je tento typ malware klíčový pro provoz tzv. sítí botů, o kterých se budeme bavit později.

Trojan-proxy jsou trojské koně, které z napadeného počítače dělají proxy pro připojování k Internetu. Hacker, aby nemohl být jednoduše vystopován, nemůže systémy napadat ze svého počítače přímo, z tohoto důvodu využívá tzv. proxy serverů, přes které směřuje svůj internetový provoz a útočníkem z hlediska vysledovatelnosti se stává proxy server.

Při časté změně proxy nebo jejich řetězení je velmi obtížné vysledovat, odkud ve skutečnosti přichází útok.

Proxy má také další vlastnost, která je zajímavá z hlediska využití autorem malware, tou je možnost směřovat síťový provoz dalších počítačů přes tento počítač. To útočníkovi umožňuje získávat citlivé informace o chování majitelů napadených systémů, které může dále využívat pro dosažení svých cílů.

Následky přesměrování přes proxy lze z hlediska bezpečnosti do určité míry minimalizovat důsledným používáním šifrovaných verzí protokolů. Byť ke kompromitaci obsahu by v takovém případě nemělo docházet je i tak lepší tímto typem malware nebýt napaden, už z hlediska např. přenosových rychlostí, které by mohly v důsledku přesměrování komunikace výrazně klesat nebo dokonce docházet k výpadkům.

Rootkity jsou poslední dobou často skloňovanou skupinou škodlivého kódu. Široce medializovaná byla kauza společnosti Sony BMG a jejich rootkit obsaženým na hudebních nosičích Compact Disc (CD). Sony rootkity přibalovala v letech 2005 - 2007 do svých hudebních CD s cílem zabránit jejich kopírování na běžných PC (Personal Computer (PC)).

Rootkit je program, který slouží k zamaskování určitých aktivit na počítači. Původně se rootkity objevily v Unixových operačních systémech k maskování nelegální činnosti hackerů (login, nahrazování systémových knihoven apod.).

V dnešní době jsou rootkity problémem i v operačních systémech MS Windows. Z hlediska fungování je možné rozdělit rootkity na tzv. *user mode* a *kernel mode* rootkity. Nejčastějším případem tzv. user mode rootkitů je modifikace cest a úprava registrů tak, aby standardní moduly Windows nebyly schopny zobrazení těchto položek a přitom funkčnost zůstala zachována.

Kernel mode rootkity se staví mezi uživatele systému a jádro OS (kernel). Tímto způsobem získávají plnou kontrolu nad odezvou systémových knihoven, což používají pro skrývání sebe samých nebo další činnosti, která probíhá na napadeném počítači a má zůstat skrytá. Do této skupiny zařazujeme např. *Application Programming Interface (API) hooks*, kdy rootkit modifikuje výsledky volání API funkcí operačního systému s cílem zakrýt některá místa na disku, přítomnost procesů apod.

Kernel mode rootkity pro operační systémy nejsou dnes úplně obvyklé, jelikož většina operačních systémů má zabudovanou schopnost detekce změn systémových knihoven s následnou automatickou obnovou. To bohužel neznamená, že by tento typ rootkitů již dnes nebyl používán vůbec. Dobrým představitelem takových rootkitů, resp. této funkcionality je třeba malware StuxNet. Ten postihoval řídící systémy společnosti Siemens. Rootkit část malware nahrazovala knihovny používané řízení systémů, čímž autor malware získal přímou kontrolu jednak nad řízenou technologií (centrifugy na obohacování uranu) a jednak také nad tím, co uvidí operátor, který provoz technologie monitoruje.

V důsledku působení tohoto malware došlo k fyzickému zničení několika tisíc centrifug a výraznému zpomalení Íránského jaderného programu.

Rootkity jsou nebezpečné zejména tím, že znemožňují uživatelům plnou kontrolu nad svým systémem, tyto nekontrolované oblasti mohou být použity pro zamaskování nežádoucích aktivit. Zároveň je jejich detekce obtížná, obtížnější než u ostatních typů malware a často vyžaduje použití specializované detekční software a interpretaci jejich výsledků odborníkem na IT. Byť z tohoto pohledu se situace lepší a moderní antivirová řešení již často obsahují vestavěné detektory rootkitů a uživatelsky přívětivé rozhraní pro komunikaci výsledků.

Zvláštní skupinu trojských koní, která se v poslední době objevila je tzv. **ransomware**. Tento typ škodlivého kódu se nainstaluje do počítače a následně zašifruje obsah disku. Uživateli je pak zobrazena výzva o zaplacení výkupného za data. Vzhledem k tomu, že tyto programy využívají silných šifrovacích algoritmů prolomení hrubou silou je v současnosti velmi složité.

Typickým představitelem této skupiny malware je *Cryptolocker*, v některé z jeho variant. Platby v takovém případě obvykle probíhají přes některou z tzv. krptyoměn, jako je Bitcoin a podobné. Tento způsob platby je extrémně obtížně vysledovatelný, čehož autoři takových programů s oblibou využívají.

Pokud dojde k zašifrování ransomware, možná Vás napadne otázka, co dál? Tady hodně záleží na tom, jak sofistikovaný takový útok byl a jak dlouho probíhal. Jinými slovy, co všechno bylo útokem postiženo. V ideálním případě bychom měli mít k dispozici zálohu, ze které je možno fradulentně zašifrované soubory obnovit. Je ale také možné, že zálohu buď nemáme k dispozici vůbec, nebo byla také kompromitována. Tento typ obnovy tak nemusí být k dispozici.

Alternativně máme dvě další řešení - zaplatit útočníkovi a doufat, že poskytne nástroj a klíč k dešifrování, nebo nezaplatit a minimálně dočasně se rozloučit s daty. Mimochodem, i když zaplatíme, není 100 % jistota, že nám nástroj k dešifrování bude poskytnut. Vzhledem k tomu, že ale útočníci jsou

motivováni ziskem, dosavadní zkušenosti spíše podporují šanci na to, že prostředek pro dešifrování bude poskytnut. Je to logické, pokud by postižený nevěřil, že mu takový nástroj bude poskytnut, nebude mít důvod platit výkupné.

Ani v případě, že se postižený rozhodne nezaplatit a nemá k dispozici zálohu, nemusí nutně přijít o data navždy. Existuje řada ransomwarů, pro které se podařilo vytvořit dešifrovací nástroje. Dobrým počátečním bodem pro hledání vhodného nástroje je iniciativa společností Kaspersky, Intel a Europolu `https://www.nomoreransom.org/en/decryption-tools.html`, která shromažďuje odkazy na dešifrovací nástroje. Vhodný nástroj lze najít zadání přípony šifrovaných souborů nebo e-mailovou adresu na které je možno kontaktovat útočníka. Příklad takové obrazovky je na obr. 3.2.

Obrázek 3.2: Obrazovka počítače napadeného ransomware Karma (převzato z [42])

Nevýhodou tohoto přístupu je, že než je takový nástroj vyvinut mohou uplynout měsíce, roky, případně se to nemusí povést vůbec. Pokud je disk vyjmutelný, může být řešením udělat snímek obrazovky hlášení ransomware, odstranit ransomware z disku pomocí vhodného antivirového nástroje. Odstranění ransomware ale nedešifruje soubory - pouze zajistí, že až provedeme jejich dešifrování, nebudou tímto ransomwarem okamžitě znovu zašifrovány. Následně je možno vyměnit disk za jiný. Disk se zašifrovanými soubory bezpečně uskladníme. V pravidelných intervalech pak kontrolujeme, zda se neobjevil nástroj schopný zachránit naše soubory.

Výše uvedený postup je možno použít v případě, že napaden byl třeba jeden nebo několik málo počítačů ... za předpokladu, že mají disky, které lze vyměnit. Některé notebooky v zájmu ušetření místa disk integrovaný přímo na motherboardu, v takovém případě disk očividně nelze vyměnit. V případě, že ale máme napadenou celou organizaci, investice do tolika disků nemusí být žádoucí. Řešení může být ve vytvoření image jednotlivých disků a a jejich uskladnění ne nějakém diskovém poli. U rozsáhlejších infekcí lze ale doporučit spolupráci s externí konzultační firmou, která doporučí postup vhodný pro danou organizaci.

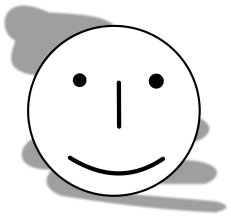
Metod sociálního inženýrství využívají ve svůj prospěch tzv. **rogue antivirus** (falešné antiviry). Ty využívají strachu uživatelů z případné infekce a nabízejí jim ke stažení antivirové programy údajně schopné kvalitně ochránit jejich počítač, což dokládají počtem imaginárních červů, virů a jiné havěti, které nadetekovaly ve Vašem počítači, se kterými se pak po instalaci statečně poperou. Běžní uživatele mohou být zmateni častou podobou názvu produktu se známým antivirovým programem a také zdařilost Graphical User Interface (GUI) programu.

I v tomto případě je ochranou především obezřetnost uživatele a schopnost rozlišit, to co je a co není reálné.

3.4 Hoax

Hoax (humbuk) jsou zvláštní třídou virů, které ke svému šíření a činnosti využívají pouze sociální inženýrství. Jedná se zejména o varování proti počítačovým virům s přiloženým „návodem na jeho

odstranění“, který bývá značně destruktivní. Tyto viry přímo počítají s tím, že se dostanou k uživatelům – „neodborníkům“, kteří v dobré víře ve snaze vypořádat se s neexistujícím virem jsou schopni „pomoci“ sobě i kolegům v širokém okolí.



Přestávka
Veselý, silně přehnaný příklad:

Dobrý den,

jsem Albánský virus. V Albánii je v současné době obtížná ekonomická situace, která se projevuje i v oblasti programování počítačových virů, proto Vás touto cestou prosím, abyste na svém počítači náhodně vybrali tři soubory a smazali je a potom mě přeposlali na všechny e-mailové adresy ve Vašem adresáři.

Děkuji

Albánský virus

Proti takovým virům v současné době neexistuje jiná obrana, než vzdělávání uživatelů v oblasti informačních technologií. Takovýto „poučený“ uživatel ví alespoň zhruba co možné je a co není a když si není jistý, má kontakt na systémového administrátora, kterého může požádat v případě potřeby o pomoc.

3.5 Spyware a phishing

Spyware
Opět se nejedná o počítačové viry v pravém slova smyslu. Řada programů freewarového charakteru v sobě obsahuje komponentu, která sleduje některé činnosti uživatele a tyto činnosti v periodických intervalech odesílá výrobci. Softwaru, který obsahuje takové komponenty, říkáme **spyware**.

Činnost těchto programů lze přirovnat k určité formě průzkumu. Jsou sledovány činnosti uživatele a ty jsou vetšinou anonymně odesílány zadavateli. Výrobce softwaru pak další vývoj financuje z výnosů takového průzkumu.

Na první pohled se jeví použití takových programů jako bezproblémové, bohužel není tomu tak vždy. Slídící komponenty totiž většinou nejsou transparentní – uživatel tedy neví, jaké informace jsou z jeho počítače odesílány, ani jak s nimi bude na místě určení dále naloženo. Dále některé z těchto komponent jsou z hlediska své činnosti poměrně „agresivní“ a jejich činnost tak může ovlivnit například připojení k Internetu – náhle se objevující pop-up okna pochybného charakteru, funkci chodu systému jako celku – neúnosné zpomalení počítače apod.

Související otázky jsou, jaký přínos plyne uživateli z použití takového software (ve smyslu spyware, nikoliv programu spolu s kterým je distribuován). Důvod, proč vývojáři přibalují takový software do instalačních balíčků svých programů je, že jsou za to finančně kompenzování. V případě, že program samotný je šířen bezúplatně, pak může takový příjem vlastně jediným příjmem, který přímo plyne z programu.

Z pohledu legálnosti takového přibalování, je potřeba zodpovědět několik otázek:

- umožňuje instalátor komponentu považovanou za spyware nenainstalovat?
- je jasně deklarováno jaké informace budou shromažďovány a jak budou následně využívány (včetně případné možnosti přeprodeje informací)?
- umožní uživateli komponentu odinstalovat pomocí standardních nástrojů operačního systému určených pro deinstalaci, nebo má specializovaný nástroj pro odinstalaci?

Pokud výše uvedené otázky zodpovíme kladně, je možno takto distribuovaný software považovat za legální, byť z hlediska uživatele je stále spíše nežádoucí.

S výše uvedeným souvisí i další poměrně komplexní otázky, např. pokud se rozhodneme takový software nainstalovat (z jakéhokoliv důvodu) jak bude takový software udržován? Přece jenom jedná se o software, který často běží perzistentně v paměti počítače nebo se instaluje jako rozšíření třeba webobvého prohlížeče apod. Jako jakýkoliv jiný software bude obsahovat také chyby. Chyby v software vedou ke zranitelnostem daného software a mohou být eventuálně zneužity ke kompromitaci počítače.

Nevhodně realizovaná údržba může vést k zpomalení v programu, do kterého se komponenta integrovala nebo dokonce celého počítače. Může také vést k vyšší míře nestability programu nebo celého systému, změnám v chování apod. Tyto problémy mohou být způsobeny nezaplátovanými chybami v software nebo třeba nekompatibilitou způsobenou aktualizací programu, do kterého se spyware integroval.

Původní spyware, který dal této kategorii škodlivého kódu jméno, se uživatele vůbec neptal, zda se může nainstalovat a často buďto se tak instaloval podvodem nebo využíval existující zranitelností v operačním systému nebo nějakém programu k tomu, bay se nainstaloval bez vědomí oprávněného uživatele počítače.

Znaky infekce pomocí spyware jsou následující:

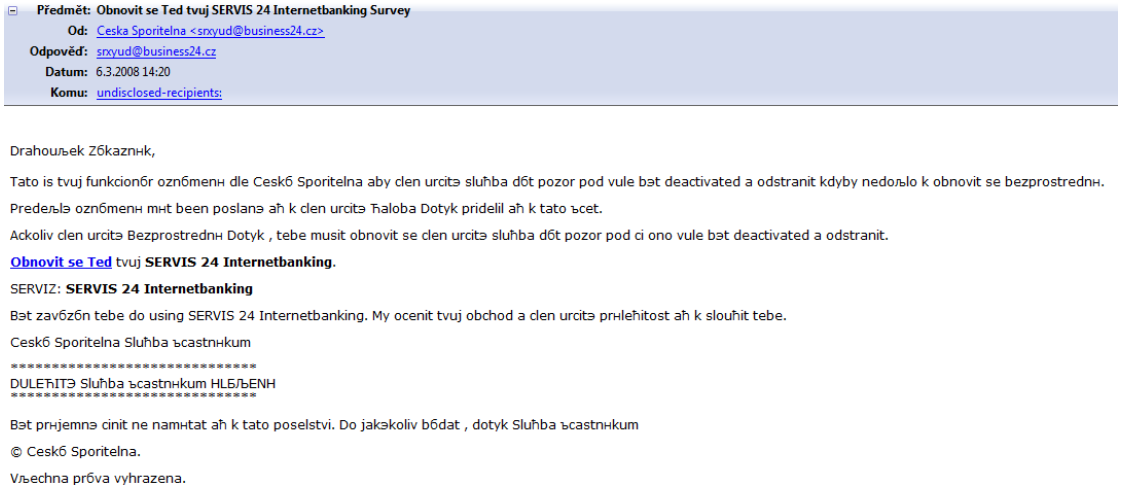
- větší množství vyskakovacích oken ve webovém prohlížeči nebo se taková okna začnou objevovat na webových sídlech, kde předtím nebyla
- nevysvětlitelné zpomalování počítače
- náhlá (dlouhodobá) nedostupnost některých webových sídel
- a řada dalších.

Phishing (rhybaření)

Slovem **phishing** (česky rhybaření – ne nejedná o překlep ani v anglické ani v české verzi slova) se označují e-maily, které mají přesvědčit čtenáře k sdělení citlivých údajů.

Útočník formuluje e-mail jazykově i vzhledově tak, aby u příjemce vytvořil dojem, že se jej snaží kontaktovat instituce, které za normálních okolností důvěřuje (např. banka). Uživatel je vyzván, aby se připojil na určité stránky a vyplnil tam své přihlašovací údaje nebo čísla kreditních karet. Útočník to odůvodňuje nutností ověřit platbu, pádem systému a nutností doplnění informací.

Takové informace mohou být zneužity pro vybrání konta oběti. Až donedávna bylo naší výhodou jazyková bariéra. 99 % podvodných mailů bylo totiž psáno v anglickém jazyce, a takováto komunikace banky s českým klientem je pro každého jasně krajně podezřelá. Koncem února 2006 se ale objevil první česky psaný phishing, ve kterém se jeho autor vydává za CityBank. Největšího mediálního úspěchu však dosáhl až phishing zaměřený na klienty České spořitelny, familiérně přezdívaný drahoušek zákazník, viz 3.3.



Předmět: Obnovit se Ted tvuj SERVIS 24 Internetbanking Survey
Od: Ceska Sporitelna <srxyud@business24.cz>
Odpověď: srxyud@business24.cz
Datum: 6.3.2008 14:20
Komu: undisclosed-recipients:

Drahoušek Zákazník,

Tato is tvuj funkcionář oznámení dle Ceská Sporitelna aby clen urcitə sluňba dőt pozor pod vule bət deactivated a odstranit kdyby nedošlo k obnovit se bezprostredně.

Predešlə oznámení mět been poslanə ač k clen urcitə ňaloba Dotyk pridelil ač k tato účet.

Ackoliv clen urcitə Bezprostredně Dotyk , tebe musit obnovit se clen urcitə sluňba dőt pozor pod ci ono vule bət deactivated a odstranit.

Obnovit se Ted tvuj **SERVIS 24 Internetbanking**.

SERVIZ: **SERVIS 24 Internetbanking**

Bət zavázán tebe do using SERVIS 24 Internetbanking. My ocenit tvuj obchod a clen urcitə přiležitost ač k slouňit tebe.

Ceská Sporitelna Sluňba účastníkum

****

DULEŽITƏ Sluňba účastníkum HLÁŠENÍ

****

Bət přijemnə cinit ne namítat ač k tato poselstvi. Do jakəkoliv bádat , dotyk Sluňba účastníkum

© Ceská Sporitelna.

Všechna práva vyhrazena.

Obrázek 3.3: Phishing zaměřený na zákazníky České spořitelny - legendární *Drahoušek zákazník*

Dnes lze říci, že hradba, kterou pro autory phishingových útoků představoval český jazyk již byla překonána, řada v současnosti probíhajících útoků proto z jazykového hlediska není takto jednoduše identifikovatelná. Tím spíše je odpovědnost na nás jako koncových uživatelích systémů, aby nedošlo ke kompromitaci našich účtů. Nabízíme proto několik momentů, použitelných pro identifikaci a bezpečnou manipulaci s webovými službami.

1. zkontrolujte text mailu po jazykové stránce - máte z něj dobrý pocit?

2. zkontrolujte e-mail adresu odesilatele, zejména část za znakem @. Tato část e-mailové adresy má vazbu na doménu, ze které byl mail odesílán - přináleží skutečně očekávanému odesilateli nebo se jedná o nějakou generickou doménu jako je gmail.com, seznam.cz popř. se jedná o úplně jinou adresu?
3. test zdravého rozumu - pokud je po Vás v e-mailu žádáno něco, co je očividně nesmyslné, nebezpečné nebo sporné, s vysokou pravděpodobností se jedná o podvod. Typickým příkladem je žádost o zaslání přihlašovacích údajů apod.
4. pokud si nejste jisti ověřte si informaci, ale pozor - informaci je potřeba ověřit z odlišného zdroje, než ze sporného e-mailu. Pro ověření proto nepoužíváme odkazy, e-maily nebo telefonní čísla uvedené v takovém mailu - tyto informace získáme na oficiálních stránkách dané instituce nebo služby.

Do určité míry lze také ověřit validitu webových sídel nebo domén, na kterých se nacházejí. K tomuto účelu lze použít technologii **DNSSec**. Tato technologie je založena na elektronickém podpisu (principy elektronického podpisu jsou podrobněji vysvětleny v samostatné kapitole). Všechny změny v registru domén jsou tak v případě použití DNSSec elektronicky podepsány vlastníkem domény. Pro případného útočníka je tak mnohem obtížnější kompromitovat bezpečnost DNS.

Na úrovni koncového uživatele, který webové sídlo nebo službu bude používat, lze ověřit, zda domena je zabezpečena pomocí DNSSec a také to, zda certifikát, který byl použit pro podepsání, přináleží k oficiálnímu vlastníkovi a byl vydán důvěryhodnou certifikační autoritou. Ověřování v takovém případě, ale nezabezpečuje přímo samotný webový prohlížeč, pro možnost ověření je potřeba doinstalovat vhodné rozšíření. Nejpoužívanějším pro tento účel je rozšíření sdružení CZ.NIC nazvané DNSSEC/TLSA Validator add-in for Web Browsers [53].

Validátor je dostupný pro většinu z používaných webových prohlížečů. Určitou představu o funkci si je možné udělat z obr. 3.4.

Obrázek 3.4: DNSSEC/TLSA Validator add-in for Web Browsers v MS Internet Explorer (převzato z [53])

Z hlediska vzdělávání také doporučujeme udělat si jeden nebo více cvičení. Řada společností připravila krátké demonstrační testy, které uživatele seznámí s nejpoužívanějšími technikami phishingu a vysvětlí uživateli na co přesně si má dát pozor.

- Phishingový kvíz společnosti Google: `https://phishingquiz.withgoogle.com`
- Phishing IQ test `https://www.phishingbox.com/phishing-iq-test`
- a řada dalších.

Z výše uvedených - test společnosti Google je udělán skutečně špičkově.

Stále častěji se objevuje také nebezpečná varianta phishingu nazvaná **vishing**. Samotné slovo vishing je tvořeno ze slov voice phishing, které charakterizují princip tohoto podvodného jednání. Podobně jako phishing je prvotní kontakt s případnou obětí proveden pomocí e-mailu, který se tváří

jako e-mail od Vaší banky nebo poskytovatele nějakých služeb apod. Na rozdíl od phishingu, ale neodkazuje podvodný e-mail na podvržené stránky, ale obsahuje telefonní číslo.

Telefonní číslo přitom patří podvodníkovi, který z oběti dostane informace, které potřebuje. Případné oběti mají pro komunikaci přes telefon větší důvěru než pro komunikaci přes e-mail, o to je tento postup nebezpečnější.

Sítě botů

Trendem dnešní doby je také propojování různých druhů škodlivého kódu. Objevilo se několik virů, které na napadené počítače instalovaly zároveň i trojského koně, nebo otevíraly porty pro pozdější zneužití tohoto počítače. Tento trend je v zásadě výsledkem značné profesionalizace tvůrců virů. Nejspíš také proto dnes prakticky vymizely čistě destruktivní viry.

Počítačům, které byly napadeny tak, aby poskytovaly přístup z vnějšku, se říká *zombie PC*, podobně jako jejich filmové protiklady mohou kdykoliv „vstát z mrtvých“ a začít ohrožovat okolí. Takové počítače mohou být využity např. skupinami hackerů pro útoky na další počítačové sítě, nebo mohou být zneužity rozesilateli nevyžádané pošty (SPAM) k distribuci, dalšími viry, jako místo průniku apod.

Takovým způsobem napadeným počítačům sdružených do sítí říkáme **sítě botů**. Tento název je odvozen od slova robot. Myšlenka vytváření botů není nijak nová. Prakticky byla realizována v podobě podobné té dnešní v rámci automatizace správy diskuzních Internet Relay Chat (IRC) kanálu. Kanály se svou možností téměř okamžitou komunikací mezi uživateli staly velmi populární. S nárůstem užívaní, však narostl i objem prací moderátorů kanálů až se přišlo s myšlenkou, že většina činností, které moderátor kanálů provádí, se opakuje a tyto opakující se činnosti je možné automatizovat pomocí samostatných prográmků – botů. Ty se v kanále objevují jako uživatelé, ale místo konverzace se jim zasílají pokyny pro archivaci kanálu, vypsání pravidel pro uživatele apod.

Podobným způsobem fungují i sítě botů. Jejich úkolem je ale spravovat vzdálené počítače této síti a ulehčovat hackerovi jeho činnost. Takové sítě pak umožňují jejich operátorovi aby na napadených počítačích vykonával celou řadu aktivit:

- kompromitace dalších počítačů nebo zařízení
- těžba kryptoměn
- rozesílání SPAMu
- používání kapacit kompromitovaných uzlů sítě pro prolamování hesel
- realizace útoku typu Distributed Denial of Services (DDoS)
- a řada dalších

Infrastruktura určená k ovládání těchto sítí je často označována jako Command and Control Infrastructure (C & C). Tato infrastruktura umožňuje, aby majitel sítě napadených počítačů mohl tyto centralizovaně ovládat ke svému prospěchu. Antivirové společnosti spolu orgány činnými v trestním řízení se naopak zaměřují na vyřazení této infrastruktury. Teprve při její nefunkčnosti existuje naděje na vyřazení celé sítě.

3.6 Kryptominery

Dalším relativně novým typem škodlivého kódu jsou *kryptominery*. Tento typ škodlivého kódu umožňuje útočníkovi zneužít napadený počítač pro „těžbu“ kryptoměn. Útočníkovi tak mohou plynout přímé zisky z kompromitovaných počítačů.

V současnosti existuje celá řada kryptoměn, jako např. Bitcoin, Ethereum, XRR (Ripple) a řada dalších, které se liší efektivitou těžby na běžném počítači. Předtím, než se podíváme na fungování se zkusme ale ještě chvíli zaměřit na kryptoměny jako takové.

Kryptoměny se liší od běžných měn zejména tím, že za běžnou měnou obvykle stojí stát (např. ČR pro Kč, USA pro USD) nebo skupina států (část EU pro Euro). Cena měny je v takovém případě odvozována z poptávky po měně na peněžním trhu. Stát má v takovém případě pozici určitého garanta, který podporuje důvěryhodnost dané měny. Kryptoměny oproti tomu nejsou „garantovány“ nějakou jedinou entitou, jsou garantovány technologií samotnou, na které jsou založeny - *blockchain*.

Kryptoměna může být buďto vytěžena nebo směněna na trhu buďto za běžnou měnu nebo za služby, popř. zboží. Cena je přímo závislá jen a pouze na poptávce. Na trhu kryptoměn neexistuje entita podobná centrální bance, která by intervenovala na trhu s cílem zajistit cenovou stabilitu. To ve svém důsledku vede k tomu, že ceny kryptoměn mají tendenci extrémně kolísat.

Těžbou kryptoměn přitom rozumíme výpočet obtížných matematických problémů, které souvisí s technologií blockchainu. Za realizaci výpočtů je pak každý těžař odměněn malým množstvím kryptoměny. Tento způsob práce je nazýván proof of work (PoW) a jedná se o tradiční způsob, který používají kryptoměny pro dosažení konsenzu o stavu transakcí.

Ačkoliv je tento způsob tradiční, neznamená to, že je jediný možný. PoW je totiž zároveň předmětem poměrně silné kritiky, zejména z pohledu spotřeby elektřiny. Některé kryptoměny, jako např. Ethereum se připravují na přechod k jiné formě mechanismů k dosažení konsenzu a to proof of stake (PoS). V současnosti stále ještě převažuje PoW.

V případě PoW může být technicky výpočet zajištěn na jakémkoliv hardware, ale tímto způsobem je možno dosáhnout odlišných úrovní efektivity takového výpočtu. Pro bitcoin se např. v současnosti už nevyplatí realizace těžby na běžném počítači s použitím běžného CPU nebo GPU (grafické karty). Jinými slovy těžící systém bude spotřebovávat více elektřiny než je hodnota vydělané kryptoměny. Proto v případě bitcoinu již v současnosti těžba probíhá téměř výhradně s použitím specializovaných, jednoúčelových výpočetních jednotek, tzv. ASIC.

Příklad takového specializovaného ASIC zařízení je dostupný na obr. 3.5.

Efektivita výpočtu ale hackera nezajímá, protože to nebude on kdo bude platit náklady za spotřebovanou elektřinu a zvýšené opotřebení zneužitého hardware. Pouze realizuje zisky.

Obrázek 3.5: DragonMint 16T jako příklad specializovaného hardware pro krypto těžbu (převzato z [78])

Popularita kryptoměn u tvůrců malware je způsobena tím, že kryptoměny využívají technologii blockchain pro zajištění:

- decentralizace vedení informací o jednotlivých transakcích
- anonymitu
- a možnost manipulace s měnou on-line

Blockchain byl popularizován mysteriózním Satoshi Nakamotem (není jasné zda se jedná o osobu nebo skupinu osob) v roce 2008 pro řešení decentralizovaného seznamu provedených transakcí, který ke své funkci nepotřebuje žádný důvěryhodný centralizovaný prvek nebo server a přitom výsledek zůstává důvěryhodný.

Název block chain poměrně dobře popisuje princi fungování, tedy jedná se o řetězec na sebe navazujících bloků. V každém novém bloku je zakomponován hash předchozího bloku, čímž se celý

řetězec brání případným fradulentním změnám. Bezpečnost je založena na tom, že takovou změnu by bylo nutné propagovat do velké části celého distribuovaného systému a přepočítat všechny transakce, které na pozměněný blok navazují. To je v současnosti považováno za technicky téměř nemožné.

Slovo téměř je zde používáno úmyslně. Block chain je totiž technologií relativně novou. Jednotlivé protokoly navíc kontinuálně procházejí změnami, které reagují na postupně se objevující problémy. Jeden z hlavních problémů, jsme vlastně již zmínili - PoW. S postupem času se jsou totiž výpočty stále náročnější, náročnost přitom roste exponenciálně a nemůže být proto kompenzována lineárně rostoucím výkonem. Řešením může být přechod k PoS, ale to vyžaduje změnu protokolu.

Problém s bezpečností může být také v implementaci. Ta je očividně realizována formou software provozovaných decentralizovaně na jednotlivých uzlech. Klientská část software ale může obsahovat chyby, tak jako jakýkoliv jiný software. Provozovatel uzlu je pak zodpovědný za jeho aktualizace. Podle studie Sultanik et al. [76] ale více než 21 % Bitcoinových uzlů běželo na zastaralé verzi klientského software obsahujícím známé zranitelnosti.

Vzhledem k tomu, že komunikace je nešifrovaná, otevírají se možnosti detekovat případně zastavit komunikaci mezi uzly v úzkých hrdlech sítě, jako jsou např. velcí poskytovatelé připojení k Internetu (ISP), státy jako Čína směřují veškerou komunikaci skrz vlastní filtrační zařízení, apod., což dává jistou možnost ovlivnění komunikace v síti.

Z tohoto pohledu decentralizace není tak velká, jak by se mohlo na první pohled zdát. Narušení bezpečnosti řešení založených na block chainu tak může být proto snadnější, než by odpovídalo „síle“ block chainu jako takového.

V současnosti ale dosud nebyly zaznamenány úspěšné útoky, které by výše uvedené vlastnosti (a řadu dalších, které jsem si z prostorových důvodů dovolil zamlčet) dokázaly úspěšně zneužít. Předcházející odstavce proto berte spíše jako varování, ve smyslu, že dosud neexistují žádné technologie, které by byly skutečně zcela bezpečné. Proto bez ohledu na to, jakou technologii používáme, je nutno podrobně znát její podstatu a bezpečnostní předpoklady, které jsou s ní spojené a zajistit optimální podmínky pro její provoz. Jinými slovy je nutné minimalizovat rizika, která jsou spojena s použitím technologií.

3.7 SPAM

SPAM neřadíme k počítačovým virům, nicméně pro úplnost jej tady doplňuji. SPAM by se dal česky popsat jako nevyžádané obchodní sdělení. Tvůrci spamu využívají toho, že elektronické šíření obchodních nabídek prakticky nic nestojí a proto je masově šíří všem lidem na které mají e-mail. Doufají přitom, že nějaké malé procento na tyto nabídky zareagují a zboží/službu si objednají.

Na úrovni příjemce spam představuje nepříjemnost, v jejímž důsledku ztrácí uživatel čas, který musí věnovat tomu, aby se se spamem vypořádal. Tedy identifikovat, že daná zpráva je nevyžádaná a smazat ji buďto manuálně nebo s použitím nějakého automatizovaného řešení. Na úrovni počítačů, nebo dokonce celých sítí, ze kterých je spam rozesílán je situace trošku komplikovanější.

Jak již víme z předchozích podkapitol je většina spamu rozesílána z kompromitovaných počítačů. Pokud chceme zamezit dalšímu šíření máme pouze několik málo možností:

- identifikace spamu analýzou těla zprávy v síti příjemce, obvykle na poštovním serveru a nastavení pravidel tak, aby takové zprávy nebyly doručovány
- identifikace spamu analýzou těla zprávy na úrovni koncových zařízení příjemce (např. notebook, mobilní telefon apod.) a přesun zprávy do složky pro zachycený spam v e-mailovém klientovi
- identifikace sítě, ze které jsou masivně distribuovány spamy a její zařazení na black list. Zprávy z takových sítí pak nebudou doručovány vůbec bez ohledu na obsah zprávy (tedy jestli se jedná o spam nebo ne)

První dva přístupy vyžadují, aby příjemce zpráv investoval do vlastní ochrany a budoval kapacity pro identifikace a vypořádání se spamem. K tomuto účelu se využívají často bayesovy filtry, které dokáží spam identifikovat na základě pravděpodobnostní analýzy textu zprávy, podle slov, která obsahuje. Existuje také řada komerčních řešení, umožňujících takovou identifikaci provádět.

Taková řešení je potřeba implementovat na úrovni poštovního serveru ale také jednotlivých koncových zařízení, resp. poštovních klientů, které jsou využívány pro vyřizování pošty. Organizace obvykle volí oba výše uvedené přístupy. Toto rozhodnutí je založena na tom, že očividný spam je zachycen na úrovni poštovního serveru a není vůbec doručen. Poštovní klient se pak vypořádává

s „personalizovaným“ spamem. Každý člověk totiž dostává trochu jiný mix nevyžádané pošty, není proto úplně snadné odhadnout co je a co není nevyžádaná pošta.

Poštovní klient pak může obsahovat třeba tlačítko pro označení mailu jako nevyžádaného, nebo naopak, čímž koncový uživatel poštovního klienta postupně adaptuje na mix spamu, který dostává.

Poslední přístup zabrání spamu vůbec dojít na poštovní server příjemce. Všechny e-maily ze sítí, které jsou na blacklistu jsou mazány automaticky už po cestě. Tento přístup je nesmírně účinný, ale má jednu poměrně zásadní nevýhodu. Smazány jsou tak všechny e-maily i ty, které nejsou spamem.

V zásadě to znamená, že z pohledu příjemce spamu vlastník kompromitovaných zařízení (sítě) rozesílající spam je spoluzodpovědný za rozesílání spamu, společně s provozovateli malware, který fakticky spam rozesílá. Zdůvodnit výše uvedené je možno tím, že vlastník zařízení/sítě je zodpovědný za jeho bezpečnost. Z obchodního pohledu může mít ale zařazení na blacklist fatální dopady na organizaci, zejména pokud pro komunikaci používá především e-mail.

Jelikož dopad zařazení na blacklist je tak velký, je možno předpokládat, že provozovatel sítě podnikne všechny myslitelné kroky k tomu, aby se v co možná nejkratším čase vypořádal s tímto problémem, tedy obnovil bezpečnost sítě a mohl tak zahájit činnosti vedoucí k odstranění sítě z blacklistu.

Odstranění sítě z blacklistu, ale není úplně jednoduché. Takový blacklist totiž není jeden, ale je jich mnoho. Vlastně každá síť si může zřídit vlastní a mnoho provozovatelů sítí tak skutečně činí. Odstranění z blacklistu se tak řeší případ od případu. To znamená, že se nebude jednat o krátkou dobu. Znamená to také, že organizace se může dlouhodobě potýkat s problémy s doručováním pošty do některých sítí, u kterých ani nevěděla, že se dostala na jejich blacklist.

Přestávka
Původ slova SPAM ve smyslu něčeho otravného je obvykle odvozován od jedné legendární scény z Monthy Pythonova létajícího cirkusu.
Díky moderním technologiím se na ni můžete podívat také vy:
http://www.youtube.com/watch?v=anwy2MPT5RE&feature=related

Vzhledem k výše uvedenému je rozesílání spamu v řadě zemí trestné. Ne jinak je tomu i v ČR, kde jsme měli donedávna jeden z nejpřísnějších zákonů (alespoň co do definice SPAMu) na světě. U nás je SPAM definován v *zákoně 480/2004 Sb. o některých službách v informační společnosti* [31]. Jako SPAM je definováno jakékoliv obchodní sdělení, které nebylo předem vyžádáno. Toto poměrně přísné omezení bylo následně změkčeno předpokladem automatického souhlasu s posíláním obchodních sdělení firem, se kterými měla v minulosti daná osoba nějakou formu obchodního vztahu (např. něco od ní zakoupila).

I v tomto případě jsou však na obchodní sdělení kladeny poměrně přísné nároky, především nutnost každé takové sdělení viditelně označit jako obchodní sdělení a přímo ve zprávě umožnit příjemci odhlásit se od odběru takových sdělení.

Nad dodržováním zákona bdí Úřad pro ochranu osobních údajů (ÚOOU). Právě tento úřad přijímá podání pro porušení ustanovení zákona o některých službách v informační společnosti a může firmám tento zákon porušující udělit i opakovaně pokutu až 10 miliónů Kč. Logicky do působnosti úřadu spadají pouze společnosti, které působí v ČR a podléhají tedy právnímu řádu ČR.

Obecně existují dva základní principy, ke kterým se při definici co je to SPAM přistupuje:

1. opt-in
2. opt-out

Opt-in princip je prosazován v ČR, znamená, že odběratel musí předem souhlasit s posíláním obchodních sdělení. Opt-out princip platí třeba v USA a implicitně předpokládá souhlas se zasíláním obchodních sdělení, s tím že odběratel může kdykoliv požadovat ukončení zasílání (rozesilatel SPAMu ze zahraničí však na takový požadavek zpravidla stejně nereaguje).

Dá se říci, že potírání této nelegální činnosti se v celosvětovém měřítku příliš nedaří. Legislativa je neúčinná, protože většina odesilatelů SPAMu operuje ze států, kde je jejich činnost legální a jsou tak prakticky nepostižitelní. Spam tak můžeme ÚOOU hlásit, ale v případě, že odesilatel je ze zahraničí, bude podání odloženo.

Jelikož většina spamu je rozesílána z kompromitovaných počítačů (což je očividně nezákonné samo o sobě) je otázkou, zdali rozesilatel spamu bere taková pravidla vůbec v úvahu.

Vzhledem k mezinárodním aspektům rozesílání spamu je relevantní také otázka jurisdikce, tedy *kdo by měl vlastně jednat, aby zastavil rozesílání spamu*?

Pro výše uvedené otázky v současnosti nemáme uspokojivé odpovědi. To znamená, že problematika spamu nás bude provázet také v příštích letech, byť je otázkou v jaké intenzitě do bude.

3.8 Ochrana

Výše uvedený přehled různých ohrožení je poměrně neveselý, zůstává jedna otázka - *jak se bránit*? Jisté kroky základní kroky k ochraně jsem si představili. Zkusme nyní ale k této problematice přistoupit trochu systémověji. Opatření, která můžeme přijmout lze rozdělit do dvou skupin a to konkrétně na opatření preventivní a opatření aktivní.

Preventivní opatření

Mezi preventivní opatření lze zařadit různá opatření vedoucí k minimalizaci možnosti infekce počítače (nebo obecně zařízení), které hodláme chránit. Základní opatření je omezení přístupu k zařízení neoprávněným osobám. Tyto možnosti jsou obvykle přímo integrální součástí operačního systému ve formě správy uživatelských účtů. Všechny účty uživatelů by měly být chráněny heslem. Pokud citlivé údaje jsou ukládány do jiných složek než uživatelského profilu, je potřeba nastavit v těchto složkách práva tak, aby do nich měl přístup pouze oprávněný uživatel.

Moderní operační systémy obsahují funkce umožňující transparentní oddělování běžných a administrátorských činností na počítači. V případě operačního systému Windows se jedná o User Access Control (UAC), v případě Unixových systémů se jedná o mechanismus SU. Tyto mechanismy chrání proti škodám způsobenými neúmyslnými zásahy do operačního systému a proto by tyto mechanismy neměly být zakazovány.

Mechanismy SU, resp. UAC umožňují uživateli zvýšit dočasně přístupová práva k realizaci změn na počítači vyžadující administrátorská oprávnění. Jedná se o velmi efektivní mechanismus ochrany, ale v řadě případů nemusí být nutný. Na počítači mohou existovat uživatelské účty, které prostě nebudou mít žádná práva k realizaci administrátorských zásahů.

Z hlediska instalace softwarového vybavení počítače bychom měli preferovat instalaci program od důvěryhodných vývojářů, z důvěryhodných zdrojů. Jednoduchým řešením, pokud to daný operační systém podporuje, je použití repozitáře aplikací (OS Linux), App Store (Apple), Play Store (Android) nebo Windows Store (Microsoft) apod. Samozřejmě za předpokladu, že daný software je v tomto repozitáři přítomen. Aplikace v nich jsou auditovány a výše uvedené nástroje lze využít také ke zjednodušení údržby aplikací formou automatické instalace aktualizací.

Dále instalován by měl být pouze takový software, který je (bude) skutečně používán. Sníží se tím jednak nároky na počítač, jednak se tím zmenší prostor, která může posloužit útočníkovi k napadení systému. Všechny instalované aplikace by totiž měly být aktualizovány, priorita u aktualizací by měla být kladena na aktualizace aplikací, u kterých je známo, že velmi často slouží jako vstupní bod infekce nebo jsou využívány posíti:

1. operační systém samotný
2. velké kancelářské balíky (MS Office, LibreOffice a další)
3. runtime moduly pro spouštění některých aplikací: Java Runtime Environment (JRE)
4. prohlížeče souborů PDF, především Adobe Reader, prohlížeče fotek, přehravače hudby nebo videa.
5. webový prohlížeč, bez ohledu na jeho výrobce
6. atd.

Někteří odborníci na počítačovou bezpečnost doporučují jako jednu z preventivních metod používat méně oblíbené/známé, ale stále ještě dobře podporované operační systémy a programy - např. místo Adobe Reader používat Foxit Reader apod. Toto doporučení zdůvodňují menší atraktivností těchto produktů pro útočníky.

Aktivní opatření

Základním opatřením, především u systému Windows je instalace *antivirového programu*. V dnešní době je poměrně obtížně vydat autoritativní doporučení na to, který produkt je nejlepší, proto se spíše zaměříme na obecné vlastnosti a zdroje informací použitelné pro kvalifikované rozhodnutí.

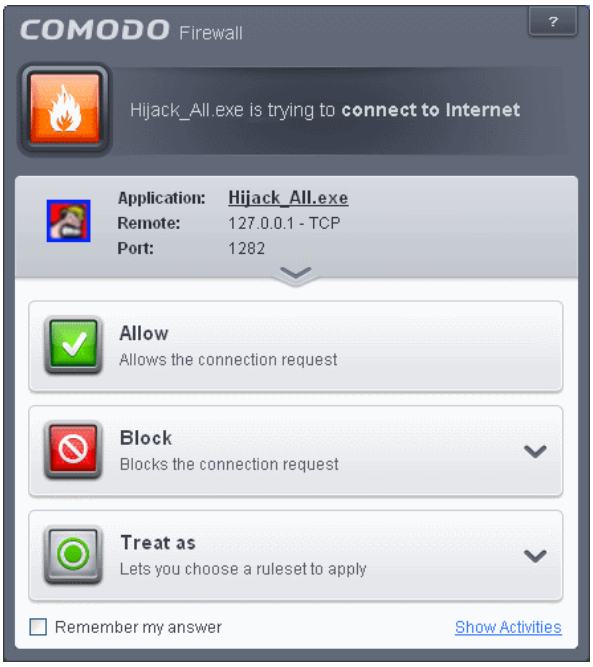
Moderní antivirové programy by kromě klasických schopností detence (on-demand - sken na vyžádání, on-access - automatický sken při přístupu k souboru). Pokud používáte podporovanou verzi operačního systému Windows, pak tyto schopnosti má operační systém vestavěné přímo prostřednictvím komponenty Windows Defender. Tyto schopnosti jsou ale v současnosti vnímány jako naprosté minimum. Vhodnou volbou antivirového řešení lze získat řadu dalších nástrojů umožňujících zvýšit efektivitu ochrany.

Nejdůležitější z nich je *osobní firewall*, zejména pokud je doplněn Host Intruder Prevention System (HIPS), popř. Network Intruder Prevention System (NIPS) moduly. Firewall by měl uživatele chránit proti nežádoucímu síťovému provozu. Základním účelem firewallu je filtrace síťového provozu. Firewall nám tedy umožňuje nastavil které počítače (IP adresami nebo jejich rozsah) mohou komunikovat mezi sebou a prostřednictvím jakých služeb (specifikováno portem).

Výše uvedená funkcionalita (filtrace síťového provozu) je ale např. ve Windows přítomna přímo jako součást operačního systému. Osobní firewall, ale tím, že je instalován na koncovém zařízení, může vykonávat mnohem více. To je rozdíl proti běžnému firewallu. Běžný firewall je totiž samostatné zařízení, které umisťujeme na sít a směřujeme přes něj síťový provoz. Osobní firewall zpracovává pouze datový provoz, který je určen zařízení, na kterém je instalován. Další funkcionalita je odvozena od kontroly aplikací, které po síti komunikují.

Představit si to můžeme následovně - webový prohlížeč Google Chrome se pokouší komunikovat po síti vs poznámkový blok se snaží komunikovat po síti. Google Chrome je webový prohlížeč, jeho úkolem tak je komunikovat po sítí. To, že se tedy po síti snaží komunikovat je možno považovat jako normální nebo dokonce žádoucí. Oproti tomu v případě poznámkového bloku to už tak jednoznačné není. Tady bychom tedy k síťové komunikaci měli přistupovat obezřetněji.

Každý počítač má do jisté míry unikátní složení nainstalovaných komponent. Předem tedy ve 100 % není možno specifikovat, které typy komunikace jsou na koncovém zařízení žádoucí a které ne. Detekcí pokusů o připojení k síti a informace o tom, zda takový pokus má být povolen je efektivní cestou jak naučit systém rozlišovat mezi žádoucí a nežádoucí komunikací. Nepříjemné je, že toto rozhodnutí obvykle musí provést člověk. Na obr. 3.6 je znázorněn příklad hlášení s možností definice pravidla chování osobního firewallu.



Obrázek 3.6: Příklad hlášení osobního firewallu Comodo Firewall (převzato z [50])

Na obr. 3.6 je pouze jedno z mnoha hlášení, reprezentující scénář, kdy se neznámý program snaží komunikovat po Internetu. Uživatel má možnost komunikaci povolit. nebo zakázat a to buďto jednorázově, nebo napořád (vytvořením pravidla). Po vytvoření pravidla bude při dalším pokusu programu o komunikaci použito toto pravidlo a uživatel už nebude osloven vyskakovacím oknem. Plný přehled všech typů hlášení je dostupný na stránkách výrobce, viz [50].

Alternativou tohoto postupu je spolehnout se na přednastavená pravidla, která ale s vysokou pravděpodobností nebudou pokrývat celé spektrum toho, co je s počítačem děláno. Problémem je, že pravidla v takovém případě bývají často mírnější, než by mohla být, což vede k omezení firewallu a jeho HIPS/NIPS modulů úspěšně odolat případnému útoku.

Některé bezpečnostní balíky obsahují i nástroj pro sandbox aplikací. *Sandbox* zjednodušeně řešeno zabraňuje aplikacím aby mohly zasahovat do dalších aplikací popřípadě operačního systému. Sandbox tedy slouží ke zpřísnění pravidel práce s aplikacemi nad rámec běžného systému práv a politik aplikovaných operačním systémem. Sandbox je možno si doinstalovat jako součást operačního systému Windows 10 verze 18305 (jarní verze 2018) nebo jako samostatný nástroj od externího dodavatel a to buď samostatně nebo jako součást antivirového (bezpečnostního) řešení.

Na kvalitu jednotlivých bezpečnostních balíků lze také usuzovat z toho, jak si vedou v různých testech nezávislých testovacích laboratoří. Nejznámější jsou:

1. Test Virus Bulletin (VB100) [81]
2. AV-Test [1]
3. Independent Tests of Anti-Virus Software [37]
4. a řada dalších

Testy se bohužel zaměřují především na detekční schopnosti jednotlivých anti-virových řešení. To je jistě důležitá funkcionalita, ale skutečného navýšení bezpečnosti může být dosáhnuto až použitím právě dodatečné funkcionality těchto řešení, která se už různí ... a bohužel je také mnohem hůře testovatelná a tak nezávislých testů v současnosti není k dispozici tolik, kolik by bylo potřeba.

Mezi tyto dodatečné funkcionality je možno zařadit:

- osobní firewall (ideálně s moduly pro behaviorální analýzu (HIPS, NIPS), výrobci označují různě)
- ochrana e-mailové komunikace (integrace s e-mail klienty) pokud používáte jiné než webové rozhraní
- integrace s webovými prohlížeči
- sandbox
- ochrana proti ransomware
- případně další funkcionality

Mějte na paměti, že moderní bezpečnostní řešení jsou rozsáhlými balíky, obsahujícími mnoho komponent. Proto, bez ohledu na to, které si vyberete je potřeba po instalaci provést konfiguraci tak, aby balík fungoval tak, jak má a Vy jste profitovali maximálně z jeho funkcionality.

Jako doplňkové nástroje mohou být použity detektory rootkitů - interpretace výsledků skenů je ale v jejich případě složitější a v současnosti to už není nutné, jelikož většina anti-virových řešení obsahuje také funkcionalitu umožňující rootkity detekovat.

V případě, že existuje podezření na infekci počítače mohou mít význam i nástroje pro shromažďování údajů o spouštěných službách a aplikacích, jak je poskytují nástroje jako je Farbar Recovery Scan Tool (FRST) [8], Random's System Information Tool (RSIT) [21] nebo DDS [20]. Výsledkem funkce těchto produktů je vygenerování logu o fungování počítače, ze kterého se dá identifikovat problém.

Zálohování
Počítejte s tím, že přestože uděláte vše proto, aby Váš počítač zůstal uchráněn, není možné zaručit, že na počítač nějaký malware nepronikne. Proto je nesmírně důležité mít vyřešeno zálohování. Moderní operační systémy obsahují řadu možností, vestavěných nebo můžete komerčně dostupných aplikací. MS Windows obsahují nástroj *Historie souborů*, Mac OS obsahuje *Time Machine*, atd.

Pokud nemáte nastaveno zálohování, může být použití výše uvedených, nebo obdobných nástrojů tím nejjednodušším nástrojem, jak minimalizovat případné škody.

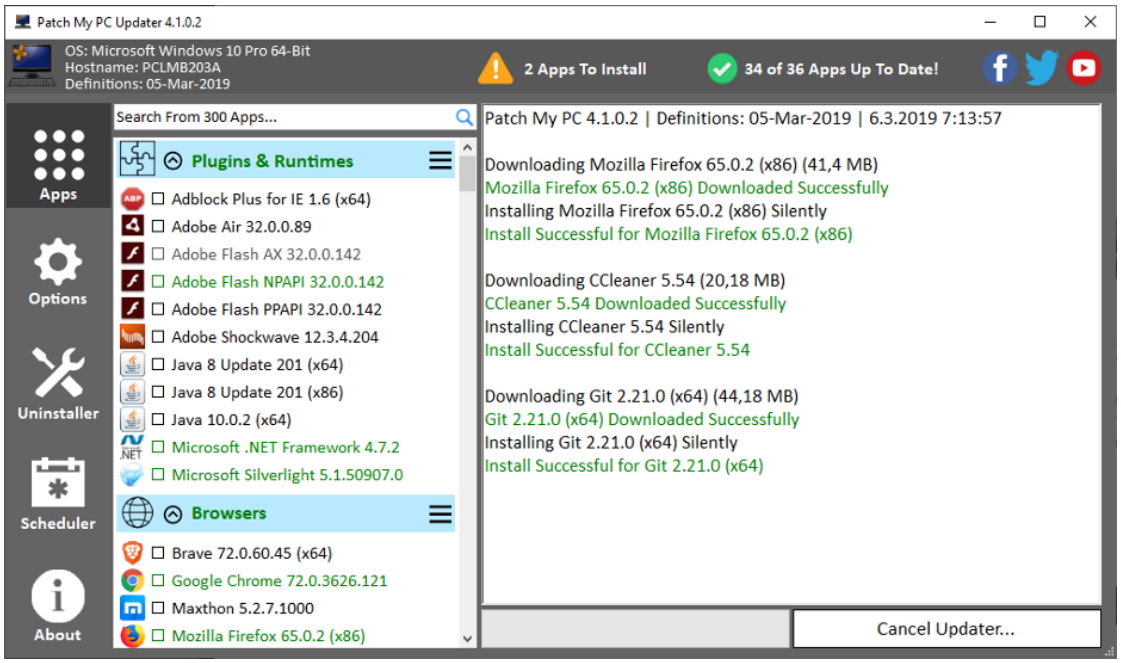
Kde aktualizovat?
Řada SW společností jako reakci na nebezpečí zneužití chyb v jimi vyvíjeném softwaru zavedla služby pro automatizované vyhledávání opravných balíčků. Microsoft zavedl tuto službu jako první s příchodem jejich operačního systému Windows 98 a tuto službu nazval jako Windows Update.

Tato služba zkontroluje registry na přítomnost aktuálních knihoven a sám nabídne opravné balíčky přehledně rozdělené do několika kategorií, dle závažnosti opravy. Podobnou službu zavedl Microsoft i pro svůj aplikační balík MS Office 2000 a vyšší. Tyto služby zde zmiňuji proto, že Windows a MS Office jsou hegemony ve své oblasti a jsou nainstalovány na až 90 % všech počítačů.

Podobné služby zavedly i jiné společnosti, například i společnosti Apple, Red Hat, Ubuntu a další pro své operační systémy. V případě těchto společností je podporována řada produktů třetích stran, což dále zvyšuje užitečnost těchto nástrojů.

Ostatní společnosti obvykle jednou za čas vydávají pro své produkty tzv. *Service Packy* (opravné balíčky), které dávají k dispozici na svých World Wide Web (WWW) stránkách. Většina softwarových společností neumožňuje automatickou detekci existence opravných balíčků. Vzhledem k závažnosti této problematiky se však počet společností, které automatické aktualizace nabízejí zvyšuje.

Pro běžné prohlížeče a utility se také nabízí možnost použití specializovaných nástrojů, které jsou schopny kontrolovat verze a v případě potřeby také aktualizovat software. Představitelem takových nástrojů je např. PatchMyPC [70], jehož rozhraní je zobrazeno na obr. 3.7.



Obrázek 3.7: Hlavní obrazovka software Patch My PC

Pro domácí užití je tento software dostupný zdarma, pro podniky je pak k dispozici mnohem mocnější verze, schopná řešit i takové problémy jako je distribuce software, údržba pracovních stanic apod.

Obdobných nástrojů existuje celá řada.

Počítačová bezpečnost v prostředí monokultury Windows

V dnešní době jsme v situaci kdy podíl nejrůznějších verzí operačního systému Windows nasazovaných v segmentu Small Office Home Office (SOHO) je přes 90 %. Dá se tedy říci, že v této oblasti funguje monokulturní prostředí Windows, které s sebou nese minimální náklady na zaškolování pracovníků, pohodlnost použití těchto nástrojů apod. Bohužel to s sebou nese také negativa – zatímco se ročně objeví tisíce virů pro Windows pro Unixové operační systémy se jich objeví 100x méně.

Přitom nelze říci, že by operační systém Windows (alespoň jeho poslední verze) z bezpečnostního hlediska podstatně hůře navržen. Samotný fakt, že má takový tržní podíl z něj činí lákavý cíl pro tvůrce virů, mají tak totiž zajištěno, že potenciálních cílů bude dostatek.

V segmentu serverů má operační systém Windows významné, nikoliv však monopolní postavení. Řada firem cíleně využívá serverů s různými operačními systémy. Tímto způsobem jednak optimalizuje náklady – vybrána je taková platforma, která je pro daný úkol vhodnější, jednak se optimalizuje i riziko, že zneužití jedné chyby určitého operačního systému povede k úplnému vyřazení celé sítě z provozu.

Podobná diverzifikace pravděpodobně v domácnostech hned tak nenastane. Z tohoto důvodu nelze

do budoucna předpokládat, že by se objevila nějaká nová platforma, která by lákala tvůrce virů, a tím by poklesl virový nápor na běžného uživatele. O to náročnější je pak práce uživatele, který musí sám vyvinout úsilí, aby mohl pracovat bezpečně.

Co s bezpečností ostatních zařízení (mobilní telefony, tablety apod.)?
Pozor Výše uvedená pravidla a také problémy jsou typické nikoliv pouze pro počítače a notebooky, ale také další zařízení - u některých byste problém čekali: chytré mobilní telefony, tablety u jiných může být zranitelnost spíše překvapením: chytré hodinky nebo náramky, smart televize, routery, k síti připojené settop boxy, chytré žárovky, různé senzory, chytré zámky, chůvičky atd.

Společným znakem těchto zařízení je to, že dosud jsme nebyli nuceni zabývat se bezpečností těchto zařízení. To se ale mění, bezpečnostní hlediska využití těchto technologií již nelze dále pomíjet, jelikož počet těchto zařízení raketově roste (viz předchozí kapitola - IoT) a dynamika nárůstu by v dohledné době neměla zpomalovat.

Významným problémem v tomto případě je, že opravování chyb není levné. V případě většiny používaných operačních systémů těchto zařízení jsou náklady rozděleny mezi společnost vyvíjející operační systém jako takový (např. Google v případě OS Android) a výrobce zařízení (např. Samsung, Lenovo, One+ a další). Výrobce pracuje tak, že vezme dostupný kód operačního systému a přizpůsobí jej pro zařízení (drivery, nadstavby OS a další). Následně takto připravenou verzi operačního systému pro podporovaná zařízení otestuje a pokud vše proběhne v pořádku zpřístupní verzi koncovým uživatelům zařízení.

Výše uvedený postup je ale drahý, proto jsou zejména lowendová zařízení podporována ze strany výrobce pouze po velmi omezenou dobu a obvykle pouze formou menších oprav. Lépe jsou pak podporována dražší zařízení, kde má výrobce výrazně větší prostor pro aktivní ochranu uživatele vytvořenou vyššími maržemi. Velmi dobře je situace viditelná např. z rozložení verzí OS Android z konce roku 2021, viz tab. 3.1.

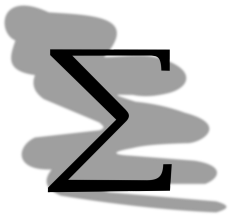
Tabulka 3.1: Podíl různých verzí OS Android k listopad 2021 (převzato z [82])

verze Android	**verze API**	**podíl**
Android 4.1 Jelly Bean	16	0.2 %
Android 4.2 Jelly Bean	17	0.3 %
Andriod 4.3 Jelly Bean	18	0.1 %
Android 4.4 KitKat	19	1.4 %
Android 5.0 Lollipop	21	0.7 %
Android 5.1 Lollipop	22	3.2 %
Android 6.0 Marshmallow	23	5.1 %
Android 7.0 Nougat	24	3.4 %
Android 7.1 Nougat	25	2.9 %
Android 8.0 Oreo	26	4.0 %
Android 8.1 Oreo	27	9.7 %
Android 9 Pie	28	18.2 %
Android 10 Q	29	26.5 %
Android 11 R	30	24.3%

V současnosti jsou ale podporovány pouze verze Android 10 a vyšší, viz [36]. Mezi údaji z tab. 3.1 a údaji z [36] je posun přibližně půl roku. Přesto je na základě těchto zdrojů možno udělat si určitou představu a stavu bezpečnosti těchto zařízení.

Prakticky to znamená pouze přibližně polovina telefonů a tabletů s OS Android, používá podporovanou verzi operačního systému. Toto číslo není vysoké, na druhou stranu se jedná o výrazný posun v bezpečnosti, protože ještě v roce 2016 se jednalo pouze o 39 %. Pro srovnání míra adopce poslední verze iOS na iPhone se uvádí v současnosti okolo 90 %. K tomu je ale potřeba dodat, že distribuční model iOS je výrazně jiný než je tomu v případě OS Android. Čistě z pohledu bezpečnosti jsou důsledky zřejmé.

Z výše uvedeného vyplývá, že problém ochrany koncových zařízení a tím také ochrany počítačových sítí jako takových je mnohem složitější, než by se na první pohled mohlo zdát. Aktivity na zajištění bezpečnosti tak musí být realizovány na všech těchto zařízeních. Odpovědnost za bezpečnost tak do jisté míry leží na každém z nás.



Shrnutí

Škodlivý kód je závažným a velmi složitým problémem dnešní doby. Mezi škodlivý kód řadíme počítačové viry, červy, trojské koně, spyware, rootkity.
Proti škodlivému kódu je nutné se bránit použitím specializovaného software – antivir, osobní firewall, detektory rootkitů apod. a také omezit použitelný vektor šíření škodlivého kódů instalací záplat a opravných balíčků k programům nainstalovaných na Vašem PC.

Kontrolní otázky

1. V čem spočívá nebezpečí rootkitů?
2. Co je to vektor šíření škodlivého kódu?
3. Mohou mít trojské koně nějaké legální opodstatnění?
4. Vyjmenujte alespoň tři metody aktivní ochrany proti škodlivému kódu.
5. Je spyware destruktivní?

Správné odpovědi

1. Skrývají některé činnosti před uživatelem a ten tak ztrácí úplnou kontrolu nad svým systémem.
2. Jedná se o způsob, kterým se daný škodlivý kód šíří, např. využití nějaké známé zranitelnosti operačního systému apod.
3. Ano, pokud slouží pro legální účely. Jejich legální užití je však značně omezené.
4. Použití antiviry, antispyware, detektorů rootkitů ...
5. Destrukce není primárním úkolem spyware. Bohužel se tento typ škodlivého kódu obvykle hluboko zavrtává do operačního systému, aby znesnadnil odhalení – odstranění, a to může být destruktivní z hlediska funkčnosti systému (tedy nikoliv aktivní výmaz dat).

Test

1. Keylogger zaznamenává
   (a) Příchody a odchody zaměstnance do práce
   (b) Stisky kláves
   (c) Jaké programy jsou spuštěny
2. Klasické počítačové viry se vyskytují (jako podíl celkového škodlivého kódu)
   (a) Převážně
   (b) Tak napůl
   (c) Skoro vůbec
3. Ve windows mi maximální bezpečnost zajišťuje účet s právy
   (a) Administrátorskými
   (b) Power user
   (c) user
4. Instalovat opravy je potřeba
   (a) Ignorovat
   (b) Nainstalovat jak si vzpomenu
   (c) Nainstalovat ihned co vyjdou
5. Pro detekci spyware mohu použít
   (a) Antispyware
   (b) Antivir
   (c) Rootkit detektor

Správné odpovědi

1. b), 2. c), 3. c), 4. c), 5. a) b) (i když pouze omezeně)

Kapitola 4

Šifrování a elektronický podpis

Náhled kapitoly
Šifrování a elektronický podpis jsou moderními technologiemi, jejichž význam stále stoupá. To je také důvod, proč se s těmito technologiemi v této kapitole seznámíme i my.

Po přečtení kapitoly budete
Vědět

1. Co je šifra a elektronický podpis
2. Jak je jejich použití upraveno legislativně
3. Jaké jsou předpoklady bezpečnosti jednotlivých šifrovacích algoritmů popř. algoritmů elektronického podpisu

Čas pro studium
Tato kapitola je jedna z nejrozsáhlejších v těchto skriptech, zároveň obsahuje celou řadu nuancí a návazností, které by bylo vhodné během studia plně pochopit. Proto studium této kapitoly může zabrat i celý den... nespěchejte.

4.1 Základní pojmy

Předtím než začneme se samotným výkladem šifrování jako takového zaměříme se na vysvětlení některých pojmů, které pak budou využity v dalším výkladu.

Šifrováním rozumíme obvykle proces převodu textu nebo dat z otevřené podoby do podoby šifrované. Účelem šifrování je tedy chránit text popř. data proti neoprávněnému přečtení.

Otevřeným textem/daty v tomto případě rozumíme text nebo data, která jsou přímo čitelná nebo interpretovatelná. Např. tento text je v češtině, není nijak chráněný, jedinou překážkou jeho pochopení proto mohou tvořit nové pojmy nebo myšlenky, se kterými čtenář dosud nepracoval.

Tento text je tedy otevřený.

Definice otevřeného textu v zašifrované podobě by mohl vypadat např. následovně: Bgriřrayz grkgrz/qngl i gbzgb cřícnqě ebmhzízr grkg arob qngn, xgreá wfbh cřízb čvgryaá arob vagrecergbingryaá. Ancř. gragb grkg wr i čršgvaě, araí avwnx pueáačaý, wrqvabh cřrxážxbh wrub cbpubcraí zbubh gibřvg abié cbwzl arob zlšyraxl, fr xgreýzv čgraář qbfhq arcenpbiny.

Jak je vidět z předchozího odstavce, šifrovaný text není přímo čitelný/interpretovatelný. Pro jeho přečtení je vyžadována jistá znalost, tu můžeme označit jako *klíč*. V předchozím příkladu tvoří klíč identifikace použitého šifrovacího algoritmu a parametru(-ú) tohoto algoritmu, v našem případě byla pro zašifrování textu použita Caesarova šifra s posunem abecedy o 13 znaků aplikovaná na všechny písmena bez interpunkce (písmena s interpunkcí a mezery zůstaly beze změn). K zašifrování byla použita jednoduchá webová aplikace Caesar cipher decryption tool [56].

S touto znalostí jsem schopen otevřený text zašifrovat a šifrovaný text zase dešifrovat.

Podle způsobu šifrování a množství klíčů, lze šifrovací algoritmy dále dělit viz další kapitoly těchto skript.

4.2 Stručná historie šifrování

Dá se říci, že šifrování je staré jako lidstvo samo, přinejmenším od vynálezu písma. První dokumentované použití šifry se datuje někdy okolo roku 1900 př. n. l. do oblasti starého Egypta, kde neznámý písař tvořil nápisy z nestandardních hieroglyfů.

Někdy k roku 1500 př. n. l. se datuje původ destičky z Mezopotámie se zašifrovaným návodem na výrobu glazur na keramiku.

Mezi 500 – 600 před naším letopočtem hebrejští učenci napsali knihu Jeremiášovu, pro kterou použili jednoduchou substituci nazývanou ATBASH, kdy použili obrácenou abecedu (místo A Z, B Y apod.). ATBASH je představitelem tzv. *substitučních šifer*. Substituce znamená, že písmena otevřené abecedy jsou nahrazována písmeny šifrovací abecedy. Jelikož v tomto případě používáme jedinou šifrovací abecedu, můžeme tuto šifru označit také jako *monoalfabetickou*.

Tento typ šifer byl pro svou jednoduchost velmi oblíben v starověku a raném středověku.

Do roku 487 př. n. l. se datuje použití nástroje „skytale“ v Řeckém městském státě Sparta. Jednalo se o dřevěný kolík, na který se namotával úzký proužek kůže. Na tuto kůži se napsala zpráva, kůže se odmotala a poslala po poslovi na místo určení. Pro dešifrování zprávy potom bylo nutné mít kolík o správném průměru. Představu o vzhledu si můžete udělat z obr. 4.1.

Obrázek 4.1: Skytale (převzato z [27])

V období svého tažení (2. pol. 1. stol. před. n. l.) Gaius Julius Caesar pro komunikaci s Římem používal jednoduchou *substituční šifru* – jednotlivá písmena abecedy byla posunuta o tři znaky doprava. Pro tuto šifru se vžilo označení Caesarova. I tato šifra je monoalfabetická.

Někdy mezi 725 a 790 byla napsána první teoretická kniha o šifrování, arabský učenec Abd al-Rahman al-Khalil ibn Ahmad ibn ‘Amr ibn Tammam al Farahidi al-Zadi al Yahmadi v ní psal o luštění kryptogramů, byl přitom inspirován svou prací luštitele pro Byzantského císaře. Do dnešní doby se bohužel původní kniha nedochovala, její obsah bych ale rekonstruován z z fragmentů knih dalších soudobých autorů citujících al Yahmadiho.

Z hlediska kryptoanalýzy se jedná o první dílo, které prokazuje, že monoalfabetické substituční šifry není možné považovat za bezpečné a při použití správného postupu je možné je prolomit téměř v reálném čase.

Al Yahmadi k tomuto účelu používal metodu tzv. *známého textu*. Jelikož většina zachycených zpráv byla mezi šlechtou, která si potrpěla na formální oslovování a adresát zprávy byl znám díky zadržení posla. Mohl al Yahmadi odhadnout znění části zprávy, čímž získal kombinaci otevřeného (byť malého) a šifrovaného textu. Z použitých písmen pak mohl odhadnout část klíče. I s částečnou znalostí klíče

mohou být některá částečně dešifrovaná slova odhadnutelná. Každé odhadnuté slovo umožní rozšířit znalost o klíči až do okamžiku, kdy je celá zpráva dešifrována.

Tento postup je poměrně jednoduchý a intuitivní. Obdobné postupy se používají dosud, byť jsou využívány mnohem sofistikovanější metody matematické analýzy.

Záhy se také ukázalo, že i bez znalosti známého textu je možno texty šifrované pomocí monoalfabetických substitučních šifer jednoduše a spolehlivě dešifrovat pomocí tzv. *frekvenční analýzy* textu. O frekvenční analýze si ale povíme něco později, v kapitole 4.3.

Právě známá slabost v té době používaných šifrovacích algoritmů vedla papeže Klementa VII, aby v roce 1379 zadal Gabrieli di Lavindemu úkol vytvořit nový šifrovací systém, který by těmito slabinami netrpěl. Di Lavinde věděl, že substituční šifru již nemůže použít, zároveň ale sofistikovanější šifrovací schémata jsou mnohem náročnější na čas a také různé potřebné pomůcky. Proto přišel s jednoduchý a přitom svým způsobem geniálním řešením. V jeho šifrovacím systému zůstává substituční šifra, ale pouze jako z vrstev ochrany mající za cíl zmást nepřítele. Skutečnou ochranu poskytuje kódování zprávy.

Kódy rozumíme posun významu slov ve zprávě. Zakódovaná zpráva tedy vypadá jako otevřený text, přesto není možné najít skutečný význam zaznamenaného sdělení, ne beze znalosti použitého kódu. Di Lavinde pak zakódovanou zprávu dále šifroval pomocí běžné substituční šifry. V případě zachycení zprávy lze předpokládat, že substituční šifra bude prolomena. Útočník dostane zprávu, která vypadá jako otevřený text, to jej může uspokojit a obsah zprávy tak zůstane v bezpečí. Nebo útočník může mít podezření (nikoliv však jistotu), že význam zprávy je jiný. I v takovém případě zůstává ale bezpečnost zachována.

Pro svou jednoduchost a relativně vysokou úroveň poskytované bezpečnosti zůstal tento šifrovací systém v použití až do 18. století.

Jak bylo zmíněno výše, sofistikovanější šifrovací schémata vyžadují sofistikovanější pomůcky. Jednou z takových pomůcek byl *šifrovací disk*, viz obr. 4.2. *Polyalfabetické šifry* využívají k šifrování více než jednu abecedu. To je obrovský posun v bezpečnosti proti monoalfabetickým šifrám. První takovou (zdokumentovanou) pomůckou byl šifrovací disk Leona Battisty Albertiho datovaný někdy okolo roku 1466.

Použití je relativně jednoduché. Vnitřní kruh představuje otevřenou abecedu, vnější kruh pak abecedu šifrovanou. Klíč je tvořen jednak šifrovacím diskem, počáteční polohou obou kol a pravidlem, jak disk použít. Takovým pravidlem může být třeba posun o dva znaky doprava pro každý následující znak. Pravidlo ale samozřejmě může být složitější. Požadavek je pouze jediný - musí být dohodnuto na obou stranách komunikace, jinak nebude možno zašifrovanou zprávu možno dešifrovat.

Blaise de Vigenère 1585 publikoval knihu o šifrování, ve které jako první zmiňuje koncept autoklíče. K šifrování se používal *Vigenèrův čtverec*, v jednotlivých řádcích byly substituční abecedy. Řádky byly seřazeny abecedně, kde počáteční písmo substituční abecedy určovalo posun abecedy. Tedy první řádek začínal A a odpovídal abecedě otevřeného textu (tedy bez posunu), 2. řádek začíná B s posunem abecedy o jeden znak, 3. začínal C...

Vigenèrův čtverec zůstává neměnný, pro nasazení je ale nutná ještě znalost klíče, kterým může být libovolné slovo nebo slova. Podmínkou je, aby písmena klíče byla obsažena ve čtverci. Klíč totiž bude použit pro postupný výběr abeced k šifrování a dešifrování textu. Klič podle velikosti zprávy opakujeme.

1917 americká vláda zaměstnala Williama Fredericka Friedmana, považovaného za duchovního otce kryptoanalýzy v USA, a jeho manželku, aby pro armádu luštili šifry a vyvíjeli nové standardy pro zvýšení bezpečnosti komunikace. W. Friedman byl také prvním ředitelem NSA, která obdobné činnosti provádí dosud.

1927 – 1933, v USA vládne prohibice, což vede k rozmachu organizovaného zločinu. Ruku v ruce s tím se začaly šifry používat utajení informací před konkurencí i policií. V reakci na to FBI zřídila oddělení, které se zabývá dešifrováním takových zpráv. Toto oddělení pracuje dosud.

1933 – 1945 šifrovací stroj Enigma nasazen a masově využíván nacistickým Německem. Nasazení Enigmy předznamenává použití moderních technologií, jako základu bezpečnosti.

4.3 Substituční šifry

Vraťme se zpět k substitučním šifrám a jejich bezpečnostním předpokladům.

Substituční šifry fungují na tom principu, že písmena abecedy nahrazujeme podle předem stanovených pravidel za jiná písmena nebo znaky. Nejznámější substituční šifru vytvořil římský císař

Obrázek 4.2: Šifrovací disk Leaona Battisty Albertiho (převzato z [45])

Caesar během svého tažení do Galie a během historie ji použil v modifikované verzi například i císař Augustus.

Caesarova šifra:

```
Otevřený text  A B C D E F G ...
Šifrovaný text D E F G H I J ...
```

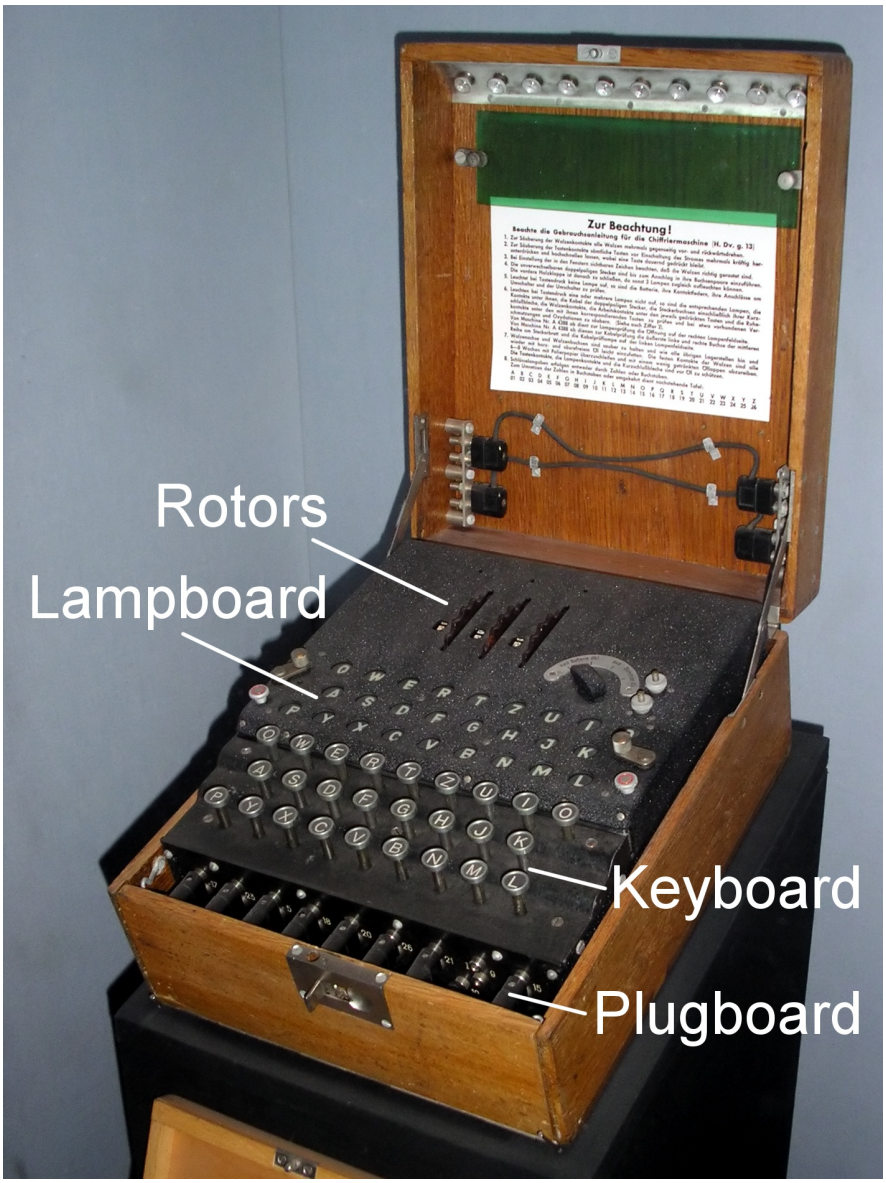
Na první pohled se jedná o šifru bezpečnou, jednotlivá písmena zprávy jsou nahrazovány jinými písmeny tak aby výsledný text nebylo možné přečíst... tedy pokud vyloučíme možnost použití metody známého textu. Pokud se ale nad celým konceptem zamyslíme, zjistíme, že prolomení šifry i tak není složité.

U každého jazyka je totiž frekvence výskytu různých písmen různá. Drobné rozdíly ve frekvenci použití písmen je možné vysledovat také v různých typech textu - např. mohou být rozdíly mezi textem odborným a beletrií. Tyto rozdíly jsou však méně významné, jelikož obvykle ovlivňují pořadí méně používaných písmen.

Na základě frekvenční analýzy otevřeného textu (libovolného otevřeného textu) v daném jazyce je tedy možné seřadit písmena abecedy podle frekvence výskytu v textu. Pokud podobným způsobem vytvoříme frekvenční tabulku výskytu písmen zašifrované zprávy a seřadíme obě abecedy podle frekvence získáme větší část klíče přiložením obou seřazených abeced k sobě.

Výsledný dešifrovaný text může obsahovat chyby v některých méně používaných písmenech, ale měl by být čitelný.

Pro svou nízkou odolnost kryptoanalýze se záhy začaly objevovat pokročilejší šifry, které jsou tzv. *polyalfabetické*. Tyto šifry nepoužívaní jedinou abecedu jako klasické substituční šifry, ale více abeced, přičemž tyto abecedy se střídají, obvykle po písmenu. Tímto způsobem se významně znesnadňuje frekvenční analýza textu. K tomu je však potřeba dodat, že při použití dlouhého šifrovaného textu a malého počtu abeced je ale dešifrování frekvenční analýzou stále možné.



Obrázek 4.3: Přístroj Enigma s třemi rotory (převzato z [6])

Pokud zajistíme, že počet použitých abeced pro šifrování bude roven poštu písmen zprávy, je možno považovat tento způsob šifrování za bezpečný i v dnešní době. K tomu je ale potřeba doplnit také to, že při zvyšujícím se počtu abeced se výrazně zvyšuje „režie“ správy klíče. Klíč v takovém případě bude mít délku odpovídající počtu písmen šifrovacích abeced vynásobeného počtem písmen zprávy. Délka klíče tedy bude mnohonásobně delší než zpráva samotná.

To je také jedním z důvodů, proč moderní šifrovací schémata používají odlišné přístupy, které ale ke své funkci vyžadují použití moderní výpočetní techniky.

4.4 Kódy

Kódy rozumíme slova, která mají v běžném jazyku nějaký význam, ale my je používáme ve významu jiném. Pro úspěšné využití kódů se musí všichni účastníci komunikace předem dohodnout, jakým způsobem bude kódování probíhat – tedy zajistit, aby zakódovaná zpráva mohla být správným způsobem pochopena (dekódována).

Využití kódů lze za dodržení určitých bezpečnostních opatření považovat za bezpečnou i dnes. Důvodem je to, že kódy na rozdíl od běžných šifrovacích schémat nejsou matematicky analyzovatelné.

Není je tedy možné prolomit tzv. *hrubou silou*. Pokud případný „špión“ nezná význam jednotlivých kódových slov, nemůže zprávu správně dešifrovat.

Prolamování kódů je tak založeno na útoku na lidskou složku, např. formou získání kódovacích knih nebo získání kódů výslechem osob, které jej znají. Alternativně v případě použití stejného kódu opakovaně je možno vypozorovat u příjemce určité vzorce chování jako reakce na přijatou zprávu, ze kterého lze usuzovat na význam kódů.

Podobně jako u polyalfabetických šifer je tak bezpečnost založena na pravidelné změně kódů, ideálně po každé odeslané zprávě. Takový postup se používal ještě během první světové války. Pro zajištění efektivní možnosti rotace kódů byly využívány tzv. *kódovací knihy*. Kódovací kniha obsahovala na každé stránce seznam klíčových slov pro zakódování. Po zakódování se stránka z knihy vytrhla a zničila – jednorázové kódy bez vlastnictví kódovací knihy prakticky není možné prolomit.

Logickým slabým místem celého procesu je ale právě kódovací kniha. Pokud se jí zmocní neoprávněná osoba získá možnost interpretovat jakoukoliv zachycenou zprávu. Navíc použití kódovacích knih představuje opět výrazné zvýšení režie celého procesu. A tak ani kódování se v dnešní době nijak masově nevyužívá.

4.5 Symetrické a asymetrické šifry

Tématem symetrických a asymetrických šifer se dostáváme již k moderní kryptografii. Na začátku kapitoly jsme si říkali, že jedním ze způsobů, jak typově rozlišit šifrovací algoritmy je podle způsobu jak pracují s klíčem. Algoritmy, které jsme probírali dosud byly z tohoto pohledu stejné - vyžadovaly znalost toho, o jaký algoritmus se jedná a parametrů, které je potřeba použít. Tato informace přitom byla totožná pro operace šifrování i dešifrování. Takové algoritmy označujeme jako *symetrické*

Výhodou symetrických šifrovacích algoritmů jejich relativně malá hardwarová náročnost, vysoká rychlost zpracování a svým způsobem intuitivnost celého procesu. Konečně jedná se o logické vyústění tisíců let vývoje. Tady pouze připomínám, že moderní šifrovací algoritmy jsou realizovatelné pouze pomocí výpočetní techniky. Na následujících stránkách sice budou demonstrovány některé postupy ručním výpočtem, ale tyto výpočty jsou velmi omezené velikostí použitelných čísel. Demonstrace tak budou používat čísla malá. Pro reálné nasazení se používají mnohaciferná čísla, tedy čísla např. se stovkami cifer.

Velikost cifer je právě jením z faktorů zajišťujících bezpečnost algoritmů. Při použití malých čísel je úroveň bezpečnosti takových algoritmů malá. Pro použití velkých čísel potřebujeme podporu výpočetní techniky.

Typově lze symetrické šifrovací algoritmy dále rozdělit do dvou podskupin: *blokové* a *proudové* (stream) šifrovací algoritmy. Hlavní rozdíl mezi nimi je v účelu šifrování.

Blokové šifry jsou koncepčně starší a slouží pro šifrování souborů, zpráv apod. Tento typ šifrovacích algoritmů pracuje tak, že zpracovává šifrovanou zprávu po blocích o určité délce - odtud název bloková šifra.

Proudové šifry jsou proti tomu jiné - jsou určeny pro šifrování datových proudů jejichž přesná délka není předem známa. Proudové šifry se používají pro šifrování datových přenosů, hovorů telefonních sítích, šifrování videokonferencí apod.

Podívejme se na jednotlivé podtypy podrobněji.

4.5.1 Blokové šifry

První komerčně nasazená symetrická šifra byla vyvinuta v laboratořích IBM (konec 60. let) a byla nazvána *Lucifer*. Hned po uvedení na trh o systém projevily zájem některé pojišťovací společnosti s hustou sítí poboček, které v něm viděli efektivní prostředek pro zabezpečení komunikace s ústředím.

V roce 1973 americký National Institute for Standards and Technology (NIST) vypsal soutěž na navržení šifrovacího algoritmu pro použití ve státní správě. Do této soutěže IBM nabídla zdokonalenou verzi svého Lucifera. IBM v té době byla jedinou společností, která byla schopna nabídnout funkční odzkoušený systém pro šifrování a z tohoto důvodu také soutěž vyhrál.

Do finálního jednání se vedle NIST zapojila také National Security Agency (NSA). NSA, jak víme z našeho historického exkurzu, byla založena mimo jiné proto, aby přispívala k zavádění nových bezpečných komunikačních postupů. Zapojení z tohoto pohledu bylo logické. V tomto případě, ale narazilo také na druhou významnou funkci NSA a to prolamovat bezpečnost šifrovacích systémů využívaných cizími státy.

Oba tyto úkoly jsou do jisté míry protichůdné, pokud budeme předpokládat, že jakékoliv šifrovací schéma (postup, algoritmus) dříve nebo později unikne a může se stát, že jej v budoucnu budou využívat nepřátelské státy. Tento vnitřní konflikt cílů se projevil neblaze právě na výsledném algoritmu, standardizovaným v roce 1976 pod názvem Decryption Encryption Standard (DES).

Výsledkem byl kompromis, ve kterém se původně navrhovaná délka klíče 128 bitů, kterou používal Lucifer, zmenšila na 56 bitů. Snížená délka klíče měla umožnit NSA, aby v případě potřeby mohla šifru prolomit tzv. hrubou silou. Z hlediska bezpečnosti je potřeba si uvědomit, náročnost útoku hrubou silou roste exponenciálně s délkou klíče. Pro srovnání komplexita útoku na Lucifer je $2^{1}28$, zatímco pro DES je to pouze $2^{5}6$.

Také proto již těsně po uvedení šifry se objevily pochybnosti o její bezpečnosti, které ve svém důsledky vedly k vytvoření alternativního proudu v kryptografii a vyvinutí asymetrických šifer.

Definitivní odpověď na otázku, zda je 56 bitů pro klíč z hlediska bezpečnosti dost dal projekt DES Cracker, který prokázal, že Již v roce 1994 by mělo být možné s investicí okolo 1 mil. dolarů sestavit počítač schopný prolomit DES hrubou silou za 3,5 hod., a to s předpokladem, že cena se každých 18 měsíců sníží na polovinu (nebo se cena útoku zmenší na polovinu).

V dnešní době jsou reálně luštitelné šifry s klíčem 80-bitů. V reakci na tato odhalení byla v druhé polovině devadesátých let vypsána nová soutěž na standard nahrazující DES. Tuto soutěž vyhrál algoritmus standardizovaný pod názvem Advanced Encryption Standard (AES). NIST specifikaci tohoto algoritmu zveřejnil v rámci řady standardů Federal Information Processing Standard (FIPS), konkrétně FIPS 197 [33].

Pro prodloužení životnosti šifry DES pro nasazení ve stávajících systémech byl také algoritmus DES modifikován tak, aby zdvojnásobila bezpečnost této šifry a vytvořil se tak časový prostor pro pohodlný přechod na AES. Tato modifikace bývá označována jako Triple DES (TDES), dnes se spíše používá označení Triple Data Encryption Algorithm (TDEA). Algoritmus – viz doporučení NIST SP 800-67 Recomendation for Triple Data Encryption Algorithm (TDEA) Block Cipher [41].

S koexistencí TDEA a AES se počítá až do roku 2030. Rok 2030 zde vystupuje jako rok mezní, do kterého všechny aplikace využívající TDEA musí zavést AES. Tak dlouhá doba (30 let) je stanovena pro to, že drtivá většina přechodů na AES bude prováděna tak, že stávající systém bude nahrazen systémem zcela novým. Předpoklad tedy je, že podpora AES nebude většinou doplněna prostou aktualizací systému. Stávající systémy se tedy nechají takzvaně „dožít“, aby byly postupně nahrazeny, až se završí jejich životní cyklus. Takto bude možné zásadně omezit dodatečné náklady na zavádění AES.

Zde zmíněné standardy samozřejmě nejsou jedinými symetrickými šiframi, které se všude po světě používají. Z těch ostatních je možné vyjmenovat například: BlowFish, IDEA apod. Pro jejich nasazování však existují určitá pravidla mající za cíl zajistit, že účel, za kterým je šifrování nasazeno bude zachován.

Z hlediska nasazení se rozlišuje obvykle mezi tzv. *legacy* a novými systémy. Legacy systémy jsou, systémy nebo programové prostředky, popř. technologie, které již byly vyvinuty, prakticky nasazeny a dále se již nevyvíjejí (resp. probíhá jejich běžná údržba, nedochází ale k přidávání nových vlastnosti). Tyto systémy v sobě obsahují určité technologické předpoklady, které ovlivňují jejich bezpečnost. U starších systémů jsme obvykle limitováni v možnostech výběru šifrovacího algoritmu. Tento algoritmus musí být totiž zaveden přímo v systému a jeho změna proto nemusí představovat triviální problém. Při použití legacy systémů jsme proto obvykle odkázáni na to, co systém podporuje a pokud je nabízená technologie nevyhovující, je často nutné systém jako celek nahradit systémem novým - který požadované technické vlastnosti již má.

U nových systémů nejsme obvykle omezováni určitou technologií, resp. lze specifikovat funkční požadavky na ni. Legacy systémy lze tedy vnímat jako systémy dosluhující, na které jsou kladeny menší bezpečnostní nároky, avšak s tím, že tyto systémy budou výhledově vyřazeny nebo nahrazeny systémem novým. Nové systémy by oproti tomu měly splňovat přísnější bezpečnostní parametry, protože se předpokládá, že budou dlouhodobě provozovány.

Určitá doporučení k použití šifrovacích algoritmů poskytuje European Union Agency for Network and Information Security Agency (ENISA), Obdobné doporučení zformuloval také Národní úřad pro kybernetickou a informační bezpečnost (NUKIB), pro potřeby organizací z ČR. Přehled používaných algoritmů blokových šifer s doporučeními pro nasazení je dostupný v tab. 4.1.

Z výše uvedených algoritmů NÚKIB preferuje použití AES, Camelia a Serpent algoritmy v uvedeném pořadí, s minimální délkou klíče 256 bitů.

Tabulka 4.1 obsahuje některé šifrovací algoritmy, se kterými jsme se dosud nesetkali, podívejme se

Tabulka 4.1: Doporučení pro nasazení algoritmů blokových šifer (adaptováno z [73] a [68])

	ENISA		**NÚKIB**	
	legacy	**nové**	**legacy**	**nové**
AES	ano	ano	ano	ano
Camellia	ano	ano	ano	ano
Serpent	-	-	ano	ano
TDES	ano	ne	ano	ne
Kasumi	ano	ne	ano	ne
Blowfish	ano	ne	ano	ne
Twofish	-	-	ano	ano
DES	ne	ne	ne	ne

na ně nyní.

Algoritmus *Camellia* byl vyvinut v roce 2000 ve společnosti Mitsubishi a Nipon Telegraph and Telephone Corporation (NTT) v Japonsku. Tento algoritmus byl certifikován v rámci Cryptography Research and Evaluation Comittees (CRYPTREC) ustaveném japonskou vládou pro certifikaci šifrovacích šifrovacích algoritmů pro použití na území Japonska a také v rámci Evropského projektu New European Schemes for Signatures, Integrity and Encryption (NESSIE). Camellia podporuje šifrovací klíče délky 128, 192 a 256 bitů.

Algoritmus Serpent se účastnil soutěže na AES a skončil druhý, zejména díky některým rozhodnutím v oblasti bezpečnosti, které způsobily sice vyšší odolnost vůči určitým typům útokům, ale za cenu výrazně vyšší výpočetní náročnosti. Výhodou Serpent algoritmu je, že byl vydán pod public domain licencí a není zatížen žádnými patenty.

Standard je dostupný také ve formě Request for Comment (RFC) nezávislé standardizační entity Internet Engineering Task Force (IETF), která se zabývá standardizací technologií používaných v celosvětové síti Internet. Konkrétně se jedná o standard RFC 3713 [64].

Šifrovací algoritmus *Kasumi* má široké použití v systémech Universal Mobile Telecomunications System (UMTS), Global System for Mobile Communications (GSM) nebo GPRS. Tento algoritmus byl odvozen ze staršího algoritmu MISTY1 (Mitsubishi Improved Security Technology (MISTY)). Také algoritmus MISTY1 byl vyvinut firmou Mitsubishi a byl jedním z „kandidátů“ na standardizaci v rámci CRYPTREC, v roce 2013, ale z posuzování vypadl. Samotný algoritmus Kasumi byl navržen pro zajištění bezpečnosti v mobilních sítích třetí generace a byl certifikován v rámci Security Algorithms Group pf Experts (SAGE), které je součástí evropského certifikačního orgánu European Telecomunication Standards Institute (ETSI).

Paradoxně je Kasumi proti MISTY1 zjednodušen. Důvodem byla příliš velká časová náročnost prováděných kryprovacích operací v rámci MISTY1 algoritmu. V roce 2010 byl publikován postup, který výrazně zjednodušuje útok na tuto šifru pomocí tzv. *útoku souvisejícími klíči*. Tento útok je založen na pozorování fungování šifrovacího algoritmu pomocí několika různých klíčů. Původní otevřeného textu sice na začátku procesu není známa, ale mezi klíči existují matematické souvislosti, které tyto klíče spojují, a které jsou známy útočníkovi. To výrazně zjednodušuje složitost útoku na šifrovací algoritmus jako takový.

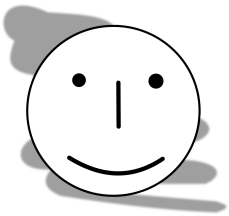
Použití algoritmu Kasumi pro nové aplikace a systémy se nedoporučuje.

Algoritmus *Blowfish* navrhla v roce 1993 jedna z nejviditelnějších osobností počítačové bezpečnosti Bruce Schneier. Pro šifrování využívá klíče o velikosti 32 - 448 bitů. Základní slabinou algoritmu Blowfish je fakt, že pro něj existují tzv. *slabé klíče*, kterým je potřeba se vyhnout. Slabé klíče jsou v tomto případě všechny klíče o délce menší než 80 bitů. Výhledově by uživatelé měli přejít buď na algoritmus AES nebo na bezpečnější verze Blowfish nazvané Twofish nebo Threefish.

Velikost klíče a bezpečnost

V této kapitole byla zmíněna celá řada šifrovacích algoritmů a různých velikostí šifrovacích klíčů. Z hlediska bezpečnosti obvykle platí, že čím větší je klíč, tím lépe jsou šifrovaná data chráněna. Při útoku hrubou silou totiž útočník musí pro odhalení klíče projít větší prostor, ve kterém může klíč být. Matematicky lze tuto skutečnost vyjádřit následovně (4.1):

$$p = \frac{a^k}{2} \tag{4.1}$$



Fakta o Bruce Schneirovi
Když Bruce Schneier pozoruje kvantovou částici, zůstane ve stejném stavu dokud Bruce pozorování nedokončí.

Bruce Schneier umí prolomit šifrování eliptickými křivkami tím, že je ohne do podoby kruhu.

Žádná prvočísla nejsou, existují pouze taková čísla, u kterých Bruce Schneier nechce, abyste je faktorizovali.

Další „fakta“ o Bruce Schneierovi můžete zjistit z http://www.schneierfacts.com/.

Kde p je průměrný počet pokusů potřebných pro odhalení klíče. Tento počet pokusů je odvozen z velikost použité abecedy a a velikosti klíče k. Se zvyšující se délkou klíče roste tedy složitost útoku exponenciálně. a^k přitom představuje úplný prostor (kombinace všech možných znaků), kde se může šifrovací klíč nacházet. /2 pak říká, že klíč se může nacházet jak v první tak v druhé polovině prohledávaného prostoru.

Z hlediska doporučené velikosti šifrovacího klíče existuje celá řada názorů - v současnosti se často doporučuje používat **šifrovací klíč o minimální velikosti 112 bitů** (viz např. [15]).

4.5.2 Proudové šifry

Zatímco blokové šifry jsou určeny pro šifrování souborů, e-mailů apod., šifry proudové jsou uzpůsobeny ochraně datových přenosů. Využívají se proto pro šifrovaní telefonních hovorů, šifrování připojení k síti WiFi apod. Jelikož šifrování proudovou šifrou pracuje v „skoro reálném“ čase, je tento typ šifer lépe optimalizován na rychlost.

Technicky je možné použít jakoukoliv šifru pro šifrování čehokoliv. Tzn., že proudové šifry technicky lze použít také pro šifrování souborů. Jde ale o to, že díky svým optimalizacím na rychlost, jsou stremovací šifry objektivně méně bezpečné a proto se nedoporučuje tento typ šifer používat pro šifrování souborů. Podobně lze blokové šifry používat pro šifrování datových proudů. Díky svým optimalizacím pro bezpečnost, ale šifrovací systém objektivně zvládne obsloužit menší objem dat.

Každý typ algoritmů má tedy své výhody a nevýhody, ze kterých lze odvodit pro jaké účely je vhodné je nasadit.

Zajímavou otázkou je nakolik nám vadí nižší bezpečnost proudových šifer? Vzhledem k tomu, že šifrovaný proud dat je časově omezen např. hovor uskutečněný pomocí mobilního telefonu délkou hovoru a faktem, že šifrovací klíče se mění pro každou „session“. Je relativní slabost použitých algoritmů vyvážena častou obměnou šifrovacích klíčů, které naopak prolomení bezpečnosti znesnadňují.

Takže ano, útočník, má sice schopnost snadněji prolomit toto šifrování, ale získá tím pouze relativně malou část dat. Pro dešifrování dalších dat musí celý proces prolomení opakovat. Účinnost takového procesu je velmi malá. Z čehož lze dovodit, že používat proudové šifry pro tento účel je naopak efektivní.

I pro proudové šifry ENISA poskytuje doporučení [73], stejně jako NÚKIB, viz tab. 4.2.

Byť NÚKIB doporučuje nasazení blokových šifer všude tam, kde je to jen možné. Jinými slovy silně preferuje použití blokových šifer před šiframi proudovými.

Tabulka 4.2: Doporučení pro nasazení algoritmů proudových šifer (adaptováno z [73] a [68])

	ENISA		**NÚKIB**	
	legacy	**nové**	**legacy**	**nové**
Rabbit	ano	ano	-	-
SNOW 3G	ano	ano	ano	ano
Trivium	ano	ne	-	-
SNOW 2.0	ano	ne	ano	ano
ChaCha20	-	-	ano	ano
A5/1	ne	ne	-	-
A5/2	ne	ne	-	-
E0	ne	ne	-	-
RC4	ne	ne	-	-

Algoritmus *Rabbit* je definován ve standardu IETF RFC 4503 [43] a je také součástí standardu ISO/IEC 18033-4 [12]. Šifra byla poprvé prezentována v roce 2003 a standardizace v rámci RFC 4503 dosáhla v roce 2006. Algoritmus používá klíč o délce 128 bitů a 64-bitový iniciační vektor.

V současné době existuje dokumentovaný útok na algoritmus, který snižuje komplexitu útoku na 2^{158}, což je však při současných možnostech výpočetní techniky považováno stále za bezpečné (jako hranice bezpečnosti se v současnosti považuje komplexita útoku 2^{128}).

SNOW 3G je zdokonalenou verzí staršího algoritmu *SNOW 2.0*. K šifrování se používá klíč o délce 128 bitů a iniciační vektor o stejné velikosti. První verze algoritmu byla posuzována v rámci projektu NESSIE, verze 2.0 se stala součástí ISO/IEC 18033-4 [12]. Algoritmy se používají primárně v mobilních sítích třetí generace UMTS.

U těchto algoritmů jsou známy některé postupy snižující komplexitu útoku, nesnižují ji ale dost na to, aby algoritmy bylo nutné považovat za nebezpečné. Pro nové aplikace se přesto doporučuje implementovat spíše bezpečnější SNOW 3G.

Algoritmus *Trivium* je algoritmem nenáročným na systémové zdroje, který je standardizován v rámci ISO/IEC 29192-3 [13]. Svou konstrukcí je algoritmus obzvláště vhodný pro hardwarovou implementaci. Používá klíč i iniciační vektor o délce 80 bitů. U plné (standardizované) verze algoritmu nejsou sice známy žádné útoky snižující komplexitu možnosti prolomení šifry, avšak délka klíče 80 bitů naznačuje, že do budoucna nebude tento algoritmus schopen poskytovat dostatečnou úroveň bezpečnosti.

Algoritmus A5/1 byl původně pro užití v rámci GSM protokolu. Je iniciován pomocí 64-bitového klíče a známého 22-bitového iniciačního čísla. Až do roku 1994 byl tento algoritmus tajen. V roce 1994 unikly na veřejnost některé informace o tomto algoritmu, které posloužily k plné rekonstrukci algoritmu metodami reverzního inženýrství. V průběhu doby se objevila celá řada slabin tohoto algoritmu, z nichž některé mohly vést až k možnosti dešifrovat hovory v síti GSM v reálném čase.

Algoritmus A5/1 je proto často uváděn jako příklad nevhodnosti nasazení přístupu *security by obscurity* v klíčových technologiích. Security by obscurity u technologie rozumíme předpoklad, že technologie je bezpečná, pokud případný útočník neví, jak vnitřně funguje. Praxe však ukazuje, že tento předpoklad se nezakládá na pravdě a útočník může usuzovat na fungování algoritmu podle vnějšího chování algoritmu, především pomocí tzv. *postranních kanálů*.

Útok pomocí postranních kanálů se nesnaží nalézt slabiny v samotné algoritmu, ale ve způsobu jakým je implementován - např. časová náročnost práce algoritmu při zpracování různých dat, analýza odběru elektrické energie, úmyslné zavádění chyb do procesu zpracování a zkoumání reakce algoritmu apod.

Algoritmus A5/2 je oslabená verze algoritmu A5/1, které byla vyvinuta za účelem vývozu z USA. V 90. letech minulého století šifrovací algoritmy vyvinuté v USA podléhaly exportnímu embargu. Cílem tohoto embarga bylo zabránit k USA nepřátelským mocnostem získat silné šifrovací algoritmy, které by pak výrazně ztížily možnosti získávání zpravodajských informací z těchto režimů.

E0 je algortimus používaný pro šifrování dat přenášených bezdrátovým přenosem pomocí bluetooth. Používá obvykle klíč o délce 128 bitů. Nejlepší známý útok je útok typu podmíněný korelační útok (conditional correlation attack) s komplexitou 2^{38}. Vzhledem ke komplexitě řešení není algoritmus E0 možné považovat nadále za bezpečný pro jakékoliv použití.

Konečně algoritmus *RC4* je využíván v řadě protokolů jako např. Transport Layer Security (TLS).

Algoritmus navrhl v roce 1987 Ronald R. Rivest (jeden ze zakladatelů velmi známé společnosti RSA zabývající se bezpečnostními řešeními na bázi šifrování). Od doby zveřejnění algoritmu se objevila celá řada útoků, pro které tento algoritmus není možné doporučit k jakémukoliv dalšímu použití.

4.6 Asymetrické šifrování

Asymetrické šifry se od šifer symetrických výrazně liší. Jejich nástup umožnilo až masivní zavádění výpočetní techniky. Algoritmy asymetrického šifrování byly také odvozovány z odlišného základního modelového problému: *mějme kulatý stůl, u kterého probíhá debata, přitom každý účastník může slyšet vše co řekne u stolu kdokoliv jiný. Základním problémem v takovém prostředí je jak dohodnout klíč komunikace. Očividně jej není možné další osobě říct, protože bude odposlechnut a možná zneužit.*

Řešením tohoto problému je vyvinutí nové skupiny šifrovacích algoritmů, které nepoužívají totožný klíč pro šifrování a dešifrování komunikace, ale používají dvojici klíčů - *privátní* a *veřejný*. Tyto klíče jsou matematicky příbuzné, ale zároveň není možné je jeden z druhého odvodit. Kontrolu nad komunikací tak útočník může získat pouze získáním obou klíčů nebo vyřešením složitého faktorizačního úkolu, jehož obecné, efektivní algebraické řešení dosud není známo.

Pro účely elektronického podpisu je možno dle stávající právní úpravy použít jeden z následujících algoritmů. Jelikož elektronický podpis je aplikací asymetrického šifrování, může nám tento výběr posloužit stejně jako kterýkoliv jiný, ovšem s tím, že se nejedná o úplný výčet dostupných algoritmů.

1. RSA
2. DSA
3. $ECDSA - F_p$
4. $ECDSA - F_m^2$
5. $ECGDSA - F_p$
6. $ECGDSA - F_m^2$

4.6.1 RSA

Název RSA je odvozen od počátečních písmen jmen Ronald Rivest, Adi Shamir a Leonard Aleman, kteří tento systém v roce 1977 navrhli.

RSA algoritmus počítá s dvěma velkými prvočísly p a q. Vynásobením těchto prvočísel čísel (viz rovnice 4.2) získáme číslo n, kterému říkáme modul.

$$n = p \cdot q \tag{4.2}$$

Zvolíme takové číslo e, které je menší než n a s matematicky příbuznými čísly našim prvočíslům p, q, tedy $(p-1)(q-1)$ nemá společného dělitele vyjma čísla 1. Mějme číslo d, takové aby $(ed\check{}1)$ bylo dělitelné $(p-1)(q-1)$. Hodnoty e a d nazveme *veřejné* a *soukromé exponenty*.

Veřejný klíč potom tvoří čísla $(n; e)$, zatímco *privátní klíč* je tvořen čísly $(n; d)$.

Matematickému postupu, kterým lze získat čísla p a q z n se říká *faktorizace*. Bezpečnost RSA je založena na předpokladu, že při současném stavu lidského vědění, je faktorizace nesmírně obtížná a pro dostatečně velké čísla p a q je reálně nemožné ji provést.

Na druhou stranu, to co dnes neumíme udělat, neznamená, že tento předpoklad bude platit také do budoucnosti. Např. problém faktorizace neumíme dnes efektivně řešit. Existuje ale tzv. *Shorův algoritmus*, pomocí kterého jej naopak efektivně řešit bude možné, nikoliv ale pomocí běžné výpočetní techniky. K výpočtu bude potřeba kvantový počítač, který ale funguje na jiných principech než počítač klasický.

V této kapitole nemáme prostor, abychom se podrobněji problematikou kvantových počítačů zabývali, trochu více prostoru je ale věnováno této problematice v kapitole budoucnost výpočetní techniky.

Podstatné pro nás ale je, že již dnes se uvažuje o nových algoritmech, které jsou takzvaně kvantově odolné, tedy nebude možné je jednoduše prolomit kvantovými počítači ... až budou k dispozici. Tyto aktivity dosud nevedly ke standardizaci nových algoritmů. Vraťme se proto zpět k algoritmu RSA a obdobným algoritmům.

Postup šifrování

Mějme dva subjekty Alici a Boba, kteří spolu chtějí komunikovat. Alice chce poslat Bobovi zprávu m.

Alice proto zprávu m zašifruje do zašifrované podoby c, tak že $c = m^e mod(n)$, kde e a n jsou získány z Bobova veřejného klíče.

Bob, aby získal původní zprávu m, musí provést inverzní operací $m = c^d mod(n)$, kde číslo d Bob získá ze svého privátního klíče.

Analogicky k tomuto postupu se provádí elektronické podepisování dokumentu. K podepsání ale nepoužijeme veřejný klíč adresáta, ale svůj soukromý klíč. Taková zpráva je dešifrovatelná pouze veřejným klíčem odesilatele.

V našem příkladě by to vypadalo následovně:

Alice podepíše dokument $c = m^d mod(n)$ (d a n Alice získá ze svého soukromého klíče).

Bob získá zprávu tak, že $m = c^e mod(n)$ (e a n Bob získá z veřejného klíče Alice).

Z hlediska bezpečnosti je tedy klíčové volba prvočísel p a q. Bylo dokázáno, že pokud délka (počet cifer) p je podstatně menší než délka q (viz (4.3)), je proces faktorizace výrazně jednodušší.

$$l(p) \ll l(q) \tag{4.3}$$

Z toho důvodu je nutné zajistit, aby obě prvočísla si svou délkou přibližně odpovídala - rozdíl v délce by neměl přesáhnout 20 cifer, viz (4.4).

$$0,1 < |l(p) - l(q)| \leq 20 \tag{4.4}$$

Je také známo, že pokud absolutní hodnota rozdílu prvočisel p a q je menší než čtvrtá odmocnina jejich součinu n (viz 4.5), existují metody pro snadnou faktorizaci (v tomto případě se jedná o Coppershmithovu metodu).

$$|p - q| < \sqrt[4]{n} \tag{4.5}$$

4.6.2 DSA

NIST publikoval algoritmus pro elektronický podpis (Digital Signature Algorithm (DSA)) jako součást standardu pro elektronický podpis [35] (Digital Signature Standard (DSS)). DSS byl vybrán NIST ve spolupráci s NSA jako standard pro digitální autentizaci pro vládní organizace USA. Tento standard byl přijat v roce 1994, s poslední verzí standardu z roku 2013.

DSS standard je zaměřen především na problematiku elektronického podpisu, algoritmy, které jsou v něm použity jsou ale využitelné i pro účely šifrování.

Parametry DSA:

1. p ... prvočíslo, kde $2^{L-1} < p < 2L$, kde L je násobkem 64.
2. q ... dělitel čísla $p - 1$, kde $2159 < q < 2160$
3. $g = h^{\frac{p-1}{q}} mod(p)$, kde h je jakékoliv celé číslo v intervalu $1 < h < p \breve{} 1$ takové aby $h^{\frac{p-1}{q}} mod(p) > 1$
4. x, k ... náhodně generované celé číslo v intervalu $0 < x, k < q$
5. $y = g^x mod(p)$

Čísla p, q a g mohou být veřejná a mohou dokonce být společná pro více uživatelů. Privátní klíč je x, veřejný y. Parametry x a k jsou využívány pouze pro vygenerování podpisu a musí být udržovány v tajnosti. Parametr k musí být vygenerován před každým podepsáním dokumentu.

Elektronický podpis s zprávy M se vygeneruje použitím rovnic:

$$r = (g^k mod(p)) mod(q) \tag{4.6}$$
$$s = (k^{-1}(SHA - 1(M) + xr)) mod(q) \tag{4.7}$$

Pro ověření pravosti podpisu se provede následující: Nechť M', r' a s' jsou čísla M, r, s, která obdržel adresát. Nejprve se provede kontrola r' a s', zda $0 < r', s' < q$, v případě, že r' nebo s' podmínce nevyhoví, je podpis odmítnut. Samotný výpočet se provede pomocí rovnic:

$$w = s'^{-1} mod(q) \tag{4.8}$$
$$u_1 = ((SHA - 1(M'))w) mod(q) \tag{4.9}$$
$$u_2 = ((r')w) mod(q) \tag{4.10}$$
$$v = (((g)^{u_1}(y)^{u_2}) mod(p)) mod(q) \tag{4.11}$$

Pokud $v = r'$, potom je podpis ověřen.

Pro úplnost $SHA - 1(X)$ je výsledek bezpečné hashovací funkce SHA-1, viz kapitola *Bezpečné hashovací funkce*.

4.6.3 ECDSA

Elliptic Curves Digital Signature Algortithm (ECDSA) znamená algoritmus elektronického podpisu založený na eliptických křivkách. Matematické základy navrhli pánové Victor Miller a Neal Koblitz někdy v polovině 80. let minulého století. Fungují analogicky ke zde již diskutovaným systémům veřejného klíče (například RSA).

Výhodou eliptických křivek je možnost jejich definice prakticky nad jakýmkoliv číselným oborem (reálných, přirozených, komplexních čísel). Eliptická křivka se skládá ze všech bodů v intervalu (x, y) které splňují podmínku (4.12):

$$y^2 = x^3 + ax + b \tag{4.12}$$

Bezpečnost algoritmů založených na eliptických křivkách je velmi podobná podmínce bezpečnosti algoritmu RSA. V případě RSA byla problémem faktorizace, v případě ECDSA tvoří tuto podmínku obtížná řešitelnost následujícího problému: *Mějme dva body G a Y na eliptické křivce jako je $Y = kG$, cílem je najít celočíselné k. Tento problém je často nazýván problémem diskrétního logaritmu eliptické křivky.*

Bohužel nemáme příliš velký prostor, který bychom mohli věnovat této problematice, zájemce le může podrobnosti poměrně jednoduše dohledat, např. ve článku [75].

V současné době výpočet obecného diskrétního logaritmu eliptického křivky je časově náročnější než například faktorizace, z tohoto důvodu jsou ECDS algoritmy srovnatelně bezpečné jako konvenční algoritmy elektronického podpisu zmiňované výše a to i s menší délkou klíče. I tento předpoklad se ale v budoucnosti může změnit.

4.6.4 Požadavky na nastavení parametrů algoritmů asymetrického šifrování

Tato podkapitola obsahuje aktuální poznatky použitelné pro správné nastavení algoritmů asymetrického šifrování, což je základním předpokladem pro bezpečné použití algoritmů. Doporučení byla převzata z doporučení ENISA [73], viz tab 4.3.

Tabulka 4.3: Doporučení pro parametry asymetrických šifrovacích algoritmů (převzato z [73])

primitivum	**parametry**	**min. legacy**	**min. nové**
RSA problém	n, e, d	$l(n) \geq 1024$ $e \geq 3$ nebo 65537 $d \geq \sqrt{n}$	$l(n) \geq 3072$ $e \geq 3$ nebo 65537 $d \geq \sqrt{n}$
Finite Field DLP	p, q, n	$l(p^n) \geq 1024$ $l(p) > 160, l(q) > 160$	$l(p^n) \geq 3072$ $l(p) > 256, l(q) > 256$
ECDLP	p, q, n	$l(q) > 160$	$l(q) > 256$
Párování	p, q, n, d, k	$l(p^{k \cdot n}) \geq 1024$ $l(p) > 160, l(q) > 160$	$l(p^{k \cdot n}) \geq 3072$ $l(p) > 256, l(q) > 256$

4.7 Elektronický podpis v zákonech

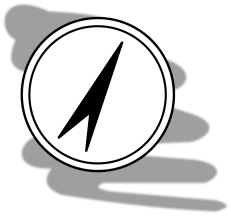
Pravidla používání elektronického podpisu v České republice jsou upravena zákonem 297/2016 Sb. o službách vytvářejících důvěru pro elektronické transakce [84], který nahrazuje do té doby platný zákon 227/2000 Sb. o elektronickém podpisu [32].

Zákon v tomto systému definuje základní pojmy a postupy které souvisí s problematikou elektronického podpisu a jeho dalších aplikací např. časového razítka. Dalším úkolem zákona je zajištění hladké přeshraniční spolupráce tak, aby zaručený elektronický podpis (vydaný dle zákona) ideálně nebyl platný pouze ve státu, který jej vydal, ale bylo možné jej ověřit v rámci celé EU.

Změna legislativy 2016
Zákon o službách vytvářejících důvěru byl přijat v září 2016 a jeho přijetím odstartovalo dvouleté přechodné období, které by mělo umožnit plynulý přechod na nová technická řešení požadovaná legislativou. Z toho důvodu v následujícím textu budou rozebrány obě právní úpravy s vysvětlenými rozdíly a důsledky.

Pro účely interoperability se implementuje v podmínkách ČR Rozhodnutí Komise č. 2011/130/EU ze dne 25. února 2011, kterým se stanoví minimální požadavky na přeshraniční zpracování dokumentů elektronicky podepsaných příslušnými orgány podle směrnice 2006/123/ES Evropského parlamentu a Rady o službách na vnitřním trhu [26].

Nová právní úprava je založena na nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (nařízení eIDAS) [17]. Už samotný název indikuje dva poměrně významné rozdíly. První je ve zvolené formě nařízení a druhé je v rozsahu řešené problematiky. Oproti původní právní úpravě je v tomto případě řešena i obecná problematika identifikace jedince nebo organizace a to v celém prostoru EU.



Nařízení EU vs směrnice EU
Směrnice EU [16] je závazná pro každý stát, kterému je určena, pokud jde o výsledek, jehož má být dosaženo, přičemž volba formy a prostředků se ponechává vnitrostátním orgánům. Prakticky se směrnice transponují ve stanoveném časovém období do právních řádů jednotlivých určených států EU formou, kterou daný stát pro daný účel zvolí, obvykle pomocí zákonů a vyhlášek.
Nařízení EU [16] má obecnou působnost, je závazné v celém rozsahu a přímo použitelné ve všech členských státech.

Původní právní úprava pracuje s následujícími prostředky:
- elektronický podpis
- elektronická značka
- časové razítko

Nová právní úprava používá následující prostředky:
- elektronický podpis (ale odlišným způsobem zaručený)
- elektronická pečeť
- časové razítko (opět odlišným způsobem zaručené)
- elektronická identita (eID)
- webové certifikáty

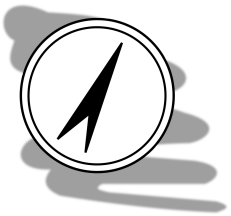
Podívejme se nejprve na nové oblasti působnosti legislativy. Účelem právní úpravy používání *webových certifikátů* je pokus získat určitou kontrolu nad bezpečností webových služeb v technologiích jako je DNSSec, protokolech https a dalších. Úprava problematiky webových certifikátů je zvláštní v tom, že je jednak nepovinná a jednak tím, že mezinárodní IT komunita toto nařízení více méně ignoruje. Přitom bez součinnosti s výrobci operačních systémů, popř. výrobců dalších softwarů jako jsou např. prohlížeče WWW není možno očekávat úspěch takové úpravy.

Účelem implementace *elektronické identity (eID)* je umožnit jednoznačně identifikovat všechny obyvatele EU bez ohledu na zemi původu. Nařízení eIDAS předpokládá postupné připojování jednotlivých členských států do tohoto systémů. Vzájemné uznávání eID je v tomto případě budováno „zdola“ - tedy od jednotlivých členských států.

Aby takového cíle bylo možné dosáhnout, je nutné, aby jednotlivá schémata byla tzv. *notifikována*:
1. členský stát vyvine za začlení do svého právního řádu eID (národní eID např. formou elektronického občanského průkazu)
2. stát poskytne popis národního eID systému ostatním státům
3. stát oznámí národní systém eID Evropské komisi
4. systém eID bude zveřejněn v Úředním věstníku
5. vzájemné uznávání

Jak je z výše uvedeného postupu patrné, jedná se o dlouhodobý proces. Předpokládá se, že do fáze vzájemného uznávání se lze dostat do dvou let (od okamžiku schválení národního eID).

V roce 2022 jsme ve stavu, kdy většina států má notifikováno jeden nebo více schémat elektronické identity, viz seznam [57]. Zatím nejsou ale patrné procesy úplně implementovány procesy vzájemného uznávání.



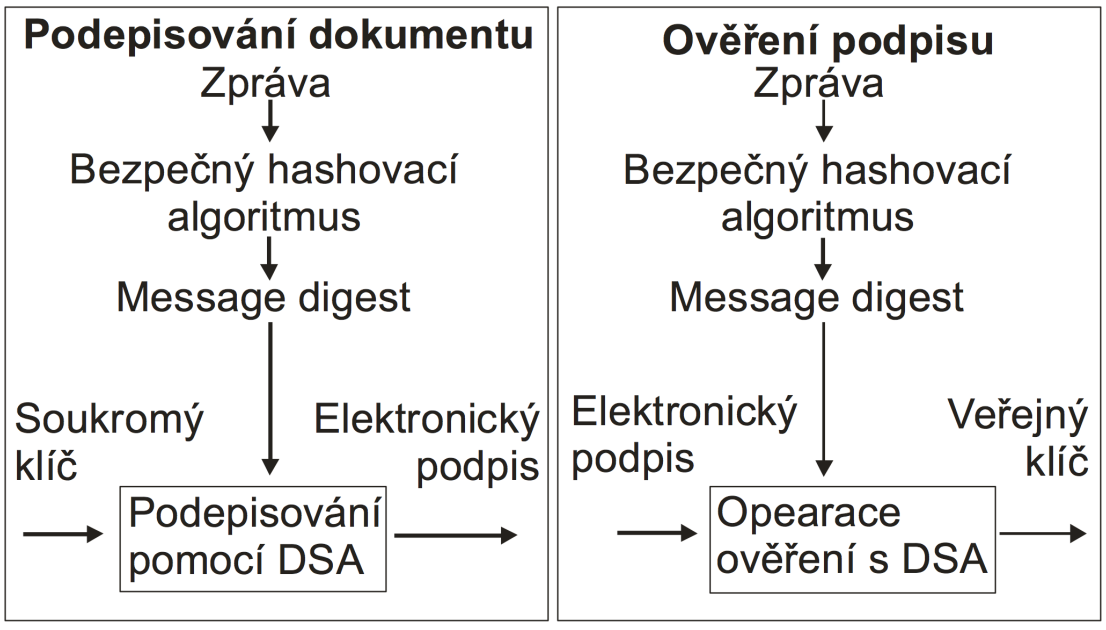
eID - elektronický občanský průkaz (eOP)
Problematika elektronické identity propojuje problematiku elektronického podpisu s problematikou e-governmentu (viz kapitola e-government). Již dnes je možno do eOP vybaveného kontaktním čipem nahrát osobní certifikát. Tuto službu poskytují oba hlavní poskytovatelé certifikačních služeb v ČR a to PostSugnum a První certifikační autorita.

Velmi důležitým pojmem, se kterým legislativa pracuje je *důvěra*. Znamená to, že cílem použití prostředků elektronického podpisu (a souvisejících prostředků) je dosažení určité úrovně důvěryhodnosti např. podepsané zprávy. Tuto důvěru lze pak využít např. pro zajištění vymahatelnosti podepsaných dokumentů apod.

Úroveň důvěry je možno rozdělit do tří stupňů zajištěné odlišnými technickými prostředky:

1. *nízká úroveň* - tuto úroveň poskytují prostředky s omezenou mírou spolehlivosti ověření totožnosti, pro tuto úroveň je požadována minimálně jednofaktorová autentizace.
2. *značná úroveň* - tuto úroveň poskytují prostředky poskytující značnou míru spolehlivosti, pro tuto úroveň je požadována minimálně dvoufaktorová autentizace.
3. *vysoká úroveň* - prostředky nabízí vyšší míru spolehlivosti při ověřování totožnosti, pro tuto úroveň je požadováno využití takových prostředků, které chrání pro vyhotovení duplikátů a neoprávněné manipulaci.

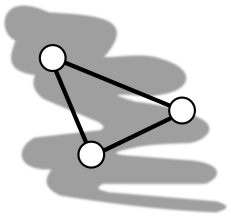
Ve výše uvedeném seznamu se objevuje několikrát pojem *autentizace*, se kterým jsme se dosud nesetkali. Autentizací rozumíme proces, kterým uživatel prokazuje totožnost systému. Z předchozí kapitoly už víme jak technicky funguje elektronický podpis (podepisování např. dokumentu) i ověření tohoto podpisu. Pro připomenutí můžeme celý postup schématicky znázornit jako na obr. 4.4.



Obrázek 4.4: Využití hashovacích funkcí při elektronickém podepisování dokumentů

V předchozí kapitole nebyla řešena jedna velmi důležitá otázka: *jak zaručit, že veřejný klíč přináleží určité konkrétní osobě?*

K takovému ověření je potřeba nezávislá třetí strana, které budou ověřit jak podepisující, tak ověřující strana. Takovou úlohu hraje Poskytovatel Certifikačních Služeb (PCS). V případě, že elektronicky podepsané dokumenty mají být právně závazné, je potřeba, aby tento PCS splňoval určitá



Bezpečné hashovací funkce
U elektronického podpisu se obvykle podepisuje pouze otisk (hash) zprávy, nikoliv zpráva celá. Jedním z důvodů je vysoká výpočetní náročnost celého procesu. Podrobnější informace o těchto funkcích můžete získat v kapitole *Bezpečné hashovací funkce* v těchto skriptech.

bezpečnostní kritéria stanovená technickými normami. Nároky jsou kladeny na PCS také z pohledu např. archivace dokumentů apod.

Proces samotného vystavování certifikátu použitelného pro generování elektronického podpisu funguje tak, že zájemce fyzicky navštíví PCS, který ověří jeho totožnost a vydá certifikát. Certifikát obsahuje data nutná ověření totožnosti uživatele. Zároveň obsahuje také data, která umožňují elektronický podpis vytvářet (privátní klíč). Za správnost těchto dat PCS ručí a je také povinen zveřejňovat pravidelně seznamy vydaných certifikátů a také seznamy certifikátů které byly revokovány (předčasně zneplatněny).

Platnost certifikátu je časově omezena, obvykle na řádově měsíce až jeden rok. Kvalifikované certifikáty s delší dobou platnosti se obvykle nevydávají.

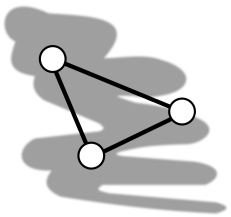
Vzhledem k vážným důsledkům, které může mít odcizení identity, což je mimochodem zločin, který se běžně stává všech vyspělých zemích a proto také u nás, jsou kladeny relativně vysoké požadavky na bezpečnost informačních systémů PCS.

Vraťme se zpět k autentizace. Jsme v situaci, kdy si uživatel pořídil certifikát od PCS. Privátní klíč z něj pak udržuje v tajnosti a může jej použít pro podepisování dokumentů. Pokud privátní klíč není žádným dalším způsobem chráněn, pak identita uživatele je prokazována prostým vlastnictvím tohoto privátního klíče. Identita uživatele je tedy prokázána pouze jediným prostředkem - odtud označení *jednofaktorová autentizace*.

Dvoufaktorová autentizace používá dva způsoby ověření totožnosti uživatele. První je stejný, jako v předchozím případě, tedy privátní klíč. Tento klíč je však navíc sám chráněn zašifrováním. K použití tedy nestačí pouhé vlastnictví privátního klíče, ale také znalost klíče, kterým se dešifruje.

U značné i vysoké míry důvěry se předpokládá použití dvoufaktorové autentizace. Rozdíl mezi nimi je však v tom, že vysoká úroveň vyžaduje použití tzv. technického prostředku, jako jsou tokeny nebo bezpečnostní karty, které samy o sobě splňují jisté bezpečnostní požadavky stanovené normami.

Příkladem takového zařízení je TokenME italské společnosti Bit4id, který nabízí v ČR certifikační autorita PostSignum. Tento produkt prošel certifikací podle standardu Common Criteria na úroveň EAL4+ (Evaluation Assurance Level) [4] a splňuje požadavky na kryptografické moduly podle FIPS 140-2 [65].



Autentizace
Podrobnější informace o problematice *autentizace* můžete získat v předmětu *Počítačové sítě a ochrana dat*, který si můžete zvolit pro studium v třetím ročníku.

Elektronický podpis

Pro různé typy elektronických podpisů jsou vyžadovány různé stupně zabezpečení. Z tohoto pohledu můžeme rozdělit elektronické podpisy na čtyři typy (se zvyšující se úrovní důvěryhodnosti):

1. prostý elektronický podpis (elektronický podpis bez přívlastku)
2. zaručený elektronický podpis (Advanced Electronic Signature (AdES))
3. zaručený elektronický podpis, založený na kvalifikovaném certifikátu
4. kvalifikovaný elektronický podpis (Qualified Electronic Signature (QES))

Elektronický podpis dle eIDAS mohou vytvářet jen a pouze fyzické osoby. Elektronický podpis je brán jako projev vůle podepisující osoby vůči podepisovanému dokumentu. Jedná se tedy o filozoficky stejný přístup jako v případě podepisování „papírových“ dokumentů.

Nejnižší úroveň zabezpečení, resp. žádnou úroveň zabezpečení poskytuje *prostý elektronický podpis*. Jako elektronický podpis slouží jakékoliv údaje připojené k podepisovanému dokumentu a používané

jako podpis. Může se jednat např. o patičku emailu.

Prostý elektronický podpis jako patička e-mailu
... tělo e-mailu ...

S pozdravem

Pavel Šenovský
Katedra ochrany obyvatelstva
Fakulta bezpečnostního inženýrství
VŠB - Technická univerzita Ostrava

Podobným způsobem může být použit naskenovaný běžný podpis přiložený k dokumentu. V obou případech není splněn ani jeden stupeň úrovně důvěry, které byly uvedeny výše. Jinými slovy nikomu nic nebrání aby vytvořil libovolný dokument a tento typ podpisu k němu připojil. Tímto způsobem podepsaný dokument proto ze své podstaty nemůže být natolik důvěryhodný, aby byl závazný (např. z hlediska vymahatelnosti takto podepsaných smluv).

To ale neznamená, že takový elektronický podpis je zcela bezcenný. Pro řadu věcí, totiž vysoké úrovně zaručené bezpečnosti není potřeba. Jako příklad můžeme použít patičku e-mailu. Řada organizací si dokonce nastavuje vlastní pravidla, jak takové podpisy mají vypadat a použití tohoto vzhledu je pak pro zaměstnance povinné. Pro běžnou e-mailovou komunikaci toto postačuje.

Podobných příkladů lze najít celou řadu - elektronický podpis na mobilní telefon kurýra předávajícího zásilku, podpis dokumentu na tablet pomocí stylusu v bance a řada dalších. Elektronický podpis ani v tomto případě sám o sobě nevytváří vysokou důvěru, ale v kontextu, v jakém jsou použity, tedy společně s procesem ověření identity kurýrem nebo bankovním úředníkem.

Zaručený elektronický podpis pro operaci podepisování používá kryptografické algoritmy. Na certifikát, pomocí kterého se operace podepisování provádí, ale nejsou kladeny žádné nároky. Takový certifikát tedy může být vygenerován jakkoliv, můžeme si jej vygenerovat také sami pomocí nástrojů jako je PGP [22] nebo OpenSSL [23].

Jelikož jsou používány kryptografické algoritmy, je podpis samotný lépe zabezpečen. Problémem v tomto případě je ověření totožnosti podepisující osoby - pokud si podepisující osoba sama může vystavit certifikát (nebyly využity služby kvalifikovaného PCS), je tento způsob podpisu bezpečnější než podpis prostý? Odpověď zní ano i ne. Pro podepsání obchodní smlouvy tento druh elektronického podpisu nevytváří dostatečně silnou důvěru. Pokud ale tento druh podpisu použijeme uvnitř firmy a oddělení IT bude vykonávat služby PCS, ale nikoliv na takové úrovni aby jej bylo možné považovat za kvalifikovaného PCS, může být relativně levně dosažena vyšší úroveň důvěry podepisovaných vnitřní dokumentů organizace.

Zaručený elektronický podpis, založený na kvalifikovaném certifikátu se liší od předchozího případu využitím služeb kvalifikovaného PCS pro vytvoření certifikátu. Za totožnost podepisující osoby tedy ručí nezávislá třetí strana (nezávislá na podepisující osobě i osobě, která provádí ověření podpisu). Důvěryhodnost kvalifikovaného PCS je zajištěna kontrolou souladu způsobu fungování PCS s legislativou i relevantními technickými normami.

Prostředek použitý pro podepisování může být ale libovolný. Není zde tedy požadavek na to, aby certifikát byl bezpečně uložen na certifikovaném tokenu nebo obdobném zařízení. Tento typ elektronického podpisu je plně v souladu s požadavky dnes již zrušeného zákona o elektronickém podpisu. Úroveň důvěry v tomto případě je z pohledu legislativy po dobu trvání přechodného období (do září 2018) stejná jako u nejvyšší formy elektronického podpisu - *kvalifikovaného elektronického podpisu.*

Zajímavostí je, že česká právní úprava se v tomto bodě rozchází se směrnicí eIDAS. Zatímco eIDAS požaduje požaduje nejvyšší úroveň důvěry (představované kvalifikovaným elektronickým podpisem, viz níže) pro všechny oficiální akty. Český právní řád tak nečiní. Nejvyšší úroveň důvěry je vyžadována pouze pro komunikaci s úřady a to oběma směry. Pokud jsou ale uzavírány smlouvy nebo podepisovány jiné dokumenty mezi sokromoprávními osobami ať už soukromníky nebo firmami, pak tato úroveň důvěry není vyžadovaná a postačuje zaručený elektronický podpis.

Toho využívají služby jako např. BankSign, která umožňuje bance podepsat smlouvu v zastoupení klienta. Tedy klient v tomto případě nemusí mít vlastní elektronický podpis. Smlouvu elektronicky podepíše banka na základě autorizace podpisu klientem s použitím ověření identity klienta pomocí bankovní identity (BankID).

Výše uvedený postup má ale některé nevýhody. U smluv totiž platí, že důkazní břemeno je na straně toho, kde není spokojen se smlouvou. Tedy toho, kdo napadá smlouvu. Pokud ale je ale elektronický

podpis pouze zaručený a logicky tak nevytváří vysokou úroveň důvěry, jaký efekt v případném soudním sporu bude takový podpis mít? Služba BankSign ještě ve finále smlouvu opatří plně kvalifikovanou elektronickou pečetí. Může být tento krok vnímán jako ten, který navýší úroveň důvěry na potřebnou úroveň. V současnosti je tedy řada otázek a také právních názorů na tuto problematiku. Co zatím není jsou judikáty, tedy rozhodnutí soudu v konkrétních kauzách o které by se dalo opřít. V právním řádu totiž platí, že autoritativní výklad práva provádí až soud.

Dle nařízení eIDAS, jsou ale požadavky na *kvalifikovaný elektronický podpis* vyšší. Pro dosažení této úrovně je nutné použití kvalifikovaného prostředku (např. tokenu). Vzhledem k nastavení legislativy je právě tento typ elektronického podpisu jako jediný použitelný pro oficiální komunikaci s úřady, popř. jiné úkony vyžadující vysoký stupeň důvěryhodnosti.

S pojmem elektronický podpis souvisí celá řada dalších pojmů.

Elektronická značka

Prvním z nich je tzv. *elektronická značka*. Tento prostředek byl upraven původním zákonem o elektronickém podpisu, nová právní úprava jej ale nezná. Elektronická značka tak nemá své místo v portfoliu oficiálně legislativou uznávaných nástrojů, může ale míst své místo pro aplikace, jejichž pravidla legislativa neupravuje.

Podívejme se tedy k čemu byla elektronická značka v minulosti využívána. Jedná se o údaje v elektronické podobě, které jsou připojeny k datové zprávě a:

1. jsou jednoznačně spojené s označující osobou a umožní její identifikaci pomocí certifikátu
2. byly vytvořeny pomocí nástrojů pro vytváření elektronický značek, které označující osoba může mít pod svou výhradní kontrolou.
3. jsou připojeny takovým způsobem, který umožní odhalit jakoukoliv následnou změnu zprávy

Naskýtá se otázka, čím se vlastně liší elektronický podpis od elektronické značky. Podle zákona se má za to, že před podpisem se podepisující osoba s dokumentem seznámila a podpisem se tak zaručuje za správnost údajů v dokumentu obsažených. Elektronický podpis je tedy chápán jako projev vůle fyzické osoby vůči podepisovanému dokumentu.

V případě elektronické značky se ale má za to, že zpráva byla označena bez předchozí kontroly obsahu zprávy - tedy něco podobného jako parafa v případě papírových dokumentů. Elektronickou značku tak obvykle používají automatizované systémy. Např. ji může použít IS pro do něj nahraný dokument, aby bylo možné zaručit, že dokument prošel, byl zpracován daným systémem.

Z technického pohledu se používají pro označování dokumentů stejné algoritmy jako v případě elektronického podpisu. Rozdíl je zde tedy v právním důsledku akce označení dokumentu.

Elektronická pečeť

Elektronická pečeť je novým nástrojem zavedeným nařízením eIDAS. Elektronickou pečetí se opět rozumí údaje připojené k dokumentu (datové zprávě), které:

1. jsou jednoznačně spojeny s „pečetící“ organizací
2. byly vytvořeny pomocí nástrojů pro vytváření elektronických pečetí, které má pečetící organizace výhradně pod svou kontrolou
3. jsou připojeny takovým způsobem, který umožní odhalit jakoukoliv následnou změnu zprávy

Elektronickou pečeť mohou využívat pouze právnické osoby (včetně organizačních složek státu). Podobně jako v případě elektronické značky i v případě elektronické pečeti je odlišný význam. Elektronická pečeť není chápána jako projev vůle, ale pouze jako specifikace původu zapečetěného dokumentu.

Elektronickou pečeť tedy organizace mohou dávat pouze na dokumenty, kterých jsou původci.

I tento posun je logický, pokud jej srovnáme s filozofií použití běžného podpisu. I v případě podepisování smluv mezi dvěma právnickými osobami akt podpisu je vykonáván fyzickou osobou, která je k tomuto úkonu zmocněna - např. statutární zástupce nebo jím zmocněná osoba.

Z technického pohledu se používají pro zapečetění dokumentů stejné algoritmy jako v případě elektronického podpisu. Rozdíl je zde tedy v právním důsledku akce zapečetění dokumentu.

Časová razítka

Kvalifikovaným *časovým razítkem* se rozumí údaje připojené k datové zpráva vydaná poskytovatelem certifikačních služeb, která spojuje zprávu s určitým časovým okamžikem.

Časové razítko je velmi důležité například pro uzavírání smluv. Smlouvu uzavíráme k určitému datu. Použití elektronických prostředků by mohlo svádět k antidatování takových smluv (nebo jiných

dokumentů). Z tohoto důvodu musí časové razítko vydávat poskytovatel certifikačních služeb, protože je nezávislý vůči podpisujícím stranám a je pod velmi přísnou kontrolou.

Poskytovatel musí ze zákona zajistit, aby čas odpovídal hodnotě koordinovaného světového času. Časové razítko si potom můžeme představit podobně jako například rádiové budíky, které se v pravidelných intervalech zachycují signál z vysílače přesného času a podle něho nastaví čas.

Velmi často je výhodné použít kombinaci časového razítka a elektronického podpisu. Použití může být např. ve formě elektronického podepsání dokumentu a aplikaci časového razítka. Tímto způsobem se dokument včetně elektronického podpisu spojí s určitým časem a je možno zkoumat, zda v té době podpis byl platný. Tedy zdali k času a datu „oražení“ dokumentu certifikát použitý k podpisu neexpiroval (neskončila jeho platnost) nebo nebyl předčasně revokován. Revokaci certifikátu lze ověřit proti seznamu revokovaných certifikátů.

Opačný postup než v předchozím případě - tedy dokument opatřit časovým razítkem a teprve následně elektronicky podepsat je také možný. Interpretace je ale rozdílná. Časová značka spojí dokument s určitým okamžikem, podepisující osoba pak získává jistotu, že podepisuje např. aktuální verzi dokumentu. Pozor v tomto případě ale časové razítko nevypovídá nic o času aktu podepsání.

Pokud jste dočetli až sem, pak Vás nepřekvapí, že pro časovou značku technicky je použit algoritmus elektronického podpisu. Ovšem s tím časovému označení se použije privátní klíč PCS a ověření pak proběhne proti jeho veřejnému klíči.

Podpisová schémata

Z předchozího textu již víme, že existuje celá řada prostředků a algoritmů, které lze elektronický podpis a obdobné služby použít. U kvalifikovaných PCS je ale jejich použití z hlediska algoritmů a jejich parametrů omezeno, aby byla zaručena dlouhodobá bezpečnost aplikací této technologie.

Kombinaci algoritmů použitelné pro elektronické podepisování a obdobné služby označujeme jako *podpisové schéma*. Schéma samotné je tvořeno:

- algoritmem elektronického podpisu,
- bezpečnou hashovací funkcí a
- paddingovou funkcí.

Algoritmy elektronického podpisu jsme se již zabývali, hashovacími funkcemi se budeme zabývat v samostané kapitole, zbývá tedy *paddingová funkce*. Paddingové funkce zajišťují služby tzv. paddingu, tedy doplnění zprávy na určitou délku. Důvodem pro použití takových funkcí jsou blokové charakteristiky ostatních funkcí podpisového schématu. To znamená, že tyto funkce vyžadují pro svou práci, aby zpráva, kterou mají zpracovat, byla beze zbytku dělitelná na bloky o určité délce.

Jelikož délka zprávy může být různá je tento požadavek zajištěn použitím paddingové funkce, která „chybějící“ část bloku doplní.

Doporučená podpisová schémata jsou obsažena v tabulce 4.4 a vycházejí ze standardu ETSI 119 312-1.4.1 (2021-08) [59]. Norma bývá revidována v pravidelných intervalech (přibližně 1x za 2 roky). Primární oblast úprav je právě v nabídce šifrovacích a SHA algoritmů a jejich doporučených parametrů. Doporučení normy vycházejí v vždy z aktuálního stavu poznání.

Tabulka 4.4: Doporučená podpisová schémata dle [59]

Podpisové schéma	**SHA**	**DSA**	**SOGIS**
SHA224-s-RSA	SHA224	RSA-PKCSv1.5	L
SHA256-s-RSA	SHA256	RSA-PKCSv1.5	L
SHA384-s-RSA	SHA384	RSA-PKCSv1.5	L
SHA512-s-RSA	SHA512	RSA-PKCSv1.5	L
RSA-PSS s MGF1SHA256 ident.	SHA256	RSA-PSS	R
RSA-PSS s MGF1SHA384 ident.	SHA384	RSA-PSS	R
RSA-PSS s MGF1SHA512 ident.	SHA512	RSA-PSS	R
RSA-PSS s MGF1SHA3 ident.	SHA3	RSA-PSS	R
SHA224-s-ECDSA	SHA224	EC-DSA	L
SHA2-s-ECDSA	SHA256, 384 nebo 512	EC-DSA	R
SHA2-s-ECDSA	SHA256, 384 nebo 512	EC-SDSA-opt	R
SHA3-s-ECDSA	SHA3-256, 384 nebo 512	EC-DSA	R
SHA3-s-ECDSA	SHA3-256, 384 nebo 512	EC-SDSA-opt	R

Senio Official Group Information Systems Security (SOGIS) v tab. 4.4 je mezinárodní dohoda která vznikla v reakci na rozhodnutí Rady Evropských Společenství o bezpečnosti informačních systémů (92/242/EHS) a doporučení Rady 95/144/EC o společných kritériích hodnocení bezpečnosti informačních technologiích. V současnosti se k dohodě připojilo 10 států[1].

Účelem je formulovat a koordinovat doporučení k užití různých technologií. Doporučení SOGIS pro podpisová schémata se vztahuje k systémům, které dané schéma podporují. Doporučení v tomto případě nabývá dvou hodnot a to L - legacy, pro dosluhující systémy a R - recommended, doporučené pro všechny ostatní.

Všimněte si, že v tab. 4.4 není obsažena informace o paddingové funkci, tedy alespoň ne přímo. Jelikož padding je spojen s DSA funkcí, je možné paddingovou funkci dohledat podle názvu použitého algoritmu elektronického podpisu. Např. RSA-PKCS v1.5 používá pevně stanovený textový řetězec, viz [62].

Pro jednotlivé algoritmy se přitom předpokládá také časově omezená použitelnost pro vystavování certifikátů. Nejexponovanějším algoritmem z tohoto pohledu je algoritmus bezpečné hašovací funkce. I tuto použitelnost definuje norma ETSI 119 312-1.4.1 (2021-08) [59] a znázorňuje ji také tabulka 4.5.

Tabulka 4.5: Použitelnost SHA algoritmů dle [59]

SHA funkce	**1 rok**	**3 roky**	**6 let**
SHA-224	A	A	N
SHA-256	A	A	A
SHA-384	A	A	A
SHA-512	A	A	A
SHA3-256	A	A	A
SHA3-384	A	A	A
SHA3-512	A	A	A

Původní verze normy obsahovaly řadu dalších bezpečných hashovacích funkcí jako SHA 1, RIPEMD-160 nebo Whirpool. Možnost použití těchto funkcí ale z nových iterací normy vypadlo a nadále tedy není doporučováno.

Časový údaj v letech je počítán od data vydání normy ETSI 119 312-1.4.1 (2021-08) [59], tedy od roku 2021. Tyto číselné údaje jsou spíše orientačního charakteru a slouží jako vodítko PCS pro volbu optimálního preferovaného podpisového schématu podle doby platnosti vydaného certifikátu. Samozřejmě nelze technicky zaručit, že třeba v příštích šesti letech nedojde k zásadnímu průlomu v SHA funkcích, který třeba zboří předpoklady bezpečnosti těchto funkcí. Znamená to spíše, že v současnosti nemáme náznaky, které by nás nutily věřit, že by se tak mělo stát a tak funkce považujeme pro toto období za bezpečné.

V tab. 4.5 jsou u jednotlivých funkcí hodnoty A (ano) a N (ne) u jednotlivých časových obdobích naznačující vhodnost, popř. nevhodnost používání daných algoritmů v daném časovém horizontu.

Z tohoto pohledu lze říci, že pro účely elektronického podepisování je možné používat pouze SHA funkce třídy 2 a 3, s tím že do roku 2025 by mělo být ukončeno používání nejslabší SHA funkce třídy 2 - SHA-224.

Kromě doporučení k použití určitých algoritmů poskytuje norma také doporučení k parametrům šifrovacích funkcí, jako třeba doporučovaná minimální délka klíče. Tyto údaje ale již pro naše potřeby jsou příliš podrobné. Zájemci je tak mohou dohledat v normě [59].

Elektronické archívy

Elektronický podpis dle eIDAS je platný (ověřitelný) po dobu trvání platnosti certifikátu použitého pro podepsání dokumentu. Obvykle je tato doba relativně krátká - do jednoho roku. Po jejím uplynutí elektronický podpis není možno ověřit. V některých případech je ale žádoucí, aby schopnost ověření trvala déle. Jedná se zejména o případy systémů, které slouží pro dlouhodobou archivaci dokumentů.

Podpis/značka v takovém případě slouží mimo jiné také k ověření toho, že archivovaný dokument nebyl pozměněn nebo poškozen. Ke změnám může dojít úmyslně nebo prostou lidskou chybou, k poškození pak může dojít třeba také v důsledku technického selhání, např. poškození sektoru na disku, v jehož důsledku nelze část dokumentu přečíst.

[1] Rakousko, Finsko Francie, Německo, Itálie, Nizozemí, Norsko, Španělsko, Švédsko a Velká Británie. Česká republika se k dohodě dosud nepřipojila.

Elektronické archívy jsou proto z mnoha pohledů velmi specifické. Problematika vedení elektronických archívů není nová a existují technická řešení. Například National Aeronautics and Space Administration (NASA) se zabývá problematikou elektronického archivnictví někdy od roku 1966. Je také zakládajícím členem Consultative Committee for Space Data Systems (CCSDS) (založen 1982). Tato organizace se zabývá příjímáním standardů souvisejících s výzkumem vesmíru. Jeden z těchto standardů, konkrétně CCSDS 650.0-M-2: Reference Model for an Open Archival Information System (OAIS) [2], také označovaný jako magenta book[2], se zabývá právě problematikou archivací dokumentů a také archivnictvím obecně.

Tento standard byt také v roce 2003 byl dokument vydán jako ISO 14721:2003 [10]. Cílem je navrhnout systém archivace dat jak v elektronické podobě, tak v podobě „papírové“, tak aby data byla přístupná cílové skupině uživatelů. K dosažení tohoto cíle vymezuje i organizační schémata jako souhrn lidí a pravidel pro archivaci odpovědnost a proces poskytování dat z archívu.

Jedná se tedy spíše o stanovení filozofie archivování než konkrétní návod se stanovením technologií k použití. Finální aplikace musí přitom mít funkce archívu a zároveň používat transparentní metody elektronického podepisování s dlouhodobou platností (např. podle ETSI TS 101 733 [7]). Zajištění právní vymahatelnosti dokumentů nebude možné bez dalších legislativních změn, které se však v současné době nepřipravují.

Zapamatujte si

Je třeba si uvědomit možnosti elektronického podpisu a způsobu jakým je jeho použití upraveno zákonem. V zásadě totiž existují dva druhy elektronického podpisu - takový, který je oficiální, lze ho použít pro komunikaci s úřady, podepisování smluv tedy splňující požadavky zákona. Pro certifikační autoritu zavádí zákon přívlastek *kvalifikovaná*.

Potom existují certifikační autority, které používají stejné nebo podobné algoritmy elektronického podpisu, nicméně se nesnaží splnit všechny požadavky zákona a prováděcích vyhlášek. Takový elektronický podpis samozřejmě není z právního hlediska použitelný např. pro uzavírání smluv, ale lze jej výhodně využít například v rámci podniků pro zvýšení bezpečnosti komunikace jeho zaměstnanců.

4.8 Bezpečné hašovací algoritmy

Hašovací funkce slouží k vytváření tzv. Message Digest (MD) jednotlivých souborů. Jedná se o matematické, jednoscestné funkce jejichž výsledkem je řetězec, unikátní pro každou zpracovávanou zprávu. Cílem je získat možnost ověřit, že zpráva, jejíž MD vlastníme, nebyla pozměněna. Message digest tedy můžeme přeneseně považovat za otisk prstu zprávy.

Samotný proces ověřování se provádí jednoduše tak, že se ze zprávy vygeneruje nový MD a ten je srovnán s MD původní.

Svou koncepcí vychází ze starších algoritmů pro vytváření kontrolních součtů (CRC). Problémem těchto algoritmů byla možnost jejich snadného pozměnění textu zprávy, aniž by došlo ke změně výsledného kontrolního součtu. Moderní hašovací funkce proto využívají metod typických pro šifrování. Možnost objevení dvou různých zpráv, které mají stejný výsledný MD samozřejmě nelze úplně vyloučit, u bezpečného algoritmu je však krajně nepravděpodobné. Možnosti vytvoření dvou zpráv mající totožný haš nazýváme *kolize*.

Z hlediska bezpečnosti použití platí, že nemůžeme používat takový algoritmus, který není odolný vůči kolizím. Případě, že algoritmus neobsahuje nějaké zneužitelné zranitelnosti, lze odvodit bezpečnost tohoto algoritmu z počtu průchodů algoritmem (pokusů), které je nutné provést pro získání dvou zpráv se stejným výsledným MD. Bezpečnost je tedy odvozena od počtu operací, které je nutno provést pro prolomení bezpečnosti a získání kolizní zprávy. Tuto bezpečnost, někdy označovanou taktéž jako tzv. *bits of security*, vypočteme takto (4.13):

$$p = 2^{\frac{m}{2}} \tag{4.13}$$

kde p maximální počet výpočtů MD pro nalezení zprávy mající hledaný MD a m délka výsledného hashe (MD) v bitech

[2] označení je odvozeno z barvy přebalu normy

Všimněte si konstrukce vzorce. Bezpečnost je odvozena od velikosti hashe (MD). Tato velikost je pro daný algoritmus vždy konstantní. Proto např. MD funkce SHA-512 bude mít vždy délku 512 bitů bez ohledu na to jak dlouhá je původní zpráva. Složitost prolomení je tedy pro daný algoritmus konstantní. Bezpečnost tak bude záviset na volbě algoritmu.

Když to porovnáme s obdobným výpočtem pro šifrování, zjistíme, že tam je situace jiná. Bezpečnost je odvozena of dvou veličin a to konkrétně velikosti použité abecedy a délky klíče. Abeceda je více méně neměnná, ale délku klíče si je možné zvolit. Bezpečnost tak závisí na volbě algoritmu a také na volbě jeho parametrů.

Bezpečnost hašovacích algoritmů zkoumáme z dvojího pohledu (tedy hovoříme o dvou typech kolizí):

1. z pohledu hledání dvou libovolných různých zpráv, které mají stejný haš,
2. z pohledu hledání zprávy s konkrétním hašem.

Rozdíl mezi těmito dvěma přístupy je jasně viditelný na tzv. narozeninovém paradoxu. **Narozeninový paradox** říká [40]: *pokud je v místnosti 23 nebo více lidí, je více než padesátiprocentní šance, že nejméně dva z nich mají narozeniny ve stejný den.* Ve skutečnosti se nejedná o logický paradox, protože toto tvrzení je velmi lehce odvoditelné, spíše se jedná o paradox z pohledu prvotní úvahy většiny lidí, kteří se nad tímto problémem zamyslí.

Vysvětlení můžeme nalézt uvažováním inverzního problému - tedy, že žádný z přítomných lidí nemá narozeniny ve stejný den jako jiný (viz 4.14).

$$p'(n) = 1\left(1 - \frac{1}{365}\right)\left(1 - \frac{2}{365}\right)\cdots\left(1 - \frac{n-1}{365}\right) \tag{4.14}$$

kde n počet lidí v místnosti

Pravděpodobnost, že se v místnosti nacházejí dva lidé se stejným dnem narozenin (4.15)

$$p(n) = 1 - p'(n) \tag{4.15}$$

Pokud tedy hledáme dvě libovolné zprávy, které mají stejný haš, tak je to podobně jako pro hledání dvou libovolných lidí s narozeninami ve stejný den, jedná se o nesrovnatelně jednodušší problém k řešení než hledání zprávy, která má jeden konkrétní haš (člověka který se narodil v určité datum).

Bezpečnost hašovacího algoritmu je proto přímo odvislá od délky výsledného haše, tak jak stanovuje rovnice 4.13. Velikost haše nám stanovuje prostor, který je nutné prohledat, abychom narušili bezpečnost daného algoritmu. Oba typy kolizí přitom vedou k odlišným aplikacím. Např. pokud pro daný algoritmus získáme schopnost generovat generovat různé zprávy, které nudou vést na stejný hash (kolize prvního typu), bude to znamenat, že takový algoritmus nebude možné nadále používat pro účely elektronického podpisu. Na druhou stranu takový algoritmus bude možné stále ještě bezpečně používat jako náhradu šifrování hesel, tedy např. pro účely autentizace uživatele do systému.

Prolomení bezpečnosti hašů hesel vyžaduje kolize druhého typu, jejichž dosažení je obvykle řádově náročnější.

Z praktického hlediska ale obvykle platí, že pokud se začne přibližovat teoretická možnost dosažení kolizí prvního typu, daný algoritmus je považován jako bezpečnostně zbořený a hledají se další algoritmy, které by jej mohly nahradit... s lepšími bezpečnostními vlastnostmi.

Jaké tedy mohou být aplikace bezpečných hašovacích funkcí?

1. ověření integrity souborů nebo obecně datových přenosů - provádí se tak ze uživatel porovná vypočtený a stažený MD
2. výše uvedený postup je také použitelný pro kontrolu integrity souborů na disku - pokud se MD souboru změnil, musel se změnit podkladový soubor. V tomto případě se porovnává vypočtený MD s MD uloženým v minulém období
3. jako náhrada za heslo – v autentizační databáz se pak neukládá heslo v čitelné ani zašifrované podobě, ale pouze jeho MD. Po zadání hesla uživatelem se vypočte MD a porovná se s MD uloženým.
4. Součást elektronického podpisu (a obdobných aplikací) – umožňuje zjistit, dokument opatřený elektronickým podpisem nebyl nijak změněn
5. a řada dalších

V současné době existuje řada algoritmů, které se pro generování MD využívají, a některé z nich tady představím podrobněji. Bude se jednat především o algoritmy MD2, MD4 a MD5 vyvinuté firmou

RSA a SHA vyvinutými na MIT. Česká vyhláška pro použití elektronického podpisu také umožňuje využití algoritmu RIPEMD-160 autorů Hanse Dobbertina, Antoona Bosselaerse a Barta Preneela. Tyto algoritmy se liší jednak délkou generovaného MD (čím větší tím bezpečnější) i použitím různých technik ochrany.

Hašovací algoritmy MD2 – MD5, stejně jako SHA-1 byly přijaty organizací IETF jako RFC doporučení defacto standardy pro celosvětovou síť internet. První dokument RFC se objevil v roce 1969. Tehdy RFC dokumenty plnily funkci diskusní platformy rostoucí komunity kolem sítě Advanced Research Projects Agency Network (ARPANET) (předchůdce Internetu) o síťových protokolech a technologiích na ARPANET použitých.

4.8.1 MD2 - 5

MD algoritmy mají společné to, že upraví vstupní zprávu na určitou délku, pro kterou je v několika „kolech“ vypočítán MD. Výsledkem, je řetězec pevné délky, která je určena použitým algoritmem.

Zpracování tedy probíhá v pěti krocích:

1. doplnění zprávy na normalizovanou délku,
2. doplnění kontrolního součtu zprávy,
3. iniciace bufferu na počáteční hodnotu,
4. zpracování zprávy a
5. zaznamenání výsledku.

Z hlediska moderního návrhu hašovacích funkcí je přelomová *MD4*, která posloužila jako základ návrhu SHA-1 i RIPEMD. Novátorským principem je zde tzv. více-kolový systém.

Na každý blok zprávy se použije několik předem definovaných funkcí. Tímto způsobem se autoři celého algoritmu snažili znesnadnit statistickou analýzu výsledku těchto funkcí a tedy zabránění nalezení jiné zprávy mající stejně MD bez nutnosti provést p-výpočtů.

Závěry výzkumů z poslední doby ukazují, že délka haše 128 bitů, kterou využívají algoritmy MD2 – MD5 již nelze považovat za zcela bezpečné. Již v roce 1994 pánové Paul van Oorschot a Mike Wiener dokázali [69], že při investici 10 miliónů dolarů je možné sestavit počítač, který mohl dvě zprávy se stejným MD najít během měsíce. Přitom autoři očekávali, že náklady by se každých 18 měsíců snížily na polovinu.

Už v roce 1995 se ale ukázalo, že taková investice nebude vůbec nutná, protože algoritmus samotný obsahuje závažné zranitelnosti, které proces útoku výrazně zjednodušují a tím pádem také zrychlují. Tento útok zpracoval a také posléze publikoval německý kryptoanalytik Hans Dobbertin [55] napadl všechny tři kola zpracování MD4 . Na běžném PC by útok na MD4 trval řádově několik sekund. MD4 se ovšem v době publikování už nepoužívalo - neboť o bezpečnosti tohoto algoritmu měly určité pochybnosti samotní autoři algoritmu, proto jej záhy nahradili o něco pomalejší, ale také výrazně bezpečnějším algoritmem MD5.

V roce 1996 Dobbertin publikoval úvahy o možném řešení MD5 aplikací stejných postupů, které použil pro prolomení MD4. Myšlenky Dobbertina, Orschota a Wiesnera dále rozvedli Číňané Xiaoyun Wang, Dengguo Feng and Xuejia Lai a Hongbo Yu [83] prokázali, že MD5 je skutečně nebezpečné a je možné najít během několika hodin dvě zprávy se stejným hashem. Proti způsobu, jakým autoři MD5 napadli nejsou imunní ani další hashovaní funkce jako je SHA-0, RIPEMD a HAVAL-128.

Počátkem roku 2006 přispěl k řešení této problematiky i Vlastimil Klíma [63], který čínský útok dále urychlil až pod jednu minutu na průměrném testovacím notebooku.

4.8.2 SHA

Definován ve standardu NIST FIPS 180-4 Secure Hash Standard (SHS) [34]. Tento standard specifikuje hašovací algoritmy pro SHA-1, SHA-224, SHA-256, SHA-384 a SHA-512. Aby se rozlišily generace algoritmu je SHA-1 někdy označováno také jako SHA třídy 1 a obsahuje pouze jedinou SHA funkci SHA-1. Oproti tomu, SHA třídy 2 obsahuje řadu funkcí SHA-224, SHA-256, SHA-384 a SHA-512

Standard 180-4 [34] byl sice aktualizován v roce 2012, jednalo se však o změny spíše kosmetické. Největší změny zavedl FIPS 180-2, který umožnil používat SHA třídy 2, které zahrnují algoritmy SHA-224, SHA-256, SHA-384 a SHA-512), zatímco původní norma umožňovala použití pouze algoritmu SHA-1.

Oproti srovnatelnému algoritmu MD5 je délka výsledného haše 160 bitů u SHA-1 a u ostatních algoritmů SHA ještě delší, z tohoto hlediska je tedy algoritmus SHA bezpečnější. Je však potřeba

dodat, že všechny v současnosti normalizované algoritmy SHA filozoficky vycházejí z MD4, proto všechny také do určité míry trpí jejími neduhy, které činí z jejich bezpečnosti spornou otázku. Z tohoto důvodu také NIST ve spolupráci s NSA vypsal soutěž na SHA třídy 3, jejichž algoritmus by měl být razantně odlišný a algoritmus by tak neměl být zranitelný stejným typem útoků jako starší SHA algoritmy. Tuto soutěž vyhrál algoritmus *Keccak* a v roce 2015 byl tento algoritmus zveřejněn jako součást standardu FIPS PUB 202 [66].

Podobně jako SHA-2 SHA-3 obsahuje také řadu různých algoritmů, konkrétně: SHA3-224, SHA3-256, SHA3-384, SHA3-512 a funkce SHAKE128 a SHAKE256. SHA-3 byl navržen pro přímou náhradu funkcí SHA-2. Všimněte si, že délka výsledných hašů je v případě obou tříd totožná. Předpoklad je takový, že v případě objevení závažných zranitelností v SHA-2 přenastaví se systémy tak, aby místo SHA-2 funkcí volaly funkce SHA-3.

V současnosti (půlka roku 2022) však SHA-3 není v praxi příliš používána. Jednou ze známějších aplikací je nasazení v ověřovacím protokolu kryptoměny Ethereum.

Všechny stávající algoritmy lze rozdělit z hlediska průběhu funkce do dvou etap *preprocesing* a *výpočet haše*. V rámci preprocesingu se připravuje zpráva podobným způsobem jako u algoritmů MD (doplnění zprávy, iniciace počátečních nastavení). Při výpočtu haše se vytvoří message shedule a ten je pak použit spolu s funkcí, konstantami a operacemi s textovými bloky k iteračnímu vygenerování série haš hodnot.

Algoritmy jsou iterační, jednocestné hašovací funkce, které zpracují zprávu a vytvoří její MD. Algoritmy se přitom liší počtem bitů (bits of security), dále se liší délkou zpracovávaných textových bloků, které jsou užity v procesu hašování.

Tabulka 4.6: Vlastnosti hašovacích algoritmů SHA

třída	**algoritmus**	**délka zprávy [v bitech]**	**velikost bloku**	**velikost slova**	**velikost MD**	**bits of security**
SHA-1	SHA-1	$<2^{64}$	512	32	160	80
SHA-2	SHA-256	$<2^{64}$	512	32	256	128
	SHA-384	$<2^{128}$	1024	64	384	192
	SHA-512	$<2^{128}$	1024	64	512	256
SHA-3	SHA3-224	-	1152	-	224	112
	SHA3-256	-	1088	-	256	128
	SHA3-384	-	832	-	384	192
	SHA3-512	-	576	-	512	256

Aplikací čínského útoku (viz. část věnována funkcím MD) došlo zatím k zmenšení složitosti útoku na algoritmus SHA-1 ze 2^{80} na 2^{69}, v roce 2015 pak pak komplexita útoku poklesla na $2^{57,5}$ [74]. Z kryptografického pohledu je tedy SHA-1 prolomena a proto se použití tohot algoritmu nedoporučuje. Algoritmus SHA-1 již byl také vyřazen z doporučených bezpečných hashovacích funkcí používaných v rámci podpisových schémat kvalifikovaných PCS. V průběhu let 2016 a 2017 také přestane většina WWW prohlížečů označovat webová sídel podepsaná certifikátem založeným na tomto algoritmu jako bezpečná.

Řešením je přechod na SHA třídy 2 (SHA-256 a vyšší), zejména pak SHA-512, kde větší délka výsledného haše poskytuje stále ještě vyšší záruku bezpečnosti.

Srovnání parametrů funkcí rodiny SHA je dostupné v tabulce 4.6.

4.8.3 RIPEMD-160

RIPEMD-160 [9] vychází z koncepce RIPEMD hashovacího algoritmu, který vznikl v rámci projektu Evropské unie Race Integrity Primitives Evaluation (RIPE) a reaguje na slabiny původního algoritmu, které objevil začátkem roku 1995 Hans Dobbertin. Zvyšuje délku výsledného hashe na 160 bitů a zvyšuje také počet kol.

Geografická oblast využití se omezuje zejména na státy Evropské unie a státy o vstup usilující. V USA je preferovaný algoritmus SHA. Na základě podrobné analýzy MD4 vznikl posílený algoritmus, který byl nazván RIPEMD.

RIPEMD se v zásadě skládá z dvou paralerních MD4, s dalšími vylepšeními v oblasti bitových operací a změnou pořadí slov zprávy. Jinak v zásadě zůstává algoritmus MD4 zachován, včetně výsledné délky hashe 128 bitů.

Po útoku Dobbertina v roce 1995, který našel slabiny ve dvou kolech algoritmu ze tří, začalo být jasné, že bude nutné algoritmus upravit. Dalším důvodem pro úpravu byla i možnost útoku hrubou silou viz. závěr podkapitoly věnované MD2 – MD5. 128 bitů v dnešní době neposkytuje záruku dostatečné bezpečnosti.

RIPEMD v žádné verzi v současnosti není součástí podpisových schémat kvalifikovaných PCS. Používání těchto algoritmu se již v praxi nedoporučuje.

4.8.4 WHIRPOOL

Funkce Whirpool má za sebou zajímavý vývoj. Byla navržena v roce 2000 Vincentem Rijmenem a Paulem S. L. M. Barettem, kteří ji přihlásili do výběrového řízení pořádaného v rámci projektu NESSIE, který funguje v rámci programu Information Society Technologies (IST) Evropské komise. Cílem projektu NESSIE je napomáhat standardizaci kryptografických primitiv a fungovat tak podobným způsobem pro Evropskou unii jako NIST pro USA.

Součástí tohoto projektu bylo i výběrové řízení pro hašovací funkce, které mělo mít podobný charakter jako výběrové řízení NIST pro výběr AES. Bohužel do výběrového řízení byla přihlášena pouze hašovací funkce Whirpool. Tato funkce logicky byla vybrána a posléze zavedena jako jeden z doporučovaných algoritmů do revidovaného normy ISO/IEC 10118-3:2004 [11].

Z hlediska implementace je zajímavé, že tato hašovací funkce používá vnitřní 512-bitovou blokovou šifru W.

Zpráva je doplněna tak, že na konec se doplní 1 (bit), potom x krát 0 (bit) a 256-ti bitové číslo reprezentující délku původní zprávy. Nuly se doplňují tak, aby celková délka zprávy byla dělitelná beze zbytku na 512-ti bitové bloky m1, m2, . . . ,mn.

Jednotlivé bloky jsou použity pro generování pracovních hodnot haše $H_0, H_1, \ldots, H_n$. Přičemž H_0 je před započetím práce iniciováno na 512 nulových bitů.

Pro výpočet H_i je využita blok zprávy mi, který je zašifrován pomocí šifry W s H_{i-1} jako klíčem. Na zašifrovaný blok zprávy je aplikována operace XOR s H_{i-1} a m_i. H_t je hledaný výsledek hašovací funkce Whirpool.

Celkově se jedná o hašovací funkci velmi bezpečnou. V současné době neexistují poznatky, které by vedly k jakémukoliv oslabení bezpečnosti této funkce.

4.8.5 Doporučení k použití bezpečných hašovacích funkcí

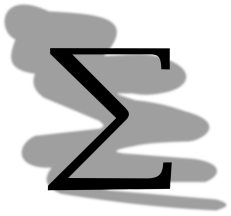
V současné době se používá několik desítek různých hašovacích algoritmů. Z hlediska zákona o elektronickém podpisu však můžeme použít pro vytváření plně kvalifikovaných certifikátů pouze některé algoritmy

1. SHA-2 (256, 384, 512) a
2. SHA-3 (224, 255, 384, 512)

Pro algoritmy SHA-1, RIPEMD-160 a Whirpool ačkoliv nedošlo k úplnému prolomení jejich bezpečnosti, se doporučuje přechod k odolnějším algoritmům s delším výsledným hašem.

Z SHA algoritmů jsou doporučovány zejména algoritmy SHA-512 a SHA3-512, jehož délka „bits of security“ poskytuje nejvyšší šanci na bezpečnost.

V současnosti platné normy však připouštějí použití i výpočetně méně náročných algoritmů, jako je SHA-256.



Shrnutí

Šifrování je staré jako písmo samo. Z hlediska techniky šifrování rozlišujeme dva typy šifrovacích algoritmů: *symetrické* a *asymetrické*.

Symetrické používají k zašifrování a dešifrování zprávy stejný klíč. Asymetrické naopak používají jiný klíč pro zašifrování a jiný pro dešifrování, využívá se pro to matematické příbuznosti obou klíčů.

Elektronický podpis a asymetrické šifrování jsou příbuzné, u obou se využívá dvojice klíčů a některé algoritmy (např. RSA) umožňují jak šifrovat tak podepisovat. U elektronicky podepisovaného dokumentu postupujeme tak, že vezmeme svůj soukromý klíč a použijeme jej na zprávu (nebo její haš), taková zpráva je ověřitelná pouze pomocí našeho veřejného klíče – za to, že veřejný klíč přináleží určité osobě, odpovídá poskytovatel certifikačních služeb.

Asymetrické šifrování má za cíl chránit zprávu, před přečtením nepovolanou osobou, proto postupujeme opačně. Pro zašifrování zprávy použijeme veřejný klíč příjemce, zpráva je pak dešifrovatelná pouze s použitím privátního klíče – ten si každý uživatel tohoto typu šifrování udržuje v tajnosti.

Časová razítka, elektronické pečetě a elektronické značky taktéž využívají postupů algoritmů elektronického podpisu. Elektronická značka se od podpisu liší právními důsledky - el. podpisem potvrzujeme (ručíme za) správnost dokumentu, el. značkou potvrzujeme, že nám dokument prošel rukama. Elektronická pečeť je určena organizacím a potvrzuje původ dokumentu. Časové razítko zase generuje nezávislá autorita časových razítek - je to jediný způsob jak zajistit prokazatelné ukotvení dokumentu v čase.

Bezpečné hašovací funkce jsou velmi důležitou avšak obvykle širokou veřejností ignorovanou problematikou. Na bezpečnosti těchto funkcí je založena bezpečnost elektronického podpisu, hesel apod. Výsledkem činnosti těchto funkcí je otisk zprávy, který je s vysokou pravděpodobností unikátní pro danou zprávu.

Kontrolní otázky

1. Proč nemůžeme substituční šifry v dnešní době považovat za bezpečné?
2. Jaký je rozdíl mezi symetrickým a asymetrickým šifrováním?
3. Popište postup použití privátního a veřejného klíče pro asymetrické šifrování.
4. Které bezpečné hašovací funkce je možné použít pro kvalifikovaný elektronický podpis v ČR?
5. K čemu slouží bezpečné hašovací funkce?

Správné odpovědi

1. Protože nemění frekvenční charakteristiky textu.
2. Symetrické šifrování používá jeden klíč pro zašifrování i dešifrování, asymetrické šifrování používá různé klíče pro šifrování a dešifrováni.
3. Veřejný klíčem příjemce se zpráva zašifruje a privátním klíčem příjemce se dešifruje.
4. SHA třídy 2
5. Využití v rámci elektronického podpisu, náhrada šifrování hesel, kontrola integrity souborů ...

Test

1. Je možné za splnění určitých podmínek považovat použití kódů za bezpečné?
   (a) Ano
   (b) Ne
2. Skytale byla
   (a) Substituční šifra
   (b) Známý kód
   (c) Šifrovací pomůcka
3. Který z následujících algoritmů lze použít pro asymetrické šifrování i elektronický podpis?
   (a) RSA
   (b) DSA
   (c) ECDSA
4. Podpisové schéma tvoří
   (a) DES, paddingová funkce, SHA
   (b) DSA, paddingová funkce, SHA
   (c) DEA, paddingová funkce, SHA
5. Elektronický podpis je ověřitelný
   (a) Stále
   (b) Po dobu jednoho roku
   (c) Po dobu platnosti certifikátu

Správné odpovědi
1. a), 2. c), 3. a), 4. b), 5. c)

Kapitola 5

Úvod do počítačových sítí

Náhled kapitoly
V rámci této kapitoly se podíváme na základy problematiky počítačových sítí, zejména jaká zařízení na síti fungují a jakou plní funkci. Podíváme se také na specifika návrhu menších (domácích) sítí.

Po přečtení kapitoly budete
Vědět

1. jaké jsou vrstvy sítě
2. jaká zařízení se na síti vyskytují a jakou funkci plní

Čas pro studium
Pro prostudování této kapitoly budete potřebovat přibližně 4 hodiny.

5.1 Rozdělení sítí

Počítačové sítě je možné dělit podle celé řady různých kritérií, např.:

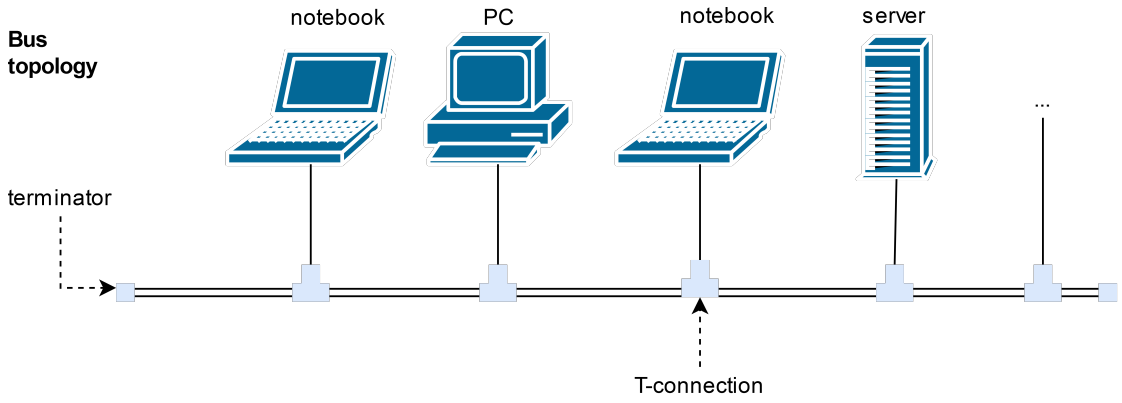
- topologie
- charakteru komunikace
- oblasti, kterou síť pokrývá
- apod.

Topologií sítě se rozumí způsob, jakým jsou jednotlivé počítače do sítě zapojeny. Historicky topologií vznikla celá řada:

- sběrnicová
- sítě typu token ring (zapojení „do kruhu“
- hvězdicová topologie
- hybridní topologie (např. stromové)

Sběrnicová topologie je z dnešního pohledu, jako síťová topologie, překonaná (alespoň ve své čisté podobě). V rámci této topologie se koncová zařízení připojují ke sběrnici. Vizuálně si lze tuto topologii představit jako na obr. 5.1.

Tento typ zapojení vyžaduje použití kabeláže, která tento typ zapojení umožňuje - obvykle se jedná o koaxiální kabel. Z tohoto kabelu se pomocí T-spojek provádějí odbočky pro jednotlivá koncová zařízení. Na obou zakončeních sběrnice je pak hlavní kabel zakončen tzv. terminátory, jejichž účelem je pohlcování volných signálů pohybujících se v síti.

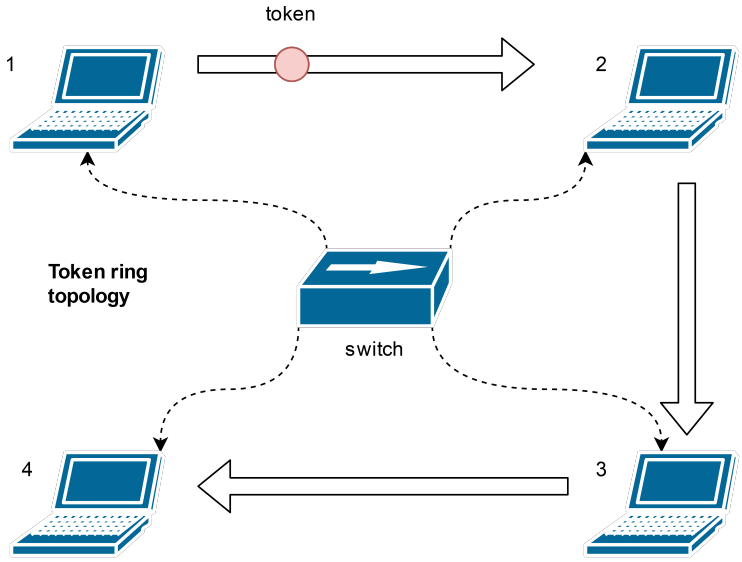


Obrázek 5.1: Sběrnicová topologie počítačových sítí

Použití koaxiálního kabelu s sebou nese relativně malé přenosové rychlosti na sítích této topologie. Dalším problémem je také závislost na sběrnici jako takové - pokud dojde k přerušení kabelu dojde také k omezení dostupnosti sítě na počítačích tento kabel využívající.

Tyto dva faktory vedly k tomu, že pro účely realizace sítí, se koaxiální kabeláž ani sběrnicová topologie již nevyužívají. Koaxiální kabel ale své využití má, např. pro účely vedení antén.

Sítě typu **token ring** jsou z hlediska topologie zajímavé. Vizuálně si je lze představit jako na obr. 5.2. Na první pohled by se mohlo zdát, že tento typ zapojení je prostou adaptací sběrnicové topologie, jenomže tomu tak není, protože zapojení do kruhu není fyzické, ale logické - je tedy implementováno softwarově, zatímco fyzicky je tato síť zapojena v *hvězdicové topologii* (viz níže).



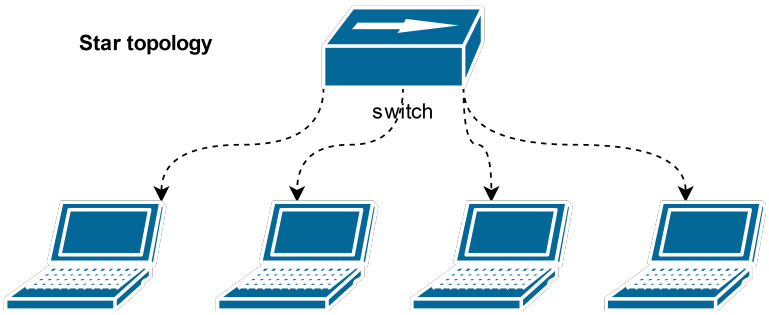
Obrázek 5.2: Topologie počítačových sítí token ring

Fungování těchto sítí si lze představit tak, že určíme zdroj komunikace na síti a na jeho umístění položíme značku (token). Tuto značku postupně posunujeme v kruhu (ring) ve směru hodinových ručiček po jednotlivých počítačích v síti, až dojdeme k cíli komunikace.

Postup v kruhu je ale z hlediska efektivity síťového provozu poměrně problematický, proto se v praxi spíše používá hvězdicová topologie, popř. topologie hybridní.

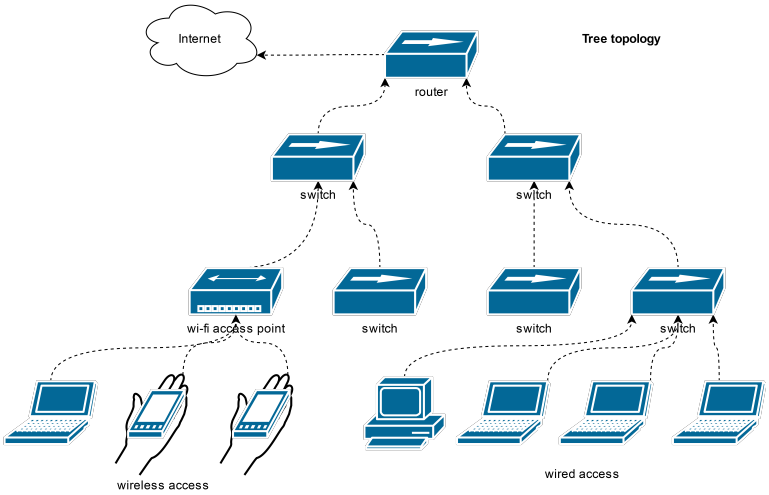
Vizuálně je možné si **hvězdicovou topologii** představit podobně jako na obr. 5.3.

V centru zapojení hvězdicové topologie je aktivní síťový prvek jako např. switch nebo router (viz podkapitola Síťová architektura ISO/OSI) a k němu jsou připojena jednotlivá další síťová zařízení. Připojení je realizováno pomocí dedikované (nesdílené) kabeláže. K tomuto účelu se obvykle využívá kabeláž známá pod názvem kroucená dvojlinka (twisted pair).



Obrázek 5.3: Hvězdicová topologie počítačové sítě

Hybridními topologiemi rozumíme kombinaci více typů topologií v rámci jediné sítě. Nejčastěji uváděným zástupcem tohoto typu topologií je *stromová topologie*, která kombinuje na nejnižší úrovni hvězdicové zapojení, aktivní prvky sítě jsou ale zapojovány pomocí sběrnicové topologie (pomocí zařízení hub nebo switch). Účelem hybridních topologií je umožnit stavbu rozsáhlejších sítí. Zjednodušený příklad je dostupný na obr. 5.4.



Obrázek 5.4: Stromová (hybridní) topologie

V síti tak vzniká několik úrovní switchů. Požadavky na ně, ale budou výrazně odlišné. Switche na nejnižší úrovni budou obhospodařovat datový provoz pouze z a do koncových zařízení. O úroveň výše ale switche budou obhospodařovat komunikaci ze všech switchů, které jsou do něj koncentrovány, což na ně kladě řádově větší nároky. Takové zařízení tak musí být mnohem výkonnější a logicky také dražší.

Při volbě topologie lze také výše uvedenou architekturu použít pro zodolnění sítě vůči výpadku některého ze switchů. To se zajišťuje tak, že switch na nižší úrovni je připojen ke dvěma switchům (místo jednoho, jak je naznačeno na obr. 5.4). V případě výpadku jednoho z nich pak bude automaticky zastoupen switchem druhým.

Stromová topologie je tak také nástrojem pro zajištění kvality síťování v organizaci.

Podle oblasti, kterou síť pokrývá je možné typově sítě rozdělit na sítě:

- Local Area Nework (LAN)
- Wide Area Network (WAN)
- Metropolitan Area Network (MAN)
- kontinentální
- celosvětové apod.

Nejčastěji používaným pojmem z výše uvedených jsou sítě **LAN**. Jedná se tzv. lokální sítě. Lokálností se v tomto případě rozumí fakt, že síť je fyzicky realizována v jedné budově nebo areálu - tedy

na jednom místě pro organizaci nebo domácnost. Sítě **WAN** jsou jiné - nikoliv nutně po technologické stránce, ale fyzickou lokací sítě.

Sítě WAN zasahují mnohem větší plochu než sítě LAN. Společným prvkem zůstávají použité technologie a vlastnictvím/užitím sítě jedinou organizací. Pomocí WAN sítí se řeší problém vzájemného propojení sítí geograficky vzdálených lokací. Dobrým příkladem může být naše univerzita - její hlavní kampus je v Porubě, Ekonomická fakulta (alespoň ještě v roce 2022) a Fakulta bezpečnostního inženýrství jsou ale fyzicky v odlišných částech města. Každá odlehlá lokace proto realizuje vlastní LAN síť a tyto sítě jsou pak propojeny do rozsáhlejší WAN sítě.

Propojování odlehlejších lokací může být realizováno různým způsobem, lze využít veřejné infrastruktury telefonního vedení (např. pro připojení pomocí ADSL nebo VDSL), pokud není požadována vysoká přenosová kapacita. V opačné případě lze propojení realizovat pomocí optických kabelů. Často je navíc v síti mezi takovými vzdálenými lokalitami síťový provoz analyzován pomocí systémů Intruder Detection System (IDS), Intruder Prevention System (IPS) popř. pomocí firewallů nové generace, které nabízejí také IDS/IPS funkcionalitu.

Tímto způsobem je možné včas detekovat, popř. i zabránit šíření virových infekcí nebo propagaci útoku hackerů mezi jednotlivými lokalitami organizace.

Sítě **MAN** je možno do určité míry připodobnit k veřejným infrastrukturám typu vodovody, kanalizace apod. M v názvu MAN znamená metropolitní, tedy infrastruktura budovaná městy. Ta si od budování takových sítí slibují obvykle zvýšení atraktivity pro větší investory, kteří se mohou na takovou síť velmi rychle připojit a získat tak vysokorychlostní připojení k Internetu, samozřejmě za úplatu. Fyzicky jsou takové sítě realizovány pomocí optických kabelů a nebo zřizováním Wi-Fi hot spotů. Organizačně města budování a provoz takových sítí řeší zřízením dceřiných firem (s plným vlastnictvím města). Např. v Ostravě funguje tímto způsobem společnost Ova.net [24].

Podívejme se jaké nabízí služby, abychom získali lepší představu o účelu a funkci tohoto typu sítí:

- poskytování přípojení k internetu domácnostem pomocí Wi-Fi (do rychlosti 20 Mbps)
- poskytování přípojení společnostem a jiným organizacím s pomocí Wi-Fi nebo optiky s garantovanými rychlostmi do 100 Mbps
- pro velké společnosti nebo organizace mohou být parametry připojení nastaveny odlišně (obvykle nejprve vyžaduje položení nové trasy optiky)
- telefonní služby společnostem nebo organizacím
- služby call center
- budování kamerových systémů
- provoz a údržba městského kamerového systému
- budování sítí pro společnosti a organizace

Představitelem **kontinentálních** sítí je např. síť CESNET2, rozvíjena sdružení CESNET. Jeho hlavním úkolem je výzkum v oblasti a vývoj v oblasti informačních a komunikačních technologií. Síť CESNET2 [3], viz obr. 5.5, propojuje pomocí vysokorychlostního připojení vzdělávací a výzkumné instituce v ČR a je připojena k podobně řešeným sítím zahraničím, zejména sítí GÉANT, kterou lze považovat za evropskou páteř výzkumu, vývoje a vzdělávání.

Typickým představitelem celosvětové sítě je pak Internet.

5.2 Kabeláž sítí

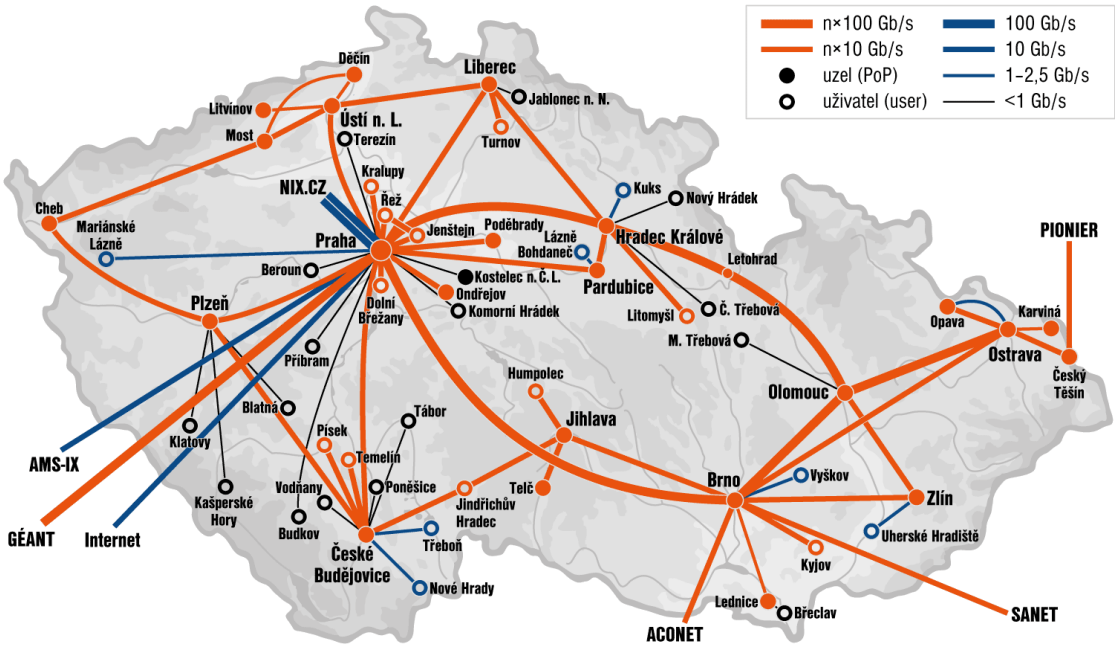
Schématické znázornění nejčastěji používaných typů kabeláže je dostupné na obr. 5.6.

Začít výklad můžeme u kabelu **koaxiálního**, tento kabel se v praxi pro konstrukci počítačových sítí již nepoužívá. Přesto se s ním lze setkat, zejména ve formě antén a také kabeláže analogových kamerových systémů. Signály jsou kabelem vedeny pomocí elektrických impulzů vedených měděným jádrem kabelu. Vzhledem k útlumu signálu je možná délka kabeláže omezená. Toto omezení se liší podle služeb, pro které bude kabel využíván a také použitím různých variant kabelu.

Koaxiální kabely se dodávají ve dvou variantách:

- tenké a
- tlusté

V tomto případě označení tlustý a tenký skutečně odpovídá tloušťce kabelu. Tlustší varianta má přibližný dosah 500 m a tenčí pak přibližně polovinu.



Obrázek 5.5: Topologie sítě CESNET2, stav v roce 2018 (převzato z [49])

Kabel typu **kroucená dvojlinka** (twisted pair) vede signál kabelem s měděným jádrem, tedy svým způsobem podobně jako v případě koaxiálního kabelu. Rozdíl je v tom, že v rámci kabelu není veden pouze jediný vodič, ale 8. Kabely jsou propleteny vždy po dvojicích, odtud pochází také název, kroucená dvojlinka. Kabel tedy tvoří 4 dvojice vodičů (viz obr. 5.6). Zkroucení kabelů není samoúčelné, ale plní velmi důležitou funkci, zmenšuje totiž přeslechy mezi jednotlivými kabely a omezuje též elektromagnetické vyzařování kabelu do okolí.

Z hlediska použití se jedná v současnosti o nejpoužívanějším síťový kabel. Použití více kabelů má své výhody ve výrazném navýšení rychlosti datových přenosů, zároveň ale kabel neumožňuje vytváření odboček - vždy bude vést signál mezi přesně dvěma zařízeními.

I tento typ kabeláže se dodává v několika různých variantách. Základní členění je mezi variantou nestíněnou (Unshielded Twisted Pair (UTP)) a stíněnou (Shielded Twisted Pair (STP)). Stíněná varianta se vyznačuje výrazně nižší úrovni vyzařování kabelu, tato vlastnost je však vyvážena vyšší cenou takového kabelu.

Kabeláž tohoto typu je možno také dělit podle tzv. *kategorie*. Kategorie se označuje CatX, kde X představuje číslo kategorie. Vyšší čísla v pořadí odpovídají novějším a proto také rychlejším kategoriím kabeláže. Z hlediska nasazení jsou používány v současnosti především kabely Cat5e, Cat6 a Cat6a.

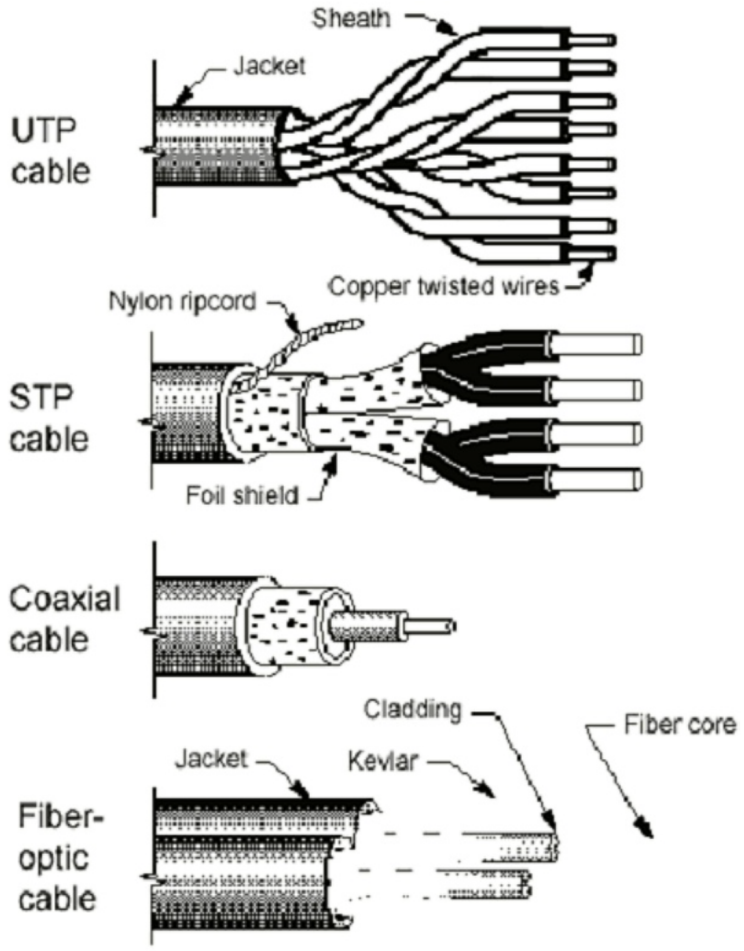
Kabely kategorie 5e jsou schopny zajistit přenosové rychlost až 1 Gb/s na vzdálenost 100 m. Tento kabel se používal především v minulosti a proto má také opravdu velký počet instalací. Pro nové instalace jsou používány především kabely Cat6 nebo dnes již spíše Cat6a.

oba kabely umožňují díky svým specifikacím dosáhnout řádově vyšších přenosových rychlostí a to až 10 Gbps. Oba kabely se ale liší maximální vzdáleností, na kterou jsou tuto rychlost schopny zajistit. V případě Cat6 je to 55 m, zatímco pro kabel Cat6a je to až 100 m.

Uvedených rychlostí je možno ale dosáhnout pouze v případě, že na obou stranách komunikace jsou zařízení, které takové přenosové rychlosti jsou schopny dosahovat. Z toho hlediska lze ale říci, že kabeláž představuje infrastrukturu, která nebude měněna tak často. Může být proto výhodné instalovat rychlejší kabeláž, byť je o něco málo dražší, s tím, že v budoucnu umožní plně využít nabízené přenosové kapacity. Investor se ale tímto způsobem vyhne úzkému hrdlu, do jehož odstranění by v budoucnu musel investovat. Jinými slovy lze předpokládat, že s postupem času jednotlivá koncová zařízení nabízeným přenosovým rychlostem „dorostou“.

Výše uvedené typy kabeláže nejsou jediné, proto pro úplnost doplňujeme přehled v tab. 5.1.

Posledním typem kabeláže, kterou se v této podkapitole budeme zabývat jsou **optické kabely**. Tento typ kabeláže se od předchozích výrazně liší, protože nepřenáší elektrické impulzy, ale impulzy světelné. Přenosové rychlosti, stejně jako maximální délka kabelu, jsou proto výrazně vyšší.



Obrázek 5.6: Nejčastěji používané typy kabeláže v počítačových sítích (převzato z [77])

Tabulka 5.1: Typy kabeláže, použití koncovky, rychlosti a délky

kategorie	**rychlost [Gb/s]**	**délka [m]**	**koncovka**	**použití**
Cat5	0,1	100	RJ-45	v budovách
Cat5e	1	100	RJ-45	v budovách
Cat6	1	100	RJ-45	v budovách
	10	55	RJ-45	v budovách
Cat6a	10	100	RJ-45	v budovách
Cat7	10	100	GG45	sdělovací technika
Cat8	40	30	RJ-45	datová centra

Optické vlákno samotné má průměr 8 - 10.5 µm, s ochranným pláštěm je pak na průměru přibližně 125 µm. Velmi malá tloušťka a relativně příznivá cena umožňuje, aby vlákno nebylo pokládáno samo, ale ve svazcích. Vzhledem k tomu, že mezi jednotlivými vlákny nevznikají interference mohou být v jednom svazku desítky, stovky nebo dokonce tisíce vláken.

I v případě použití optické kabeláže dochází k určitému útlumu signálů, vzhledem k tomu, že signály jsou v tomto případě světelné, je možno překlenout relativně velké vzdálenosti. Opět pro různé typy služeb se doporučují různé maximální délky kabelu, pro většinu služeb se jako bezpečná vzdálenost uvádí 50 km.

Hlavní použití kabeláže je pro překlenutí velkých vzdáleností - předpokládá se proto, že kabel bude tažen vně budov. Kabel je obvykle tažen v zemi.

O tomto typu kabeláže lze také říci, že tvoří páteř vysokorychlostního internetu.

5.3 Síťová architektura ISO/OSI

Upozornění
Tato podkapitola není z hlediska použité terminologie úplně korektní. Aby se autor vyhnul některým pokročilejším tématům (např. vysvětlování toho jak vypadá packet apod.), byl text zjednodušen až na samotnou „hranu“. Cílem této kapitoly je seznámit čtenáře primárně se základními síťovými zařízeními a jejich funkcí. Pro podrobnější informace o problematice lze doporučit např. server *Svět sítí* [77] nebo články na specializovaných serverech, např. [44].

Jedním z nejznámějších popisů síťové architektury je tzv. *referenční model ISO/OSI*. Tento model vznikl jako snaha o standardizaci síťové architektury. Ačkoliv proces standardizace se nepodařilo dotáhnout do úplně zdárného konce, je tento přístup v podstatě dodržován (s určitými odchylkami).

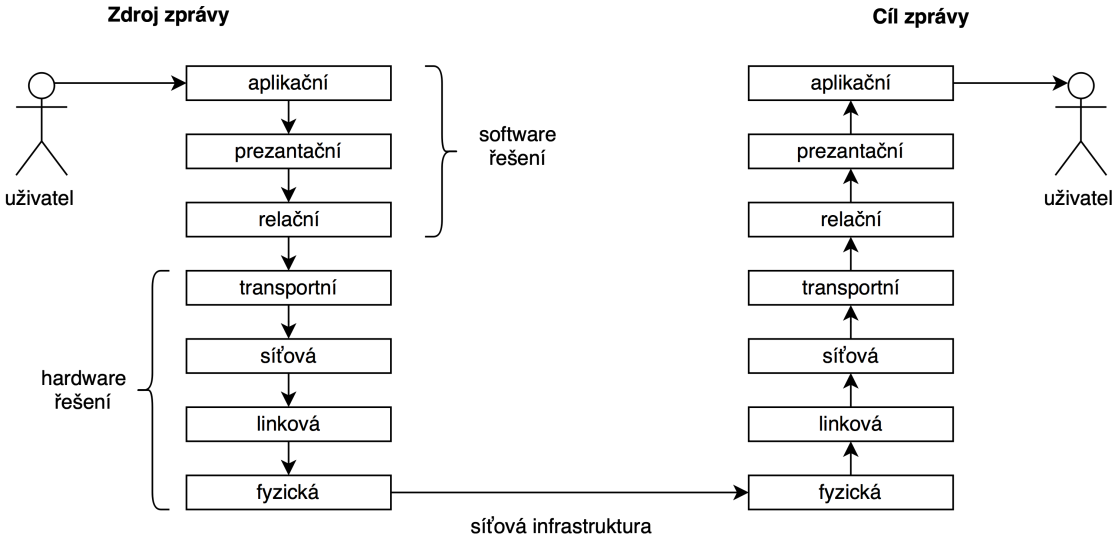
Referenční model se skládá ze sedmi na sebe navazujících vrstev:

1. fyzická
2. linková
3. síťová
4. transportní
5. relační
6. prezentační
7. aplikační

Vrstvy 1 - 4 jsou exaktně definovány a výrobci síťových zařízení tyto definice poměrně přesně dodržují. Důvod odhalíme relativně jednoduše při pohledu na seznam vrstev, první vrstvy jsou spojeny s více s hardware. Odchylky v jejich realizaci by proto mohly snadno způsobit nekompatibilitu mezi zařízeními - zařízení na síti by prostě nemohla vzájemně komunikovat a to je samozřejmě nepřijatelné.

Zbylé tři vrstvy jsou spojeny spíše se síťovými protokoly, implementace protokolů různých výrobců se mohou v určitých aspektech lišit. Této vlastnosti lze dokonce využít pro tzv. *computer fingerprinting* (snímání otisku prstů počítače). Metoda funguje tak, že na cílový počítač se vyšle určitý požadavek a analyzuje se způsob jak vzdálený počítač na takový požadavek zareaguje. Jelikož odchylky v implementacích protokolů jsou známé, lze takto odhadnout např. jaký operační systém, popř. v jaké verzi na počítači pracuje. Tento postup funguje obecně i pro programy, které nejsou součástí operačního systému, ale poskytují síťové služby.

Nyní se zaměřme na jednotlivé vrstvy modelu. Fungování vrstev nejprve znázorníme společně, viz obr. 5.7.



Obrázek 5.7: Komunikace v síti - pohled referenční model ISO/OSI

Jak z obr. 5.7 vyplývá, každý požadavek uživatele vyžadující síťovou komunikaci se propaguje

operačním systémem od aplikace směrem k hardware, který pošle požadavek pomocí připojené síťové infrastruktury. Na straně příjemce se postupuje analogicky, ale popačně, tedy směrem od hardware interpretujícího požadavek nahoru až do aplikační vrstvy, která jej vyřídí.

Fyzická vrstva zajišťuje bitový přenos dat mezi zařízeními připojenými k síti. Na tuto vrstvu zařazujeme různé typy modemů, síťových karet apod., které toto připojení fyzicky zajišťují. Kromě toho, na této vrstvě fungují některá specializovaná zařízení, která mají svůj význam pro stavbu sítě jako takovou. Do této skupiny patří *repeatery* (opakovače)[1] a *huby* (rozbočovače).

Úkolem **repeaterů** je, jak naznačuje jejich název, zopakovat přenášený signál. Z výkladu o síťových kabelech již víme, že v kabeláži dochází k postupnému útlumu signálu se zvětšující se vzdáleností, kterou signál musí urazit. Z hlediska délky kabelu jsme proto omezeni. Repeater přijme signál, posílí jej a pošle dál. Z hlediska funkcí se tedy jedná o zařízení jednoduché, které je relativně levné, pracuje v reálném čase.

Huby neboli rozbočovače slouží pro propojování jednotlivých uzlů na síti. Pomocí hubu lze vyřešit problém použití různých typů kabelů (např. kroucená dvojlinka a optický kabel), jedná se také o základní prostředek pro hvězdicovou topologii sítě. Funguje tak, že signály přijaté na kterémkoliv portu jsou posíleny a přeposlány na zbývající porty (tedy dále do sítě). Zařízení připojená k hubu, pro která není komunikace určena je budou ignorovat - ozve se zpět pouze zařízení, kterému byla komunikace určena.

Z hlediska praktického se ale od jejihc použití postupně upouští, jelikož přeposílání komunikace do všech portů představuje neúměrně vysoké zatížení sítě, zejména tam, kde je do sítě zapojeno větší množství zařízení ... a to jsou dnes více méně všechny sítě. Alternativu k použití hubu představují zařízení typu *switch*, tato zařízení fungují ale až o úroveň výše na linkové vrstvě počítačové sítě.

Linková vrstva sítě zajišťuje přístup k přenosovému médiu a je odpovědná také za adresaci na fyzickém spojení. Na této vrstvě se pracuje s adresou, která je spojena přímo s hardware - tzv. MAC adresou (Media Access Control (MAC)). MAC adresa se skládá ze dvou částí - identifikátoru výrobce a sériového čísla zařízení. Tato adresa by proto měla být unikátní a to celosvětově.

Na úrovni linkové vrstvy pracují zařízení důležitá pro architekturu sítě, jedná se o zařízení typu *bridge* (můstek) a *switch* (přepínač), na který jsme narazili již při výkladů významu hubů.

Switch v zásadě vypadá vizuálně velmi podobně jako hod (viz obr. 5.8) a plní také podobnou funkci. Tím ale, že funguje o úroveň výše v síťové architektuře, může pracovat s větším množstvím informací a tak může pracovat také inteligentnějším způsobem. Jak je z obr. patrné, hlavním vizuálním prvkem jsou síťové porty, v tomto případě je jich 48. Z hlediska počtu portů se dodávají switche s počtem portů obvykle v násobcích osmi (tedy 8, 16, ..., 48). Počet 48 portů již lze pro praktické nasazení možno považovat za mezní. Výjimku tvoří malé switche určené pro segment SOHO, kde se dodávají také 4-portové switche.

Obrázek 5.8: Switch Cisco Catalyst 2950

V čem je tedy switch lepší než hub? Výhodou je, že si switch vytváří automatizovaně určitou představu o architektuře sítě - komunikaci proto nemusí přeposílat na všechny aktivní porty, ale pouze tam, kde předpokládá, že se nachází cílové zařízení komunikace. Tímto způsobem se výrazně omezí síťový provoz aniž by utrpěla kvalita datových přenosů na síti.

Další výhodou je, že switch pracuje transparentně. Transparentností rozumíme to, že z hlediska funkce sítě se jedná o zařízení, které nemění data jím procházející, funguje automatizovaně a proto není potřeba v rámci komunikace switch adresovat (přímo oslovovat). Pro zařízení fungující na vyšších vrstvách počítačové sítě je tak switch prakticky neviditelný - nemusí se starat o to jak funguje.

[1] v praxi se používají spíše anglické názvy zařízení, než jejich české ekvivalenty

Zařízení typu **bridge** slouží pro propojení (přemostění) různých sítí nebo jejich segmentů. Můstek musí mít povědomí o tom, zda adresát komunikace je v „jeho“ segmentu nebo ne. Tuto představu si vytváří transparentně na základě síťového provozu, který přes něj prochází. V případě, že adresát komunikace není v segmentu, ze kterého tato komunikace vzešla přepošle bridge komunikaci do všech připojených segmentů sítě.

Opět se tedy nejedná o příliš „inteligentní“ zařízení. Z hlediska praktického nasazení proto často nahrazováno buďto pomocí switchů nebo routerů.

Síťová vrstva zajišťuje adresaci v rámci sítě s více segmenty, Adresa je v tomto případě logická (není proto spojena přímo s hardware např. síťové karty). Nejčastěji používaným protokolem na této vrstvě sítě je *IP protokol*. Tento protokol je v současnosti používán ve dvou různých verzích, konkrétně IPv4 a IPv6. Hlavním rozdílem (ale ne jediným) mezi nimi je vzhled a počet IP adres, se kterými může protokol pracovat.

IPv4 adresa se skládá ze čtveřice čísel v intervalu 0 - 255 oddělených tečkami. Adresa samotná vypadá následovně např., 148.196.200.15. IPv4 tedy umožňuje použití 2^{32} (4 294 967 296) adres. Aby komunikace na síti fungovala, musí být zajištěno, aby použité IP adresy byly na síti unikátní - tedy neopakovaly se. V případě, že by se na síti vyskytly dvě různá zařízení se stejnou IP adresou, došlo by k tzv. konfliktu IP adres, který by se prakticky vyřešil tak, že první (dříve) připojené zařízení do sítě by tuto adresu mohlo používat a všechna další mají smůlu a zůstala by tedy bez připojení do sítě.

Prudký rozvoj Internetu jasně ukázal, že počet IP adres poskytovaný IPv4 je absolutně nedostatečný - definitivní řešení bude představovat až přechod na IPv6. Předtím, než se trošku podíváme na novější IPv6, se podívejme ještě na některé adresy IPv4, popř. jejich rozsahy, které mají speciální význam.

Např. adresa 127.0.0.1 je tzv. *loopback adresa* - tedy adresa odkazující se sama na sebe. Existuje také několik rozsahů IP adres sloužících pro tzv. *privátní sítě*. Privátní sítí rozumíme síť, která je neveřejná, tedy její jednotlivá koncová zařízení nemají veřejnou IP adresu. To znamená, že může existovat stovky sítí využívající stejné (privátní) IP adresy a přesto to nevyvolává síťové konflikty. Pokud takové zařízení ale má mít přístup na Internet nemůže se k němu připojit přímo, ale pouze prostřednictvím dalšího zařízení, jako je např. sítová maškaráda (NAT) apod.

Rozsahy adres privátních sítí jsou definované standardem RFC 1918 [25]:

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

IPv6 adresa je tvořena osmi čtveřicemi čísel v šestnáctkové soustavě. IPv6 adresa by proto mohla vypadat následovně: fdce:9f6a:0995:0000:0000:0000:0000:0047. Prakticky to znamená, že k dispozici je 2^{128} adres, což je počet z dnešního pohledu nevyčerpatelný. IPv6 má ale také řadu dalších užitečných vlastností reagujících na změny ve způsobu využívání sítí:

- jumbo packety - podpora pro efektivní přenos větších souborů, popř. streamování
- podpora pro elektronické podepisování jednotlivých uzlů v síti (mělo by tak být obtížnější pro útočníka vydávat se za jiné zařízení)
- podpora šifrování komunikace
- a řada dalších

Výrazná odlišnost IPv6 od IPv4 způsobuje ale, že přechod je pomalý, a není bezproblémový. Proto protokoly IPv4 i IPv6 v současnosti fungují „vedle sebe“, což rozhodně není úplně ideální. Ukončení provozu IPv4 je přitom v nedohlednu.

Na síťové vrstvě pracují **routery** (směřovače). Jedná se o zařízení, která mají jisté povědomí o architektuře sítě, tedy kde se co nachází, a snaží se směřovat síťový provoz tak, aby byl co možná nejefektivnější. Oproti zařízením typu bridge tedy nerozesílá komunikaci do všech připojených segmentů sítě, ale pouze tam, kde se skutečně nachází cílové zařízení.

Je zajímavé, že pro některé routery jsou označovány také jiným názvem - konkrétně *gateway*, tedy brána. Toto označení se někdy používá pro routery, které se starají o směřování síťové komunikace mezi sítí LAN a jejím okolím. Funkčně není mezi běžným routerem a gateway rozdíl - jedná se tedy spíše o historickou záležitost.

transportní vrstva zajišťuje spolehlivost přenosu dat po síti dle požadavků vyšších vrstev architektury ISO/OSI. V rámci této vrstvy sítě se poskytují dva druhy služeb a to tzv. *spojové* a *nespojové* služby.

Spojovými službami rozumíme takové, které zajišťují spolehlivost datových přenosů - jinými slovy obsahují kontrolu kvality síťové komunikace. Jde tedy o to, že spojová služba zajistí navázání spojení, odeslání a příjem dat a kontrolu toho, zda byla přijata všechna požadovaná data, a že přijatá data jsou v pořádku, např. že nebyla poškozena po cestě. Typickým představitelem protokolu spojových služeb je *TCP*.

Nespojové služby se oproti tomu vůbec nestarají o kvalitu spojení, tím pádem ale odpadá určitá režie. Datové přenosy po síti tak mohou být rychlejší. To je zajímavá vlastnost, protože stále větší část našich životů a aktivit je realizována na Internetu a tak požadavky na datové přenosy všech možných typů poměrně prudce, dlouhodobě rostou.

Typickým představitelem nespojových služeb je protokol *UDP*. Nad tímto protokolem mohou na vyšších vrstvách síťové architektury fungovat fungovat další protokoly, popř. programy, které UDP budou využívat. Z protokolů lze zmínit např. HTTP/3 (v současnosti podporuje většina web browserů, podpora na straně serverů je ale problematická), nebo Bittorent.

Použitím nespojových služeb se nemusíme nutně zcela vzdát kontroly kvality datového přenosu, tuto kontrolu pouze nevykonáváme na této vrstvě sítě. Kontrolu kvality proto v takovém případě nejčastěji přesunujeme až na úroveň aplikací.

Spojová vrstva zajišťuje pravidla pro navázání a ukončování datových přenosů mezi uzly sítě. Příklady protokolů fungujících na spojové vrstvě, se kterými se lze setkat v praxi jsou:

- Network File System (NFS) . používá se na síťových datových úložištích
- SQL - jazyk pro manipulaci s relačními databázemi
- Remote Procedure Call (RPC) - protokol starají se o manipulaci se vzdálenými zařízeními, např. nástroj vzdálená plocha využívá RPC.
- apod.

Pro protokoly pracující na spojové vrstvě je typické, že signalizují stav připojení, jsou schopné předávat příkazy, hlásit výsledek (ať už formou dat nebo chybového hlášení).

Prezentační vrstva je zodpovědná za formátování a syntaxi dat. Jde o to, že v různých kulturách se dělají věci různě. Vezměme si takovou banální věc jako je číslo. V ČR bychom číslo tisíc s dvěma desetinnými čísly mohli napsat třeba takto 1.000,00 nebo takto 1 000,00, ale v USA by zápis vypadal spíše 1,000.00 nebo 1 000.00. Tedy zatímco u nás se používá symbol desetinné čárky v USA se používá desetinná tečka, zatímco u nás se používá jako oddělovat tisíců tečka, v USA je to čárka. Takových rozdílů je obrovské množství v datech, v používaných písmenech (diakritika), speciálních znacích apod.

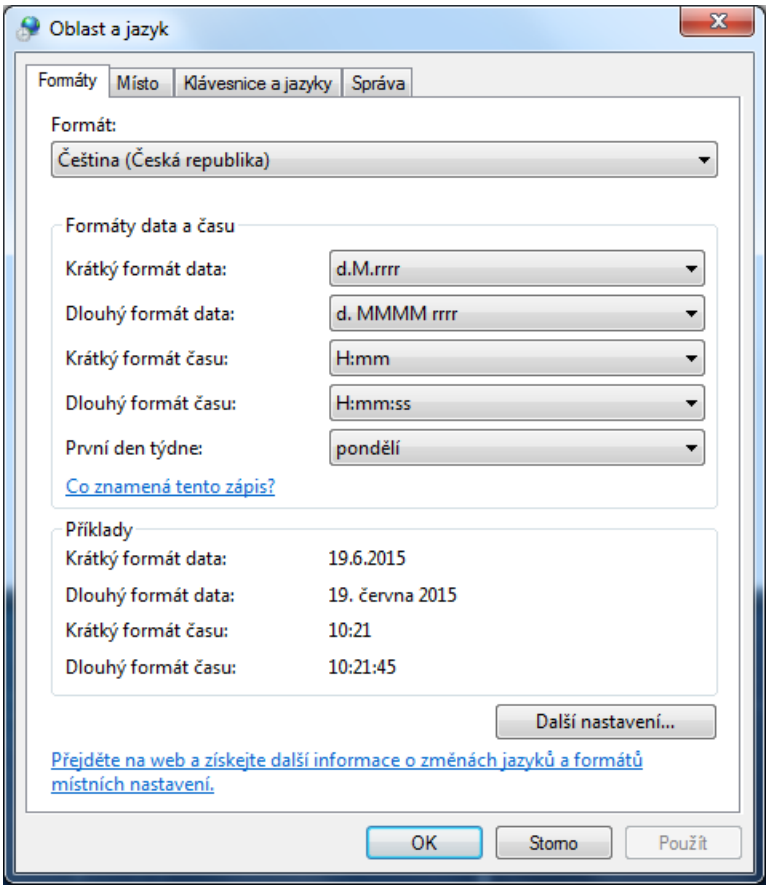
Tyto rozdíly nevznikly přes noc - jsou výsledkem dlouhodobého vývoje jazyků. Problémem je, že počítače nejsou vnitřně navrženy tak, aby se dokázaly s takovými rozdíly samy vypořádat. Uznávají pouze jednu definici čísla, data apod. Prezentační vrstva se proto stará o překlad údajů v těchto striktních definicích do podoby lokální specifik a zpět. O tento úkol se obvykle stará samotný operační systém. Ve Windows toto nastavení najdete například v Ovládacích panelech - Oblast a jazyk, viz obr. 5.9.

Na prezentační vrstvě mohou také nastat některé problémy v kompatibilitě. Tyto problémy vznikají tak, že tvůrce programu předpokládá použití určité specifické znakové sady nebo formátu čísel a nepočítá s tím, že např. existují státy, kde se nemluví anglicky (nebo japonsky nebo ... dosaďte jiný více či méně oblíbený exotický jazyk). Takové problémové programy je často možno zprovoznit změnou nastavení formátu čísel nebo data, pokud jej tedy nutně musíte použít.

U **aplikační vrstvy** již pracujeme s běžnými aplikacemi, které nějakým způsobem pracují se sítí.

5.4 Ostatní síťová zařízení

Kromě síťových zařízení, kterými jsme se zabývali v předchozí podkapitole, na síti funguje celá řada dalších zařízení, o kterých byste měli mít určité povědomí. Pravděpodobně nejdůležitějším zařízením je *server*. Serverem rozumíme počítač, který je nastaven tak aby poskytoval na síti určité služby. K serveru se pak dálkově připojují další počítače - *klienti* a tyto služby využívají.



Obrázek 5.9: Nastavení formáty data a čísel ve Windows 7

Nejdůležitější informace ze sítí
V této kapitole jsme toho probrali velké množství, ačkoliv všechny informace obsažené v textu jsou relevantní, některé jsou přece jenom důležitější než jiné. Věnujte proto obzvláště velkou pozornost zařízením typu: switch, router, protokolům IP a TCP (TCP/IP) a funkci prezentační vrstvy.

Servery lze členit podle různých kritérií, např. podle použitého operačního systému, jelikož prostor těchto skript je poměrně omezený zaměříme se na jiný druh členění - podle typů služeb, které server provozuje. Z tohoto pohledu lze rozlišovat:

- databázové servery
- WWW servery
- souborové
- tiskové
- aplikační
- atd.

Tento typ rozčlenění je potřeba chápat jako do určité míry umělá. Technicky totiž nebrání nic tomu, aby jedno zařízení (server) neplnil všechny výše uvedené úlohy. K samostatnému řešení výše uvedených služeb nás vede především snaha provoz těchto služeb lépe zabezpečit a také je lépe škálovat.

Lepším zabezpečením máme na mysli především to, že lze mnohem lépe specifikovat okruh uživatelů, kteří budou využívat službu, a také způsob užití serveru - zmenší se tak prostor zneužitelný pro případnou kompromitaci serveru pomocí malware nebo útokem hackera. Škálovatelností rozumíme přizpůsobení výkonu počtu požadavků uživatelů. Službu z tohoto pohledu lze provozovat na jediném serveru nebo v případě potřeby zátěž rozložit na serverů více (např. cluster serverů).

Pro zvýšení efektivity provozu jednotlivých serverů se v poslední době extenzivně využívá tzv. *virtualizace*. Virtualizace umožňuje vytvoření specializovaných virtuálních strojů provozovaných na jednom fyzickém serveru. Hardwarové prostředky serveru jsou v takovém případě rozloženy mezi jednotlivé virtuální servery podle konfigurace a jejich aktuálního zatížení.

To umožňuje, aby jednotlivé virtuální stroje byly konfigurovány minimalisticky z pohledu poskytovaných služeb, což je považováno za dobrou praxi z pohledu bezpečnosti a zároveň nevyžaduje po provozovateli investici do většího množství fyzických serverů.

Nyní už blíže k jednotlivým typům serverů. **Databázový server** se stará o poskytování služeb systému řízení báze dat. Česky to znamená že klientům poskytuje data a umožňuje také jejich pořízení/editaci/výmaz. K tomuto účelu obvykle využívá jazyka SQL, o kterém jsme se zmínili již v předchozí podkapitole.

Jako představitele databázových serverů lze uvést např.:

- open source databázové servery
  - MySQL
  - PostgreSQL
  - a další
- proprietální databázové servery
  - Oracle
  - MS SQL Server
  - DB2
  - a další

WWW server poskytuje WWW stránky nebo jiné zdroje dostupné pomocí protokolu http nebo jeho šifrované varianty https. WWW stránky přitom mohou být *statické* (ve formátu html nebo xhtml) - v takovém případě jsou poskytovány jako jiné zdroje dostupné na Internetu (např. obrázky nebo videa) a nebo mohou být *dynamické*. Dynamičnost WWW stránky spočívá v tom, že obsah stránky se vygeneruje dynamicky pomocí skriptu na serveru, obvykle s využitím databázového backendu na základě požadavku který byl na server zaslán.

O spuštění a management výsledků skriptů se stará právě WWW server. V současnosti nejpopulárnější WWW servery jsou:

- Apache
- MS Internet Information Service
- Ngix

Souborové servery poskytují svým uživatelům prostor na disku - tento prostor se také někdy označuje jako disková kvóta. Souborové servery mohou být realizovány různě - mohou poskytovat WWW rozhraní pro manipulaci se soubory, pomocí FTP/FTPs nebo mohou využívat některý z protokolů pro mapování síťových zdrojů (např. ve Windows SMB). Mohou, ale také nemusí, být integrovány se systémy řízení identity uživatelů na síti. Integrace v tomto případě umožňuje „inteligentní“ přidělování diskových kapacit jednotlivým uživatelům nebo jejich skupinám podle rolí, které v organizaci zastávají.

Existují specializovaná zařízení, která se zaměřují pouze na poskytování diskových služeb. Taková zařízení často označujeme jako Network Attached Storage (NAS). Taková zařízení umožňují domácnostem, malým a středním firmám efektivně spravovat relativně velké diskové kapacity. Představu o vzhledu NAS si lze udělat z obr. 5.10.

Disková kapacita NAS je zajištěna použitím řady disků konfigurovaných do podoby Redundant Array of Independent Disks (RAID). Pro domácí použití často stačí použití dvou disků v konfiguraci RAID-1 pro zajištění zrcadlení disků. V takové konfiguraci může jeden z disků selhat aniž by se to jakkoliv projevilo na dostupnosti dat. Z důvodu efektivity se ale častěji používají konfigurace RAID-5 (min. 4 disky) nebo RAID-6 (min. 5 disků), které poskytují možnost zotavení se ze ztráty 1 (RAID-5) nebo 2 (RAID-6) disků. Tato schopnost je vykoupena snížením dostupné diskové kapacity pole o výše uvedený počet disků. Tato kapacita je totiž vyčleněna na ukládání paritních informací, které slouží pro rekonstrukci dat způsobených selháním disku.

Nastavování zařízení se obvykle děje pomocí WWW rozhraní.

Úkolem **tiskového serveru** je spravovat tiskárny a jejich tiskové úlohy. Použití tiskového serveru má tu výhodu, že správa tiskáren je centralizovaná, to umožňuje:

Obrázek 5.10: 6-ti diskový NAS TVS-671 společnosti QNap (převzato z: [28])

- nastavovat, kdo a na jaké tiskárně (popř. kdy) může tisknout
- lepší diagnostiku problémů s tiskárnami
- kontrolu vytíženosti tiskáren
- implementaci nástrojů pro monitoring nákladů spojených s tiskem
- a další

Použití tiskových serverů tedy představuje velmi efektivní nástroj umožňující efektivní správu všech aspektů použití tiskáren v organizace.

Aplikační server slouží pro zprostředkování aplikační logiky klientským počítačům. Co přesně to znamená? Klasické programy (tzv. thick (tlustý) klient) jsou provozované celé na klientském počítači. Tedy veškerá programová logika se provádí na běžném PC uživatele. Tento způsob práce je, dalo by se říci, tradiční, je s ním ale spojena řada nevýhod, zejména v okamžiku kdy takových klientů organizace provozuje stovky nebo tisíce a všechny je musí udržovat. Jakákoliv změna v aplikační logice si v takovém případě vyžádá provedení změn (distribuci upraveného programu) na všech klientských počítačích. Provedení takových změn je ale časově i finančně náročné. Nejedená se přitom nutně pouze o nutnost provedení změn v souvislosti s přidáním nějaké nové funkčnosti, ale také běžné údržby, podpory nových zařízení, opravy chyb apod.

Použití aplikačního serveru tyto problémy řeší pomocí konsolidace aplikační logiky na jednom místě - serveru. Na straně klienta zůstává pouze logika jeho přístupu k aplikační vrstvě na serveru. Veškeré změny v aplikační logice včetně oprav budou tak centralizované na serveru - řešíme tedy pouze jejich distribuci na server. Po provedení jeho aktualizace je nová verze programu dostupná okamžitě všem klientům.

Vzhledem ke způsobu fungování označujeme takové klienty často jako tzv. tenké. Nejčastěji je pro realizaci takového klienta používán webový prohlížeč, který uživatel použije aby se připojil k serveru. Aplikace je mu pak servírovaná pomocí webového rozhraní.

Na síti se nachází také celá řada dalších zařízení, které plní různé funkce, některá z nich tady proto ještě zmíníme. První z nich je Dynamic Host Cache Protocol (DHCP). DHCP je služba běžící na serveru, která se stará o přidělování IP adres klientským počítačům. Toto přidělování probíhá dynamicky, což znamená, že IP adresa se přiděluje na dobu určitou (hodiny až dny podle nastavení), a že adresa IP pro jednotlivé počítače v síti obvykle není stálá - mění se dynamicky podle toho, které IP adresy jsou právě k dispozici.

DHCP využívá toho, že v praxi je velmi nepravděpodobné, aby v jeden okamžik byla zapnuta všechna zařízení, která se v dané organizaci mohou připojit k síti. Vzniká tak určitý prostor pro to, aby organizace mohla manipulovat s relativně malým počtem veřejných IP adres pro větší množství

zařízení. To je klíčová vlastnost počítačových sítí pracujících na bázi protokolu IPv4, jelikož již víme, že počet adres, které tento protokol má k dispozici, je značně omezený.

V protokolu IPv6 je sice podpora DHCP přítomna, ale jeho význam je menší a plní trošku odlišné úlohy.

Pro použití WWW (a nejenom jej) je klíčové použití **DNS** (Domain Name Server (DNS)). Úkolem DNS je zajistit překlad adresy IP na tzv. doménové jméno (např. www.vsb.cz). Bez doménových jmen bychom se museli k jednotlivým zdrojů dostávat přímým zadáním IP adresy - to by bylo jednak dosti nepohodlné a také dosti problematické, protože moderní WWW servery jsou schopny na jedné IP adrese provozovat desítky nebo dokonce stovky webových sídel.

Domény se rozlišují podle tzv. řádů. Doména I. řádu je většinou spojena se státem (např. .cz) nebo tématem (např. .edu - vzdělávání). Z praktického hlediska může být vždy správce takové domény pouze jeden, v případě ČR je to sdružení CZ.NIC.

Doména II. řádu, vždy spadá pod některou doménu I. řádu. Registrace takové domény se provádí u tzv. registrátora domén. Takových registrátorů přitom může (a také je) v jednotlivých státech obvykle více. Žádost o registraci provádí předpokládaný uživatel domény. Žádosti se vyhoví v případě, že je doména dostupná a byl zaplacen poplatek. Registrace je vždy časově omezena - obvykle na jeden rok. Za pronájem domény se platí každý rok.

Po expiraci domény (uplynutí doby na kterou byla doména zaplacena) je obvykle registrátorem poskytována určitá ochranná lhůta pro případ, že původní vlastník pouze zapomněl doménu zaplatit. V této lhůtě však již na doméně není dostupná webová prezentace původního vlastníka. Po uplynutí ochranné lhůty se doména vrací na běžný trh a může ji tak zakoupit kdokoliv.

Příkladem domény druhého řádu může být např.: vsb.cz.

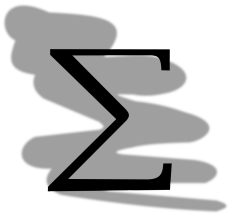
Doména III. řádu, někdy také nazývaná subdoména, se vytváří u domén II. řádu a může vypadat např. takto www.vsb.cz nebo fbi.vsb.cz. Za zřizování domén třetího řádu se již správci domény neplatí. Větší organizace se servis domén třetího řádu dokonce zajišťují sami.

Posledním typem zařízení, které v této podkapitole zmíníme je **Network Address Translation (NAT)**. Někdy se pro NAT používají také odlišné názvy, např. síťová maškaráda a jiné. NAT řeší problém připojování privátních sítí k síti Internet. Jelikož na privátní síti jsou používány IP adresy, které nejsou nutné unikátní celosvětově - není možné privátní síť připojit k Internetu přímo (konečně proto je ta síť privátní). K připojení je nutné použít zařízení, které zprostředkuje toto připojení. Přesně tyto úkoly plní NAT.

NAT funguje tak, že umožňuje počítačům na privátní síti použít jeho veřejnou IP adresu k připojení k Internetu. Představit si to lze tak, že požadavky z koncových počítačů na privátní síti jsou směřovány přes NAT a teprve ten osloví cílové zařízení na Internetu.

NAT si pamatuje odkud požadavek vzešel a směřuje tam odpovědi ze zařízení na Internetu. Pro vzdálená zařízení, je ale NAT netransparentní - vidí a komunikují přímo pouze s ním, protože pouze NAT na dané síti má veřejnou IP adresu.

V okamžiku, kdy se plně do praxe plně nasadí IPv6 (a zejména se ustoupí od užití IPv4), pozbude NAT smysl, jelikož IP adres bude dostupných tolik, že vlastní veřejnou IP adresu bude moci mít každé zařízení přítomně na síti a to celosvětově.



Shrnutí

Počítačové sítě lze členit podle různých vlastností nejčastější rozdělení ale rozlišuje sítě LAN lokalizované v jedné budově nebo jednom areálu budov a sítě WAN, které jsou schopny překlenout velké vzdálenosti mezi jednotlivými areály podniků.

Ze zařízení nezbytných pro konstrukci počítačových sítí je nutné zmínit *switch* sloužící pro propojení většího množství počítačů pomocí kabeláže. *Router* slouží pro směřování provozu na počítačových sítích, umožňuje tak propojovat různé segmenty sítí.

IP protokol umožňuje adresovat jednotlivá zařízení v síti pomocí IP adres. DNS je pak schopno tyto adresy překládat do podoby doménového jména (a zpět).

Kontrolní otázky

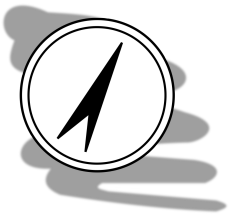
1. Co je účelem NAT?
2. Jakou funkci plní prezentační vrstva sítě?
3. K čemu slouží switch?
4. Jaká je funkce routeru?
5. Je možné z kroucené dvojlinky (kabel) vést odbočky?

Odpovědi

1. Účelem NAT je zprostředkovat připojení se k internetu počítačům přítomným v privátních sítích (počítačů nemající veřejnou IP adresu).
2. Prezentační vrstva sítě se stará o převod údajů z podoby pochopitelné počítačem do podoby odpovídající lokálním specifikům (např. desetinná čárka nebo desetinná tečka).
3. Switch slouží pro přípojení a komunikaci více počítačů do počítačové sítě.
4. Router směřuje síťový provoz. Slouží pro propojování jednotlivých segmentů sítě.
5. Ne.

Kapitola 6

E-government



Náhled kapitoly
Problematika e-governmentu je v ČR založena na několika základních pilířích, které v příštích dvou kapitolách postupně probereme. Jedná se:

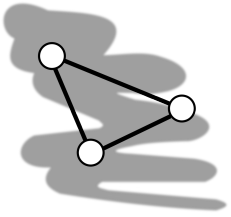
- základní registry
- informační systémy veřejné správy (ISVS)
- datové schránky a elektronické podatelny
- ostatní nástroje

V této kapitole se zaměříme především na problematiku základních registrů a datových schránek, s návaznostmi, které to má na problematiku elektronického podpisu. V kapitole následující se pak budeme podrobněji věnovat problematice ISVS.

Po přečtení kapitoly budete
Vědět

1. co jsou to základní registry a jaké údaje udržují
2. jak fungují datové schránky
3. co jsou to elektronické občanské průkazy

Čas pro studium
Pro prostudování této kapitoly budete potřebovat přibližně 2 hodiny.



Návaznost na elektronický podpis
Tato kapitola úzce navazuje na problematiku elektronického podpisu. Aby elektronická komunikace mezi orgány státní správy a firmami (popř. občany) byla důvěryhodná musí být dokumenty předávané např. datovými schránkami elektronicky podepsané. Před začátkem studia této kapitoly byste proto měli mít minimálně základní představu o tom, jak technicky funguje elektronický podpis a jak je jeho použití právně upraveno.

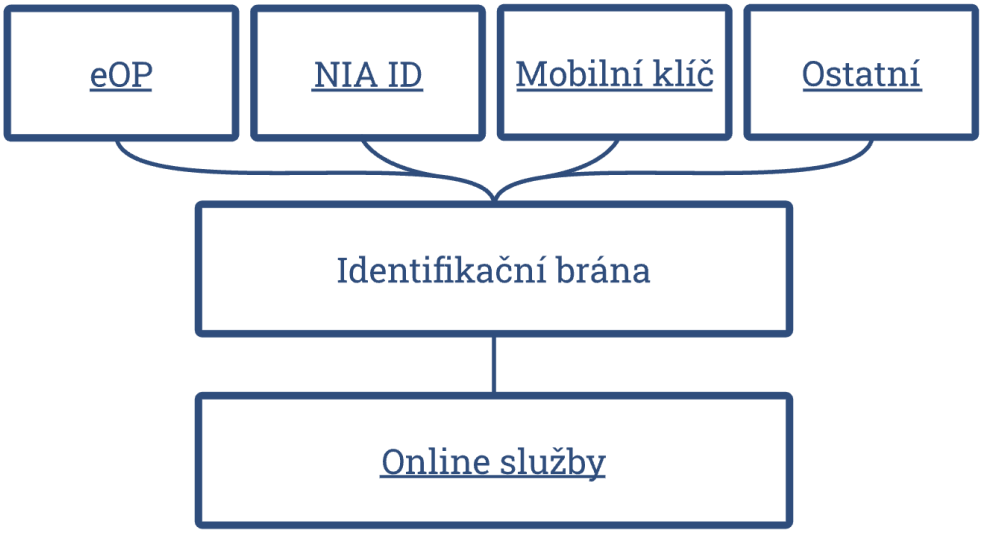
6.1 Elektronická identita

Předtím, než se podíváme na jednotlivé komponenty e-governmentu zkusme se ještě chvíli zastavit u problematiky *elektronické identity*. Této problematiky jsme se ve skutečnosti již dotkli při našem

výkladu služeb vytvářejících důvěru. Konkrétně, když jsme se bavili o eOP (občanských průkazech s aktivovaným elektronickým čipem) a také když jsme zmiňovali službu BankSign.

Zkusme se ale na tyto nástroje a služby podívat v širším kontextu e-governmentu. V tomto kontextu elektronická identita je vnímána jako *identita občana*, tedy jako nástroje a prostředky, kterými občan může prokázat svou identitu, aby mohl využít určitých služeb e-governmentu. Takovými službami může být např. vyplnění dotazníku sčítání lidu nebo třeba podání daňového přiznání.

Způsob, jakým může přistupovat občan k poskytovaným službám je znázorněna na obr. 6.1.



Obrázek 6.1: Přístup ke službám - prokázání identity občana (převzato z [85])

Z obr. 6.1 vyplývá, že občan může prokázat svou identitu třemi státem poskytnutými prostředky a pak skupinou prostředků, která se skrývá pod označením ostatní.

Identifikační jsou vydávány v souladu se zákonem 250/2017 Sb. o elektronické identifikaci, který rozlišuje:

- občanský průkaz s aktivovaným kontaktním elektronickým čipem (eOP),
- NIA ID,
- mobilní klíč eGovernmentu,
- ostatní

eOP jsem již zmiňovali, co ale znamená *NIA ID*? Jedná se o identifikační prostředek založený na dvou faktorovém ověření identity občana prostřednictvím znalosti uživatelského jména a hesla a vlastnictví registrovaného mobilního telefonu, na který budou chodit ověřovací SMS kódy.

Prvním krokem je vytvoření uživatelského účtu vyplněním registračního formuláře. Jelikož je ale registrační formulář volně přístupný, může jej vyplnit kdokoliv jakkoliv. Vyplněné údaje tak ve skutečnosti nejsou samy o sobě dostatečně důvěryhodné. Proto je sice na základě vyplnění registračního formuláře vytvořeno patřičné konto, ale zároveň není aktivováno. Aktivaci konta je možné provést jedním ze tří způsobů a to pomocí datové schránky, eOP nebo fyzicky na kontaktním místě Czech POINT.

Dalším prostředkem, který je možno použít pro prokázání identity občana je *mobilní klíč eGovernmentu*. Jedná se o aplikaci pro mobilní telefony, kterou lze používat např. pro přihlašování k datovým schránkám.

V případě, že občan má již aktivovanou datovou schránku je použití mobilního klíče pro něj v podstatě vyřešeno. Jiná je situace, kdy schránku nemá aktivovanou a nemá ani aktivovanou NIA ID identitu. V takovém případě totiž platí podobné pravidla jako v případě registrace NIA ID. Podobně jako zde, také mobilní aplikaci může nainstalovat kdokoliv kamkoliv, je proto potřeba další krok pro ověření skutečné identity občana. Tento krok se provádí na Czech POINT.

Konečně do ostatních spadají:

- čipová karta Starcos První certifikační autority - ověření probíhá z pozice kvalifikovaného poskytovatele certifikačních služeb

- služba MojeID sdružení CZ.NIC - po propojení účtu s Národním bodem pro identifikaci a autentizaci (NIA) a zabezpečením účtu bezpečnostním klíčem a ověřením totožnosti datovou schránkou, eOP nebo fyzicky na Czech POINT
- ověření pomocí bankovní identity - identita je ověžována na základě existujícího smluvního vztahu mezi bankou a jejím klientem

6.2 Základní registry

V roce 2009 byl přijat zákon 111/2009 Sb. o základních registrech [30], která definuje soubor základních registrů s informacemi o občanech. Základními registry ve smyslu tohoto zákona jsou:

1. Registr obyvatel
2. Registr právnických osob, podnikajících fyzických osob a orgánů veřejné moci (registr osob)
3. Registr územní identifikace, adres a nemovitostí (registr územní identifikace)
4. Registr agend orgánů veřejné moci a některých práv a povinností (registr práv a povinností)

Tyto registry jsou určeny pro sdílení údajů mezi základními registry a mezi agendovými informačními systémy tak, aby tyto údaje byly udržovány pouze na jediném místě. Ostatní IS, které s těmito údaji pracují, jejich správnost dále nezkoumají.

Zajímavé je také to, že fyzické osoby, o kterých se agenda vede, jsou identifikovány pomocí neveřejného identifikátoru, který je navržen tak, že z něj nelze odvodit žádné osobní nebo jiné údaje vztahující se k dané osobě.

V **registru obyvatel** jsou vedeny následující informace:

- jméno a příjmení
- adresa/místo pobytu
- datum, místo o okres narození (+ stát u cizinců)
- datum, místo a okres úmrtí
- státní občanství
- čísla elektronicky čitelných identifikačních dokladů
- záznam o zpřístupnění datové schránky

Správce registru obyvatel je Ministerstvo vnitra.

V **registru osob** jsou vedeny následující údaje:

- obchodní jméno/jméno a příjmení u fyzických osob
- agendou identifikátor osoby
- datum vzniku/zápisu do evidence
- datum zániku/výmazu z evidence
- právní forma
- informace o zpřístupnění datové schránky
- statutární orgán
- právní stav
- adresa sídla
- datum zahájení/ukončení činnosti v provozovně
- adresa místa provozovny
- adresa místa pobytu

Správcem registru osob je Český statistický úřad.

Registr územní identifikace obsahuje řadu údajů o území, ale také jednotlivých objektech, které jsou na něm postaveny. O území samotném jsou vedeny následující informace:

1. území státu,
2. území regionu soudržnosti
3. území vyššího územního samosprávného celku
4. území kraje
5. území okresu
6. správní obvod obce s rozšířenou působností
7. správní obvod obce s pověřeným obecním úřadem
8. území obce

9. území vojenského újezdu
10. správní obvod v hlavním městě Praze
11. území městského obvodu v hlavním městě Praze
12. území městské části v hlavním městě Praze
13. území městského obvodu a městské části územně členěného statutárního města
14. katastrální území
15. území základní sídelní jednotky
16. stavební objekt
17. adresní místo
18. pozemek v podobě parcely

O samotných objektech se pak shromažďují tyto informace:

1. měsíc a rok dokončení,
2. počet bytů u stavebního objektu s byty,
3. zastavěná plocha v m^2,
4. obestavěný prostor v m^3,
5. podlahová plocha v m^2,
6. počet nadzemních a podzemních podlaží,
7. druh svislé nosné konstrukce,
8. připojení na vodovod,
9. připojení na kanalizační síť,
10. připojení na rozvod plynu,
11. připojení na rozvod elektrické energie,
12. způsob vytápění a
13. vybavení výtahem.

Funkci editora vykonává obec, městský obvod nebo městská část územně členěného statutárního města, městská část hlavního města Prahy a kraj v přenesené působnosti.

Je zajímavé, že ze všech registrů je tento jediný dostupný široké veřejnosti v otevřené formě, dokonce lze říci, že je dostupný v atraktivní podobě interakivních mapových podkladů. Použití údajů je poměrně široké. Jednak je k dispozici samotné rozhraní pro koncového uživatele, viz https://vdp.cuzk.cz/, náhled rozhraní je pak k dipozici na obr. 6.2, jednak existuje řada dalších služeb které z tohoto registru čerpají data, remixují je, spojují s dalšími daty a poskytují výsledek svým uživatelům.

Pro katastrální úřad toto představuje poměrně zásadní problém, protože řada těchto služeb pracuje v reálném čase a využití tak poměrně silně zatěžuje servery úřadu. již nějakou dobu proto probíhají veřejně debaty, zda by se přistup do tohoto registru neměl omezit. Odsud ale převládat veřejný zájem a tak registr zatím zůstává otevřen.

V **registru práv a povinností** se eviduje především seznam činností a rolí, které vykonávají jednotlivé orgány veřejné moci. Správce registru je opět Ministerstvo vnitra.

V souvislosti s registry je zajímavé jedno datum a to konkrétně *1. 7. 2012*. Od tohoto data totiž vstupují v platnost všechna ustanovení zákona o základních registrech v platnost. V praxi by to mělo znamenat, že úředník při komunikaci s občanem již nebude moci přímo od občana zjistit danou informaci, pokud je již obsažena v některém z registrů.

V současnosti jsou již základní registry zavedeny plnohodnotně. A tak komunikace a sdílení informací mezi systémy funguje funguje už standardně.

Veškeré přístupy k registrům jsou navíc pečlivě evidovány. Občan tak má možnost požádat o výpis „aktivity“ v registrech týkající se jeho osoby. Může tak teoreticky zjistit, kdo (např. jaký úřad) se o jeho osobu zajímal. Slovo teoreticky je tady použito proto, že je ve výpisu aktivity velmi obtížné rozlišit automatizované zásahy systémů čistě technického rázu, které jsou prováděny v celém systému, a situací, kdy byl dotaz proveden některým z úřadů na určitou osobu přímo. Právě informace o druhém typu přístupu je přitom pro občana zajímavější.

To výrazně snižuje užitečnost celého mechanismu.

Přes veškeré problémy se základní registry staly páteří, ze které čerpají prakticky všechny informační systémy používané ve státní správě.

Obrázek 6.2: Registr území - oblast Ostrava Výškovice (převzato z [54])

6.3 Elektronické podatelny

Povinnost zřizovat elektronické podatelny byla stanovena vyhláškou 496/2004 Sb. o elektronických podatelnách. Samotné zřízení elektronické podatelny se dělo podle nařízení vlády 495/2004 Sb., kterým se provádí zákon č 227/2000 Sb. o elektronickém podpisu ve znění pozdějších předpisů.

Uznávány jsou podané dokumenty, které splňují určité požadavky na formát zprávy (obvykle jsou podporovány formáty doc, xls, pdf a html – požadavky na formáty musí být také zveřejněny). U některých typů dokumentů je nutné pak ještě připojení elektronického podpisu, značky nebo časového razítka. Požadavky na tyto typy dokumentů jsou stanoveny samostatnými zákony a vyhláškami.

Zaslaná elektronická zpráva se na úřadu zaregistruje a je vyřízena v souladu s pravidly, která byly pro tento typ dokumentů přijaty.

Technicky se v podstatě nejedná o nic jiného než běžné schránky elektronické pošty, které prokazatelně přináležejí k určitému orgánu státní správy nebo samosprávy.

Elektronické podatelny se z hlediska technického i legislativního přežily a jak vyhláška 496/2004 Sb., tak nařízení vlády 495/2004 Sb. byly zrušeny zákonem 167/2012 Sb. Přesto některé obce nebo úřady elektronické podatelny ponechaly v provozu jako jednu z cest komunikace s občany.

Pro formální předávání dokumentů se pak většinou využívá služeb datových schránek nebo písemných podání (v „papírové“ podobě).

6.4 Datové schránky

Datové schránky byly přijaty v roce 2008 zákony 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů a 301/2008 Sb. kterým se mění některé zákony v souvislosti s přijetím zákona 300/2008 Sb.

Pro funkčnost datových schránek jsou velmi důležité další navazující zákony a vyhlášky, především 191/2009 Sb. o podrobnostech spisové služby, 193/2009 Sb. o stanovení podrobností provádění

autorizované konverze dokumentů a 194/2009 Sb. o stanovení podrobností užívání a provozování informačního systému.

Zákon 300/2008 definuje informační systém datových schránek a jeho využití. Na rozdíl od elektronické podatelny datová schránka funguje jinak. Není založena na technologii elektronické pošty, ale na existenci státem garantovaného informačního systému, kde každý uživatel má svůj prostor a také nástroje pro komunikaci, primárně s orgány státní moci, v omezené míře i dalšími uživateli datových schránek. Tímto způsobem odpadají problémy s identifikací uživatele, ale také problémy s doručovacími adresami, s vyzvedáváním pošty (listovních zásilek) apod.

Současným „technickým“ provozovatelem informačního systému datových schránek je Česká pošta.

Datové schránky mohou využívat orgány veřejné moci, právnické a fyzické osoby. Zřízení pro všechny typy uživatelů probíhá bezúplatně a to do tří dnů od podání žádosti. Použití datových schránek je přitom pro právnické osoby a orgány veřejné moci povinné a pro tyto zřízení datové schránky probíhá automaticky.

Fyzické osoby mohou využít služeb datových schránek nepovinně. Pokud si ale už datovou schránku zřídí, jsou orgány státní moci povinny s uživatelem komunikovat právě pomocí ní. Z tohoto pohledu nás v souvislosti s použitím datových schránek čeká významná změna počátkem roku 2023. Tyto změny souvisí s další elektronizací postupů orgánů veřejné moci (zákon 261/2021 Sb.). Jeho součástí je zavedení povinnosti datových schránek pro všechny osoby samostatně výdělečně činné.

Datové schránky budou zřízeny také občanům, kteří použijí prostředek pro elektronickou identifikaci vydaný v rámci kvalifikovaného systému elektronické identifikace. Typicky se bude jednat o tzv. bankovní identitu. V tomto případě bude ale datová schránka pouze aktivovaná, občan se ale může rozhodnout ji opětovně deaktivovat. Předpokladem veřejné správy přitom je, že většina obyvatel tak ale neučiní a schránku začnou využívat.

Datové schránky samotné zřizuje a spravuje Ministerstvo vnitra.

Uživatel k obsahu datové schránky přistupuje obvykle přes WWW rozhraní. Existují ale také desktopové aplikace, které umožňují s datovou schránkou pracovat také, často pohodlněji. Příkladem takové aplikace je Datovka 4 [52] vyvíjená sdružením CZ.NIC.

Veškeré zasílané dokumenty v rámci komunikace prostřednictvím datových schránek musí být elektronicky podepsány. Pasivní užití schránek je tak sice zdarma, ale v případě, že uživatel chce využívat datovou schránku pro zasílání dokumentů (není to ve všech případech povinné), musí získat patřičný certifikát od poskytovatele certifikačních služeb dle eIDAS. Tyto služby jsou již zpoplatněny.

Jednou ze zajímavých vlastností datových schránek, tedy alespoň z právního pohledu, je tzv. *doručovací fikce*. Podle ní, je zpráva považována za doručenou okamžikem, kdy se uživatel s oprávněním zaslanou zprávu přečíst přihlásí k datové schránce. Není přitom podstatné, zda zprávu ve skutečnosti během své práce se schránou otevřel a přečetl. Zpráva je považována taktéž za doručenou 10 dnem po dodání zprávy do schránky.

Současná interpretace je taková, že termínem 10 dní se rozumí 10 pracovních dní (tedy přibližně 2 běžné týdny). Po uplynutí této doby, je zpráva považována za doručenou, bez ohledu zda se vlastník schránky do ní přihlásil nebo ne. V tomto okamžiku pak začínají běžet případné lhůty na odvolání apod. Fikce doručení je sice na jedné straně velmi výhodná z hlediska státní správy, jejíž funkce se tím zrychluje, na straně druhé nemusí být výhodná z hlediska občana. To je také jedním z důvodů proč datové schránky u fyzických osob dosud nebyly příliš populární.

V současné době je zatím většinou možná komunikace se státními orgány v „papírové podobě“ směrem podnik → státní orgán, komunikace opačným směrem je však ze zákona možná pouze v elektronické podobě prostřednictvím datových schránek.

Jedinou výjimkou kdy i orgán veřejné moci může využít klasickou „papírovou“ formu je případ, kdy povaha dokumentu samotného zaslání v elektronické podobě, to neumožňuje. V současné době se tedy stále v papírové podobě přepravuje dokumentace s velkým rozsahem obrazového materiálu např. ze soudů apod.

Zasílání zpráv, faktur nebo v budoucnu jiných dokumentů právnickým nebo fyzickým osobám je přitom také zpoplatněno. Po několika letech provozu se nedá říci, že by právě posílání faktur mezi společnostmi pomocí datových schránek bylo nějak zvláště oblíbeno.

Pro zasílané zprávy je vždy vytvořena tzv. obálka s identifikačními údaji zprávy (tzv. metainformace o datové zprávě). Tato obálka se zasílá spolu se samotným souborem zprávy. Po uplynutí 10 dní, se zpráva automaticky považuje za přečtenou, se všemi právními důsledky, které to má. Uživatel datové schránky pak má možnost zprávu přečíst dalších 90 dni. Po uplynutí této doby je zpráva ze systému smazaná (pokud si uživatel nezaplatil dodatečnou službu nazvanou Datový trezor). V systému

zůstane zachována pouze obálka datové zprávy obsahující:

1. Kdo zprávu poslal
2. Komu ji poslal
3. Kdy ji poslal
4. Informaci zda a kdy byla přečtena
5. Název zprávy
6. Hash samotné zprávy

Pokud, tedy příjemce zprávy potřebuje zprávu zachovat pro pozdější použití, musí použít buď zpoplatněnou službu – tato služba ovšem neřeší expiraci certifikátu, kterým byla zpráva podepsána, a tedy možnost pozdějšího ověření pravosti zaslaného dokumentu – nebo musí použít služeb tzv. *autorizované konverze dokumentů*.

Autorizovanou konverzi je možné provést na CzechPOINTu. Sestává se z ověření datové zprávy z hlediska validity elektronického podpisu (elektronické značky, elektronické pečeti, popř. časového razítka), následného tisku a zkontrolování souladu s původní zprávou. O celém procesu se vytvoří ověřovací doložka, která je uložena do centrálního úložiště. Celý proces tak připomíná proces standardního úředního ověřování dokumentů a jako takový je také zpoplatněn.

Platnost elektronického podpisu
Ověření dokumentu/datové zprávy je možné pouze po dobu platnosti certifikátu, který byl použit pro podepsání dokumentu.

Po uplynutí platnosti nebo revokaci certifikátu dokument/zprávu není možné ověřit bez ohledu na zákonné lhůty pro doručování zpráv do datové schránky a 90 denní ochranné lhůty pro archivaci zpráv. Takové zprávy již není možné ani autorizovaně konvertovat do listinné podoby.

Problém 24 hodin
S autorizovanou konverzí je spojován ještě jeden problém, který zasluhuje Vaši pozornost. Pro tento problém se vžil název *problém 24 hodin* a je spojován s procesem revokace certifikátu. Problém spočívá v tom, že v okamžiku, kdy osoba revokuje certifikát, PCS musí ověřit, že žádost je oprávněná, následně certifikát zařadí na seznam revokovaných certifikátů a ten zveřejní. Celá tato operace může zabrat až 24 hodin. Při autorizované konverzi se ověřuje zda certifikát použitý pro podpis není na aktuálně platném seznam revokovaných certifikátů. Tím ale není zaručeno, že certifikát nebyl revokován, ale aktualizovaný seznam revokovaných certifikátů ještě nebyl zveřejněn.
CzechPOINT tento problém přenáší na svého zákazníka upozorněním v průvodce konverzní doložky.

Do budoucna se uvažuje s možností dlouhodobého ověřování platnosti dokumentů uskladněných v datových schránkách. Předpokládá se přitom použití kombinace časového razítka a elektronické značky. Časové razítko umožní ukotvit dokument v čase a zkoumat, zdali v okamžiku zaslání zprávy byl certifikát použitý k podepsání zprávy v platnosti nebo ne.

Bohužel ani časové razítko nezajistí schopnost ověřování pro situace, kdy došlo k prolomení bezpečnosti použitého schématu elektronického podpisu, které by umožnilo padělání těchto dokumentů. Z tohoto důvodu se uvažuje o použití různých tzv. „solí“, které znesnadňují útoky, ale ani tento mechanismus nezaručuje dlouhodobou bezpečnost – zejména s uvážením možnosti úniku mechanismu generování soli.

Na ověřování dokumentů z datových schránek ale existuje ještě jeden pohled, který je v přímém rozporu s výše uvedeným názorem. Alternativní pohled pracuje s pojmem vyvratitelná domněnka pravosti, podle zákona 499/2004 Sb., o archivnictví a spisové službě. Domněnka pravosti totiž zjednodušeně říká, že dokument se považuje za pravý, pokud byl podepsán a není prokázáno, že by pravý nebyl.

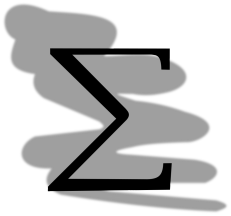
Tento pohled se vůbec nezabývá platností certifikátů (ať už použitých pro podpisové operace nebo operace časového razítka) – dokument může platit věčně. To znamená, že na zájemci o zneplatnění dokumentu je důkazní břemeno prokázání toho, že dokument není pravý.

Takový přístup byl jednu dobu preferovaný státní správou. Dnes se však i státní správa spíše přiklání k nutnosti pečlivého udržování řetězce důvěry nutného pro technické zajištění zaručení pravosti elektronických dokumentů.

Elektronický podpis a datové schránky, zajímavosti a podrobnosti
Celá problematika elektronického podpisu a datových schránek je velmi zajímavá, bohužel však také velmi složitá a dynamicky se vyvíjející.

Pro zájemce proto doporučuji studium z dalších zdrojů. Začít doporučuji s podnětnými články Jiřího Peterky na lupa.cz [14].

Pozornost věnujte především článkům s nálepkou e-government, datové schránky, e-podpis a eIDAS (ačkoliv i ostatní články jsou nepochybně zajímavé).



Shrnutí
Základní registry jsou centrálně vedené databáze obsahující informace o občanech, osobách, nemovitostech a také jednotlivých agendách správních úřadů. Svým rozsahem se v podmínkách ČR jedná o nebývalý posun v oblasti e-governmentu, který se jinak nevyvíjí příliš dynamicky. Hlavní myšlenkou základních registrů je, že budou představovat důvěryhodný zdroj informací pro další agendy a systémy provozované veřejnou správou. Informace vedené v registrech proto občan nebude muset opakovaně hlásit na různých úřadech, ale prostě se načtou z těchto registrů.

Elektronickými podatelnami rozumíme „virtuální“ místa, provozovaná orgány státní moci, kam je možné posílat oficiální komunikaci. V dnešní době se již do velké míry jedná o přežitek, jelikož úřady je možno kontaktovat jak elektronicky např. e-mailem (ideálně elektronicky podepsaným), tak pomocí datových schránek.

Datové schránky, přesněji řečeno *informační systém datových schránek* je systémem pro zaručenou komunikaci mezi úřady, úřady a osobami (právnickými nebo fyzickými) a osobami mezi sebou. Použití datových schránek je povinné pro úřady a také právnické osoby (je povinné mít schránku a vybírat její obsah). Osoby fyzické si mohou datovou schránku nechat zřídit.

Pro komunikaci ze strany úřadů funguje tzv. doručovací fikce - tedy zpráva se po uplynutí určité doby považuje automaticky za přijatou se všemi právními důsledky, které to může mít, bez ohledu na to, zda ji ve skutečnosti někdo opravdu četl nebo ne.

Kontrolní otázky

1. Co řeší nařízení eIDAS?
2. Co rozumíme pojmem fikce doručení (u datových schránek)?
3. Jaké základní registry jsou provozovány v rámci ČR?

Odpovědi

1. Nařízení eIDAS řeší problematiku důvěryhodné identifikace fyzických a právnických osob pro on-line služby provozované veřejnou správou v rámci celé EU.
2. Fikcí doručení rozumíme to, že po uplynutí stanovené doby předpokládá úřad, že jím zaslané podání bylo doručeno (se všemi právními důsledky) bez ohledu na to, zda k přečtení datové zprávy skutečně došlo nebo ne.
3. Registr obyvatel, registr osob, registr územní identifikace, registr práv a povinností.

Kapitola 7

Informační systémy veřejné správy

Průvodce studiem
V této kapitole se seznámíme s koncepcí informačních systémů ve veřejné správě (ISVS).

Po prostudování této kapitoly budete
Vědět

- Jaké systémy považujeme za veřejné
- Jakým způsobem jsou ISVS sestavovány
- Jaké úlohy plní v této oblasti ministerstvo vnitra

Čas nutný pro studium
Pro prostudování této kapitoly budete potřebovat přibližně hodinu.

7.1 Stručná historie informačních systémů veřejné správy v ČR

Budování informačních systémů veřejné správy je spjato s nasazováním informačních technologií ve státní správě. Každá z institucí, která tyto systémy nasazovala tak činila proto, aby do určité míry automatizovala svou činnost a také získala jednotné úložiště, které by umožnilo sdílet data mezi pobočkami veřejných institucí.

Primárním cílem tak bylo zajistit plnění úkolů svěřených těmto institucím prostřednictvím v té době platné legislativy. To znamená, že každá instituce buduje vlastní, samostatné systémy, které nepředpokládají spolupráci se systémy jiných institucí nebo dokonce sdílení dat mezi nimi.

Slabiny této koncepce si vláda uvědomila už v roce 1996, kdy vzniká zákonem 272/1996 Sb. Úřad pro státní informační systém (ÚSIS). Ještě téhož roku měl být přijat další zákon, který tomuto úřadu měl definovat práva a povinnosti (tedy kompetence). Díky politickým turbulencím ale tento kompetenční zákon přijat nebyl a tak ÚSIS až do svého zániku zůstal „bezzubý“.

Výsledkem jeho práce tak bylo pouze několik spíše obecnějších dokumentů zabývajících se koncepcí informačních systémů ve veřejné správě.

Ke změně došlo až v roce 2000, kdy je přijat zákon 365/2000Sb. o informačních systémech veřejné správy, který ÚSIS ruší. Úkoly v oblasti ISVS tak přejímá nově zřízené Ministerstvo informatiky a Úřad pro veřejné informační systémy.

Úřad pro veřejné informační systémy dostává za úkol řešit především praktickou realizaci opatření v oblasti ISVS, zatímco Ministerstvo informatiky řeší oblast normalizace, vývoj legislativy apod.

Ministerstvo informatiky tak oblast řeší především návrhem standardů ISVS, které definují životní cyklus informačních systémů, jakým způsobem budou mezi nimi vyměňována data apod.

Poslední větší změna se udála v roce 2006, kdy zaniká Ministerstvo informatiky a jeho úkoly přebírá Ministerstvo vnitra. V rámci této transformace pozbývají platnost standardy ISVS, ve své původní podobě (tedy jako normy), některé z nich jsou ale přijaty ve formě vyhlášek v rámci nově přijaté legislativy ISVS.

7.2 Informační systémy veřejné správy

Informační systémy veřejné správy jsou definovány zákonem 365/2000 Sb. o informačních systémech veřejné správy. Tento zákon definuje ISVS jako soubor informačních systémů, které slouží pro výkon veřejné správy. Tedy v podstatě jakýkoliv informační systém, který je využíván orgány veřejné správy. Za ISVS jsou považovány i jiné informační systémy, které této definici nepodléhají. V takových případech tyto systémy do skupiny ISVS zařazuje nějaký jiný právní předpis (např. zákon o státní statistické službě, živnostenský zákon, apod.).

Naopak u některých informačních systémů, které by výše uvedenou definici splňovaly, se o ISVS nejedná a to opět ze zákona. Jedná se především o takové systémy, které nakládají s údaji takové povahy, že okruh užití těchto údajů by měl zůstat pouze v kompetenci daného orgánu.

Mezi ISVS proto neřadíme informační systémy používané zpravodajskými službami, Policií ČR, Vězeňskou službou, orgány činnými v trestním řízení, Národním bezpečnostním úřadem. Zákonu o ISVS také nepodléhají některé činnosti Ministerstva financí (v souvislostí s finanční kriminalitou) a Ministerstva obrany (v souvislosti s obranou státu).

Zákonu také nepodléhají orgány veřejné správy nebo právnické osoby (resp. IS, které provozují), které tyto IS využívají výlučně pro účely krizového řízení dle krizového zákona (240/2000 Sb.).

Specifické je také postavení Ministerstva vnitra, do jejíž gesce ISVS spadají. Ministerstvo vnitra má:

- kontrolní a tvůrčí pravomoci v této oblasti,
- působí v akreditaci a atestaci,
- stanovuje pravidla pro sdílení informací,
- vyjadřuje se k projektům ISVS,
- vydává věstník.

Pokud mají být finanční prostředky vynaložené na rozvoj ISVS vynaloženy efektivně, musí existovat místo, kde se tyto systémy (a jejich schopnosti) budou registrovat a orgán, který bude kontrolovat, že navrhovaný systém již není realizován a používán např. nějakým jiným orgánem státní správy. To znamená, že investice do pořízení nebo rozšíření ISVS není zbytečná.

Jednotlivé systémy musí být také vzájemně kompatibilní, pokud si mezi sebou mají vyměňovat informace. Tato kompatibilita by přitom měla jít až na co možná nejnižší úroveň – tedy na úroveň stanovení datového typu a rozsahu a také pravidel validace správnosti vyplněného údaje. Tyto definice pak musí být veřejně dostupné tak, aby je mohly správně do svých systémů implementovat další orgány státní správy. Těmto definicím a pravidlům souhrnně říkáme *referenční rozhraní*.

ISVS musí také splňovat určité bezpečnostní podmínky, s tím souvisí akreditace a atestace.

Akreditací rozumíme pověření nezávislé právnické osoby prováděním atestací ISVS. Akreditaci provádí Ministerstvo vnitra a může ji udělit pouze nezávislé právnické osobě (nezávislé na posuzovaných ISVS), která je zároveň členem mezinárodních sdružení zabývajících se akreditacemi.

V rámci akreditace se prověřuje zejména existence schválených akreditačních pravidel a také to, zda daná organizace má proces atestace odborně zajištěn kvalifikovaným personálem.

Atestace samotné pak provádí akreditované atestační středisko, které nesmí mít pohledávky vůči orgánům státní správy (nesplňovalo by podmínku nezávislosti). Atestace se provádí dvojího typu:

- posuzování dlouhodobého řízení ISVS a
- způsobilost k realizaci vazeb mezi systémy ISVS

Atestace se provádí vždy podle předem stanovených atestačních podmínek. Výsledkem atestace je protokol o zkoušce. Atest se uděluje vždy na dobu určitou a to maximálně na 5 let. Atest je však možno opakovaně prodlužovat a to maximálně o 2 roky.

Své úkoly v oblasti ISVS mají taktéž orgány státní správy a to především:

- spolupracují s Ministerstvem vnitra,
- předkládají Ministerstvu vnitra návrhy na pořízení nebo změnu informačních systémů,
- zajišťují vazby na jiné informační systémy pomocí referenčního rozhraní,

- zveřejňují číselníky,
- odstraňují nedostatky zjištěné v rámci kontrol.

Jakým způsobem konkrétně se výše uvedené činnosti provádějí, definují prováděcí vyhlášky tohoto zákona.

Vyhláška 469/2006 Sb. o *informačním systému o datových prvcích* definuje fungování informačního systému shromažďujícího informace o jednotlivých datových prvcích.

Datovým prvkem přitom rozumíme datovou položku a její popis. Účelem je, aby data vedená v informačních systémech veřejné správy vedla tato data stejně napříč systémy – a tyto systémy tak byly kompatibilní.

Aby bylo možné tyto informace efektivně využívat napříč informačními systémy, musí být shromážděny na jediném místě, a to je právě informační systém o datových prvcích. Implementátor systému ISVS tak nejprve nahlédne do tohoto systému, aby zjistil, jak přesně má datový prvek být implementován.

U datových prvků platí jedno omezení, vyhlašovány (v IS o datových prvcích) jsou takové prvky, kde lze předpokládat, že může docházet k výměně nebo dat mezi systémy. Udaje, které nesmí být sdíleny tak nemá smysl vyhlašovat.

Vzhledem k výše uvedenému lze informační systém o datových prvcích považovat za základní stavební kámen možnosti implementace tzv. *referenčního rozhraní*, které umožňuje vzájemnou komunikaci mezi systémy.

Vyhláška 528/2006 Sb. o *informačním systému o informačních systémech veřejné správy* definuje náležitosti informačního systému, který bude shromažďovat informace o existujících systémech veřejné správy. Takový systém umožňuje zjišťování, zda existuje IS s požadovanými vlastnostmi včetně toho, kde je takový systém nasazen.

Účelem takového systému je vytvořit prostředí motivující k efektivním investicím do IT. Organizace pořizující nebo modifikující IS tak nemůže činit svévolně, ale až poté co prokáže, že změna je nutná (v souvislosti s legislativními požadavky) a nejsou k dispozici takové systémy, které umožňují vedení potřebné evidence.

Vyhláška 529/2006 Sb. o dlouhodobém řízení informačních systémů veřejné správy se zabývá různými aspekty životního cyklu ISVS a zejména dat v něm obsažených. IS musí být spravován dlouhodobě – dokud bude trvat potřeba dat v něm obsažených. Z toho také vyplývá nutnost provádět plánování na pořízení nebo vytvoření informačního systému, ale také plány na udržení kvality poskytovaných služeb a bezpečnosti.

Základním dokumentem nutným k dosažení těchto cílů je *informační koncepce*, která se přijímá (na úrovni orgánu státní správy) na dobu určitou a tyto problémy by měla řešit.

Vyhláška 530/2006 Sb. o postupech atestačních středisek při posuzování dlouhodobého řízení ISVS stanovuje způsob, jak postupovat během atestace orgánů státní správy na jejich způsobilost dlouhodobě řídit své informační systémy. Atestace se zaměřuje především na hodnocení informační koncepce a provozní dokumentace provozovaných informačních systémů. Výsledkem atestace je certifikát s jedním z možných výsledků:

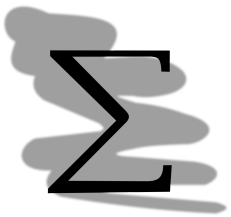
- splněno,
- splněno s výhradou,
- nesplněno.

Vyhláška 52/2007 Sb. o postupech atestačních středisek při posuzování způsobilosti k realizaci vazeb ISVS prostřednictvím referenčního rozhraní stanovuje způsob atestace způsobilosti orgánu státní správy realizovat vazby na jiné ISVS pomocí referenčního rozhraní.

Během atestace se hodnotí zejména soulad mezi implementací vazby a její soulad s dokumentací (viz. 469/2006 Sb.). Výsledkem atestace je certifikát s hodnocením splněno nebo nesplněno.

Vyhláška 53/2007 Sb. o referenčním rozhraní stanovuje povinnost používat v rámci ISVS vyhlášené datové prvky. Ovlivňuje také technologii, která bude použita pro výměnu informací mezi jednotlivými ISVS – předpokládá se totiž výměna pomocí jazyka XML.

Konečně vyhláška 64/2008 Sb. o přístupnosti garantuje přístupnost služeb ISVS také lidem se zdravotními postiženími.



Shrnutí

Informačními systémy veřejné správy (ISVS) rozumíme veškeré systémy využívané veřejnou správou pro vykonávání úkolů veřejné správy. Účelem legislativy ISVS je zajistit, aby jednotlivé IS implementované veřejnou správou:

- znovu „nevymýšlely kolo“ - tedy aby neřešily již vyřešené problémy
- byly vzájemně kompatibilní ve smyslu datových definic udržovaných údajů, které se objevují ve více systémech
- byly vyvíjeny pouze v případě, že je to opravdu nutné, tedy implementaci vyžaduje nová nebo změněná legislativa a neexistuje žádný systém, který by tyto požadavky plnil
- byly dlouhodobě udržitelné - tedy aby bylo možné IS dlouhodobě provozovat.

Koordinační úlohu v pro oblast ISVS má Ministerstvo vnitra, které jednak vede samo některé systémy zejména pak informační systém o informačních systémech ve veřejné správě (katalog používaných ISVS) a také vede IS datových prvků, obsahující definici datového prvku, která by měla být dodržena napříč jednotlivými systémy. Ministerstvo vnitra také akredituje atestační střediska, která hrají velmi důležitou roli v životním cyklu ISVS, atestují totiž jednotlivé úřady z hlediska schopnosti systémy dlouhodobě udržovat v provozu.

Kontrolní otázky

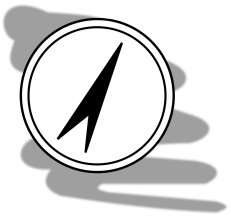
1. Co je to ISVS?
2. Jak probíhá atestace úřadu na schopnost dlouhodobě provozovat informační systém?
3. Co je to datový prvek ISVS?
4. Jaké úlohy plní v oblasti ISVS Ministerstvo vnitra?

Odpovědi

1. ISVS jsou všechny systémy provozované veřejnou správou pro plnění úloh jí svěřených platnou legislativou.
2. Atestace probíhá u akreditovaného atestačního střediska na základě žádosti úřadu. Atestuje se způsobilost k dlouhodobé udržitelnosti systému a také realizaci vazeb mezi různými systémy. Atestace je na dobu určitou, ale je možné podat žádost o její prodloužení.
3. Datová prvek je specifikace jména, datového typu a popisu údaje, který má být uložen v některém z ISVS. Účelem datového prvku je zajistit kompatibilitu mezi systémy za účelem výměny údajů mezi nimi.
4. Schvaluje pořízení nového ISVS, akredituje atestační střediska, vede informační systém o informačních systémech veřejné správy a informační systém o datových prvcích.

Kapitola 8

Kybernetická bezpečnost v ČR



Náhled kapitoly
Problematika kybernetické bezpečnosti, je již dlouhá léta skloňována ve všech pádech v soukromé sféře. Sféra veřejná ale po dlouhou dobu zůstávala stranou zájmu útočníků tak bezpečnostních expertů. V posledních letech se však situace výrazně změnila a jsme svědky výrazných posunů řízení kybernetické bezpečnosti jednotlivých států a také užšího zaměření se na ochranu řídících systémů kritických infrastruktur.

V této kapitole se seznámíme se stavem řešení kybernetické bezpečnosti v ČR.

Po přečtení kapitoly budete
Vědět

1. jaké úlohy plní vládní a národní CSIRT tým
2. jaké je postavení kybernetické bezpečnosti s ohledem na ochranu kritické infrastruktury

Čas pro studium
Pro prostudování této kapitoly budete potřebovat přibližně 45 minut.

8.1 Kybernetická bezpečnost

Dlouhou dobu byla otázka kybernetické bezpečnosti spíše doménou jednotlivých organizací - nebylo jasně patrné, že tuto problematiku je nutné řešit komplexněji i na té nejvyšší, tedy celostátní úrovni nebo dokonce na nadnárodní úrovni. Tento pohled se ale v průběhu posledních několika let zásadně změnil v souvislosti se změnou přístupu k ochraně kritické infrastruktury na straně jedné a odhalením řady dlouhodobých útoků, kterým musely čelit společnosti provozující významné prvky kritické infrastruktury i provozovatelé významných informačních systémů.

Z útoků, které by stálo za to zmínit, je možno zmínit např. Stuxnet nebo operaci Night Dragon. Stuxnet je malware zaměřený na fyzické poškození vybraných zařízení - konkrétně centrifug používaných pro obohacování uranu. Night Dragon byla operace kladoucí si za cíl kompromitaci sítí firem podnikajících v chemickém průmyslu USA, především pro účely získání intelektuálního vlastnictví společností, ale také plánů budov apod. V obou případech se předpokládá, že se jedná o tzv. *státem sponzorované útoky*, byť důkazy, že tomu tak skutečně bylo, chybí.

V poslední době také prakticky nemine týden, kdy by nebyl publikován nějaký případ velkého úniku informací nebo úspěšného útoku na významné počítačové sítě. Změna celkové bezpečnostní situace v oboru IT tak nutně vedla ke změně postoje i v oblasti řešení této problematiky i na nejvyšší úrovni.

V ČR se problematiky kybernetické bezpečnosti ujalo Ministerstvo vnitra jako ministerstvo, které plně přejalo veškeré agendy zaniklého Ministerstva informatiky. Ukázalo se však, že portfolio činností, které musí Ministerstvo vnitra zajišťovat je natolik široké, že efektivní rozvoj problematiky kyberbezpečnosti v podstatě nebyl možný.

Z tohoto důvodu se změnila koncepce přístup k řešení této problematiky a proto se hlavním garantem této problematiky stal Národní bezpečnostní úřad (NBU). Primární oblastí zájmu NBÚ je ochrana informací, především těch utajovaných. Vzhledem k tomu, jakým způsobem jsou takové informace v současnosti obvykle vedeny, popř. předávány, je očividné, že NBÚ má k problematice kybernetické bezpečnosti blíže nežli Ministerstvo vnitra.

Jako prvním krokem bylo zřízení národního CSIRT týmu (viz následující podkapitola) a v roce 2011 také zřízení Národního centra kybernetické bezpečnosti (Národní centrum kybernetické bezpečnosti (NCKB)), které bylo provozováno přímo v rámci NBÚ.

Toto centrum už bylo vyčleněno vyloženě k realizaci úkolů v oblasti kybernetické bezpečnosti. Jedním z důležitých úkolů bylo provozovat vládní CERT České republiky GovCERT.CZ. Centrum plní také další úkoly, jako je spolupráce s obdobnými organizacemi v zahraničí, příprava bezpečnostních standardů pro různé kategorie organizací v ČR, osvěta, ale také výzkum a vývoj v oblasti kybernetické bezpečnosti.

K výše uvedenému je ale potřeba uvést, že NBÚ a tudíž také NCKB spadají pod státní správu a pro ni platí, že musí být zmocněna k výkonu všech činností legislativou (především zákony). Změny v legislativě však přišly až 1.1.2015, kdy vešel v platnost zákon 181/2014 Sb. o kybernetické bezpečnosti, který konečně zmocnil úřad k výkonu některých činností. Zákon totiž zakotvil postavení vládního a národního CSIRT týmu v ČR a stanovil určité povinnosti některým osobám, zejména v oblasti hlášení kybernetických bezpečnostních incidentů a také jejich detekce a reakce na ně.

Před tím než se zaměříme na některé podrobnosti zákona o kybernetické bezpečnost. Zkusme ještě chvíli zůstat u organizace kybernetické bezpečnosti. NBÚ totiž tato problematika nezůstala v gesci dlouho. 1.8.2017 bylo totiž NCKB osamostatněno do podoby samostatného správního úřadu známého pod zkratkou NUKIB.

Tento úřad přejímá veškerá práva a povinnosti původního NCKB a dostává některé další úkoly. Osamostatnění také umožnilo vytvořit prostor (vyjádřený počtem pracovních pozic). V současnosti tak NÚKIB zaměstnává něco přes 250 zaměstnanců (stav k roku 2021) s plánovaným cílovým stavem více než 400 zaměstnanců.

Z hlediska činností zajišťuje NÚKIB především:

- provozovat Vládní CERT České republiky (GovCERT.CZ)
- spolupracovat s ostatními národními a mezinárodními CERT a CSIRT týmy
- připravovat bezpečnostních standardů pro informační systémy kritická informační infrastruktura (KII) a veřejný informační systém (VIS)
- osvěta a podpora vzdělávání v oblasti kybernetické bezpečnosti
- výzkum a vývoj v oblasti kybernetické bezpečnosti
- ochrana utajovaných informací v oblasti informačních komunikačních systémů
- kryptografická ochrana

Vzhledem k poměrně vysokému počtu zaměstnanců má NÚKIB také kapacity v případě nutnosti zasáhnout a pomoci organizacím při řešení jejich bezpečnostních incidentů. K tomu je však potřeba dodat, že takový zásah je velmi raritní a je vždy spojován s veřejným zájmem. Z minulosti lze tak zmínit např. pomoc NÚKIB při zvládání infekce ransomware v Benešovské nemocnici, podobný případ v OKD apod.

Z výše uvedeného bychom měli vyvodit, že běžné komerční společnosti na takovou pomoc nedosáhnou ... a je to tak správně.

Z hlediska osob, které podléhají zákonu o kybernetické bezpečnosti, se jedná především o:

a) poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací
b) orgán nebo osoba zajišťující významnou síť
c) správce a provozovatel informačního systému kritické informační infrastruktury,
d) správce a provozovatel komunikačního systému kritické informační infrastruktury,

e) správce a provozovatel významného informačního systému,
f) správce a provozovatel informačního systému základní služby
g) provozovatel základní služby
h) poskytovatel digitální služby

Významnou sítí se ve smyslu zákona rozumí síť, která zahrnuje systémy, zařízení a prostředky pro přenos signálů a vysílání, bez ohledu na druh přenášení informace, jejichž prostřednictvím je kybernetický prostor na území ČR propojen do zahraničí, nebo sítě, které zajišťují připojení kritické informační infrastruktury ke kybernetickému prostoru.

Z definice významné sítě vyplývá, že v podmínkách ČR jich bude relativně málo. První půlka definice se týká připojení kybernetického prostoru ČR do zahraničí - bude se proto týkat zejména Internet Service Provider (ISP) a to jak těch, kteří připojují jednotlivce a firmy (např. Telefónica-O2, UPC a další) tak těch, kteří provozují specializované sítě připojené do zahraničí, např. sdružení CESNET propojující vzdělávací a výzkumné instituce. Druhá půlka definice se týká kritické informační infrastruktury.

Kritickou infrastrukturou rozumíme obecně zvláštní kategorii systémů, které jsou kritické z hlediska udržení základních funkcí státu. Existuje řada definic, které pokrývají různé aspekty kritické infrastruktury (těmi se budete případně zabývat v jiných předmětech), pro účely tohoto předmětu si můžeme kritickou infrastrukturu nadefinovat jednoduše, jako systémy jejich vyřazení by vedlo k velkým ztrátám na životech, hospodářských škodách nebo jinému výraznému poškození zájmů ČR. Původní platná legislativa před zákonem o kybernetické bezpečnosti řešila problematiku kybernetické bezpečnosti v rámci odvětví *Komunikační a informační systémy*, kam spadají technologické prvky [18]:

- pevné sítě elektronických komunikací
- mobilní sítě elektronických komunikací
- sítě rozhlasového a televizního vysílání
- pro satelitní komunikaci
- pro poštovní služby
- informačních systémů

Problémem tohoto pohledu je zejména to, že řešeny jsou především technologické prvky, to odpovídá primárně fyzické ochraně těchto prvků. Problém kybernetické bezpečnosti je ale komplexnější, obsahuje sice složku fyzické ochrany, ale v případě, že daný systém je připojen k Internetu (a v některých případech i když připojen k internetu není) je možno jej kompromitovat čistě softwarovou cestou dálkově. Fyzická bezpečnost je proto sice důležitá a je nutné ji vždy řešit, avšak sama o sobě nemá dostatečný potenciál účinně ochránit zájmová aktiva proti plné škále hrozeb.

Zákon o kybernetické bezpečnosti proto definici kritické infrastruktury rozšiřuje o *systémy kritické informační infrastruktury*, které nejsou tak konkrétně vymezeny jako komunikační a informační systémy, neboť prostupují všechna odvětví kritické infrastruktury. Lze tedy dovodit, že v případě kritické informační infrastruktury se bude jednat o veškeré systémy IT (software i hardware), které řídí nebo „pohánějí“ systémy kritické infrastruktury.

Řízením v tomto případě rozumíme především systémy průmyslové automatizace, které fyzicky řídí výrobní nebo distribuční procesy. Součástí systémů kritické informační infrastruktury budou také systémy, které nespadají do oblasti průmyslové automatizace ale jsou přitom zodpovědné za zajištění fungování určitého odvětví kritické infrastruktury (např. v bankovnictví nebo pojišťovnictví).

Rozlišování kritická infrastruktura (KI) a KII je typické pro Evropské pojetí této problematiky. USA ale proti tomu nepokládají za účelné tyto dva pohledy rozlišovat, jelikož technicky nelze KI provozovat bez KII a KII nemá bez KI smysl. Z tohoto důvodu v USA preferují spíše integrované způsoby řízení bezpečnosti, které berou zřetel jak ne fyzické, tak na informační charakteristiky infrastruktur.

Významným informačním systémem se ve smyslu zákona rozumí informační systém se zásadním významem pro fungování veřejné správy. Do této kategorie budou spadat zcela jistě systémy základních registrů, informačního systému datových schránek a některé z agendových systémů. Kritéria pro rozlišení toho, co do této definice spadá a co ne poskytuje v obecné rovině vyhláška 317/2014 Sb. o významných informačních systémech a jejich určujících kritériích hovoří o systémech.

Do této skupiny ale patří více systému než by se na první pohled mohlo stát. Podle v současnosti používaného výkladu spadají zde také některé systémy, které provozují vysoké školy. Ty bychom si s veřejnou správou na první pohled asi nespojovali. Výklad je založen na tom, že některé činnosti vykonávané univerzitou mají charakter správních rozhodnutí, např. přijetí ke studiu (nebo naopak

jeho ukončení), udělování titulů po absolvování studijních programů apod. Systémy, které tyto agendy zajišťují pak budou splňovat kritéria pro začlenění pod významné informační systémy.

Tady je potřeba podotknout, že legislativa předpokládá, že identifikaci významného informačního systému provede primárně jejich provozovatel sám na základě kritérií specifikovaných ve vyhlášce. V okamžiku, kdy organizace takový systém identifikuje, provede jeho přihlášení na NÚKIB a začne automaticky spadat pod zákon o kybernetické bezpečnosti. V okamžiku přihlášení začíná také běžet jednoletá lhůta, pro naplnění všech požadavků zákona.

Nejzásadnějším požadavkem je přitom zavedení SŘBD, což obvykle není jednoduchá ani levná záležitost. Zákon a jeho prováděcí vyhlášky specifikují základní požadavky na takový systém, nespecifikují ale standard, podle kterého by se mělo postupovat. Organizace se tak mohou rozhodnout implementovat např. systém na bázi ISO 27000, dokonce s možností certifikace (certifikaci systému ale legislativa nevyžaduje), nebo se mohou rozhodnout implementovat vlastní systém.

Systém řízení bezpečnosti informací musí pokrývat minimálně významné informační systémy. Organizace se ale mohou rozhodnout takový systém rozšířit i na další vykonávané činnosti, u kterých to legislativa nevyžaduje. Výhodnost takového postupu můžeme spatřovat v tom, že náklady na zavedení nemusí nutně vzrůstat lineárně s rozsahem SŘBD. Rozšíření systému tak může ve skutečnosti zvýšit efektivitu investice, kterou organizace musí stejně provést.

Alternativní cestou s určení významného informačního systému je forma opatření uloženého NÚKIB. To si lze představit tak, že např. většina vysokých škol si určila významné informační systémy a oznámila je NÚKIB. Některé vysoké školy tak ale neučinily. Vzhledem k tomu, že činnosti realizované na vysokých školách jsou obdobné, lze předpokládat, že budou zajištěny také obdobnými systémy. Z toho může NÚKIB usoudit, že i vysoké školy, které své systémy nevidí jako významné, je vlastně provozují a může se tak domáhat splnění povinností pro jejich zajištění.

Zákon o kybernetické bezpečnosti dává do rukou NÚKIB (prostřednictvím GovCSIRT.CZ) do rukou možnost vydávat varování stran odhalených zranitelností systémů nebo hrozící možnosti jejich zneužití (hrozícím útokem). NÚKIB má také právo nařídit reaktivní a ochranná opatření.

Reaktivní opatření reaguje na probíhající útok - jeho cílem je útok zastavit a nebo omezit jeho dopady. Účelem *ochranného opatření* je preventivně zabránit nebo ztížit útok na zájmový systém. Opatření k zavedení SŘBD řadíme právě do kategorie ochranných opatření.

Provedení opatření může nařídit NÚKIB pouze zájmovým osobám (dle seznamu výše). Platnost nařízení je 3 dny od vyvěšení na úřední desce, ovšem s tím, že NÚKIB má za povinnost pokusit se doručit nařízení do vlastních rukou. Zájmová osoba pak musí hlásit výsledek realizace nařízeného opatření. Poskytování zpětné vazby je tedy povinnou součástí celého procesu. V případě neplnění opatření umožňuje legislativa NÚKIB udělit pokutu a to až do výše 1 000 000 Kč.

Posledním, ale také nejmocnějším, nástrojem je možnost vyhlásit **stav kybernetického nebezpečí**. Tento stav je možné vyhlásit v případě, že je ve velkém rozsahu ohrožena bezpečnost informací v informačních systémech nebo bezpečnost a integrita služeb nebo sítí elektronických komunikací a tím by mohlo dojít k porušení/ohrožení zájmu České republiky ve smyslu zákona na ochranu utajovaných informací.

Na první pohled nemusí být návaznost na tento zákon zřejmá, tady je potřeba říci, že nejde (!) primárně o ochranu utajovaných skutečností, ale jiný koncept, který je v zákoně extenzivně řešen a to *chráněné zájmy*. Vzhledem k tomu, že většina činností, které pro realizaci těchto zájmů stát vykonávána je realizována v kyber prostoru, je logické že potřebujeme nástroje, které budou použitelné pro ochranu tohoto prostoru.

Nouzový stav, nebo podobné stavy definované krizovým zákonem k tomuto účelu nestačí, neboť se soustředí především na fyzickou rovinu problému. Zákon o kybernetické bezpečnosti tak doplňuje právě aspekt ochrany kyberprostoru.

Během stavu kybernetického nebezpečí spadá pod pravomoc NÚKIB širší skupina zájmových osob, které pak může taktéž nutit je spolupráci ve smyslu možnosti nařizování provedení opatření. Tento stav vyhlašuje ředitel NÚKIB na dobu maximálně sedmi dní. Tuto dobu je ale možno opakovaně prodlužovat maximálně však do celkové výše jednoho měsíce.

Zkušenosti z nasazení tohoto stavu ale v současnosti nejsou, neboť tento stav dosud (2022) nebyl vyhlášen.

V blízké budoucnosti dojde k novelizaci zákona v souvislosti se vstupem v platnost Evropského nařízení NIS2. V souvislosti s ním dojde k významnému rozšíření povinných osob a také ke změně pohledu na požadovanou úroveň zabezpečení.

Z hlediska osob tak aby byla komplexně pokryta všechna odvětví, které mají zásadní význam pro

klíčové společenské a hospodářské činnosti v rámci vnitřního trhu EU. Očekává se, že pouze v ČR tak spadne pod působnost zákona nově více než 5 000 organizací.

Dvourychlostní bezpečnost vychází z nového dělení služeb na základní a důležité (v současnosti zákon takové dělení nezná). Do *základních služeb* budou zařazeny služby odpovídající současné právní úpravě a nově také:

- energetika - pododvětví dálkového vytápění, chlazení a vodíku.
- zdravotnictví - referenční laboratoře EU, subjekty provádějící výzkum, výrobu léčiv, výroba zdravotnických prostředků
- pododvětví odpadních vod
- digitální infrastruktura - poskytovatelé služeb cloud computingu, služeb datových center, sítí pro doručování obsahu, služeb vytvářejících důvěru, veřejných sítí elektronických komunikací, služeb elektronických komunikací
- veřejná správa - ústřední subjekty veřejné správy, orgány samosprávy
- vesmír - pozemní infrastruktury podporující využívání kosmického prostoru

Do *důležitých služeb* pak bude spadat:

- poštovní a kurýrní služby,
- nakládání s odpady,
- výroba, produkce a distribuce chemických látek,
- výroba, zpracování a distribuce potravin,
- výroba (zdravotnických prostředků a diagnostických zdravotnických prostředků in vitro; počítačů, elektronických a optických přístrojů a zařízení; elektrických zařízení; strojů a zařízení j.n. (tj. strojů a zařízení, které mechanicky nebo tepelně působí na materiály nebo na materiálech provádějí výrobní procesy); motorových vozidel; přívěsů a návěsů a ostatních dopravních prostředků a zařízení),
- digitální služby (poskytovatelé online tržišť, internetových vyhledávačů a platforem služeb sociálních sítí).

Požadavky na zabezpečení důležitých služeb budou mnohem nižší než na zabezpečení služeb základních.

8.2 CERT a CSITR týmy a jejich význam

Jak bylo zmíněno v předchozí podkapitole, významnými hráči na poli kybernetické bezpečnosti jsou CERT a CSIRT týmy. Primárním úkolem takových týmů je především informování o možných hrozbách a také způsobu ochrany proti nim. Typově lze CERT/CSIRT týmy rozlišit následovně:

- vládní
- národní
- resortní
- týmy jednotlivých organizací

Státy obvykle mají pouze jeden vládní a jeden národní CERT/CSIRT tým. Ostatních týmů může být více. Z předchozí kapitoly víme, že funkci vládního týmu plní GovCSIRT.CZ provozovaný NBÚ v rámci NCKB, proto se zaměříme především na národní tým.

V České Republice roli národního Computer Security Incident Response Team (CSIRT) týmů zastává CSIRT.CZ provozovaný sdružením CZ.NIC od 1. ledna 2011. Obdobný národní tým v USA US-CERT vznikl už v roce 2008 (už od 80. let 20. století ale fungoval Computer Emmergency Response Team (CERT) při Carnegie Mellon Universitě). V Polsku CERT.GOV.PL vznikl v roce 2008, na Slovensku CSIRT.SK byl zřízen nařízením vlády 479/2009 Sb. [29].

Role jednotlivých CSIRT týmů může být odlišná, například CSIRT.CZ popisuje [5] svoji roli následovně:

- Udržování zahraničních vztahů - se světovou komunitou CSIRT týmů a organizacemi, které tuto komunitu podporují.
- Spolupráce se subjekty v rámci ČR - ISP, poskytovateli obsahu, bankami, bezpečnostními složkami, akademickým sektorem, úřady státní správy a dalšími institucemi.
- Poskytování služeb v oblasti bezpečnosti:
  - Řešení a koordinace řešení bezpečnostních incidentů

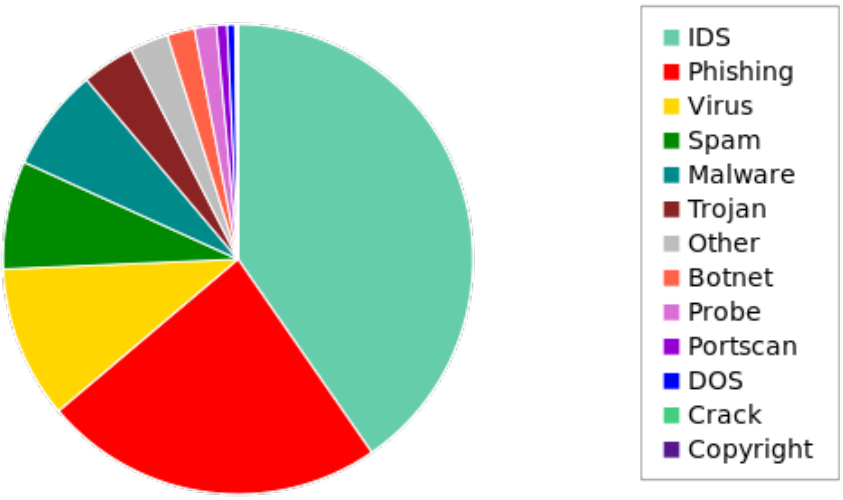
– Osvětová a školící činnost
– Proaktivní služby v oblasti bezpečnosti

Národní govCERT.cz hraje klíčovou roli při ochraně kritické informační infrastruktury a významných informačních systémů. Účelem je efektivně čelit bezpečnostním výzvám, reagovat na incidenty, koordinovat činnosti při jejich řešení a účelně působit při předcházení incidentům. Tým také působí jako prvotní zdroj bezpečnostních informací a pomoci pro orgány státu, organizace i občany. Neméně důležitou roli hraje při zvyšování vzdělanosti v oblasti bezpečnosti na internetu.

Efektivita výše uvedeného je zaručena poměrně silným zmocněním v zákoně o kybernetické bezpečnosti, zejména pravomocemi, kterými je vybaven NÚKIB, který tento tým provozuje.

US-CERT definuje [79] své poslání jinak: Posláním US-CERT je zlepšit národní postavení v oblasti kyber bezpečnosti, koordinovat sdílení informací a proaktivní řízení kyber rizik ohrožující USA při ochraně ústavních práv Američanů. Vizí US-CERT je stát se důvěryhodným globálním vůdcem v oblasti kyber bezpečnosti – spolupracující, agilní a pružný v komplexním prostředí.

CSIRT týmy menších států pochopitelně nemohou aspirovat na vedoucí úlohu v oblasti IT bezpečnosti, ale řada činností by se měla překrývat. Činnost jednotlivých týmů lze zkoumat pomocí statistik a analýzou činnosti na domácích stránkách týmů. Rozložení řešených bezpečnostních incidentů týmu CSIRT.CZ je znázorněn na obr. 8.1.



Obrázek 8.1: Typové rozložení řešení bezpečnostních incidentů týmu CSIRT.CZ v letech 2008-2011 (převzato z [51])

Většinu bezpečnostních incidentů připadá na detekované průniky do sítí následované phishingovými útoky a napadení různými typy malware. CSIRT tým pracuje tak, že upozorní správce zdrojové sítě útoku a pomůže (informační podpora) případně s identifikací problému.

Postavení CSIRT.CZ
Národní tým CSIRT.CZ je zajišťován nestátní organizací - může se jednat o soukromou firmu, sdružení osob apod. Jelikož národní CSIRT tým může být pouze jeden, výběr organizace, která jeho provoz zajistí probíhá výběrovým řízením. To je celkem paradoxní situace, protože aby byl CSIRT tým funkční, musí spolupracovat se zahraničím. Aby mohl spolupracovat se zahraničím, musí být sdružen v některém mezinárodním uskupení takových týmu. Paradox spočívá v tom, že provoz CSIRT týmu je brán jako služba.

CERT.GOV.PL [48] kromě standardní minimální úrovně služeb (jak je realizována např. týmem CSIRT.CZ), poskytuje ještě aktuální informace, doporučené nástroje, doporučení na konfigurace systémů a také zpracovávání bezpečnostních incidentů ARAKIS-GOV [47].

CSIRT.SK jako slovenský národní CSIRT tým byl akreditován teprve v polovině roku 2011, přesto poskytuje oznámení a varování, základní návody a doporučení pro konfiguraci a zabezpečení IT aktiv.

Jako etalon toho, jaký typ informací může poskytovat CERT, lze použít US-CERT [80]. Tento národní tým poskytuje údaje o hrozbách a zranitelnostech, aktualizacích, ale také aktivitách a dalších zdrojích a to v úpravě pro techniky (IT odborníky), netechniky (domácí a podnikové uživatele), státní správu a samostatně řeší také bezpečnost řídicích systémů.

Bez ohledu na to, jaké přesně úkoly CSIRT tým dostává od svého zřizovatele, existují některé úkoly, které mají všechny týmy a to především sloužit jako místo pro reportování bezpečnostních incidentů a být nápomocni při jejich řešení. K tomuto účelu je ale vyžadováno, aby jednotlivé CSIRT byly certifikovány, tedy aby někdo ručil za to, že CSIRT tým je skutečně určen pro řešení takových problémů, a zájemce o využití služeb tak získal určitou jistotu, že důvěrné informace o bezpečnostním incidentu nepadnou do nepovolaných rukou.

Pro tyto účely se uznávané CSIRT týmy sdružují do různých mezinárodních uskupení. Na úrovni EU funguje ENISA [**?**]. ENISA jako instituce je poradním orgánem Evropské komise v oblasti IT bezpečnosti, zabývá se také organizací konferencí, seminářů, školení a cvičení pro národní CSIRT týmy.

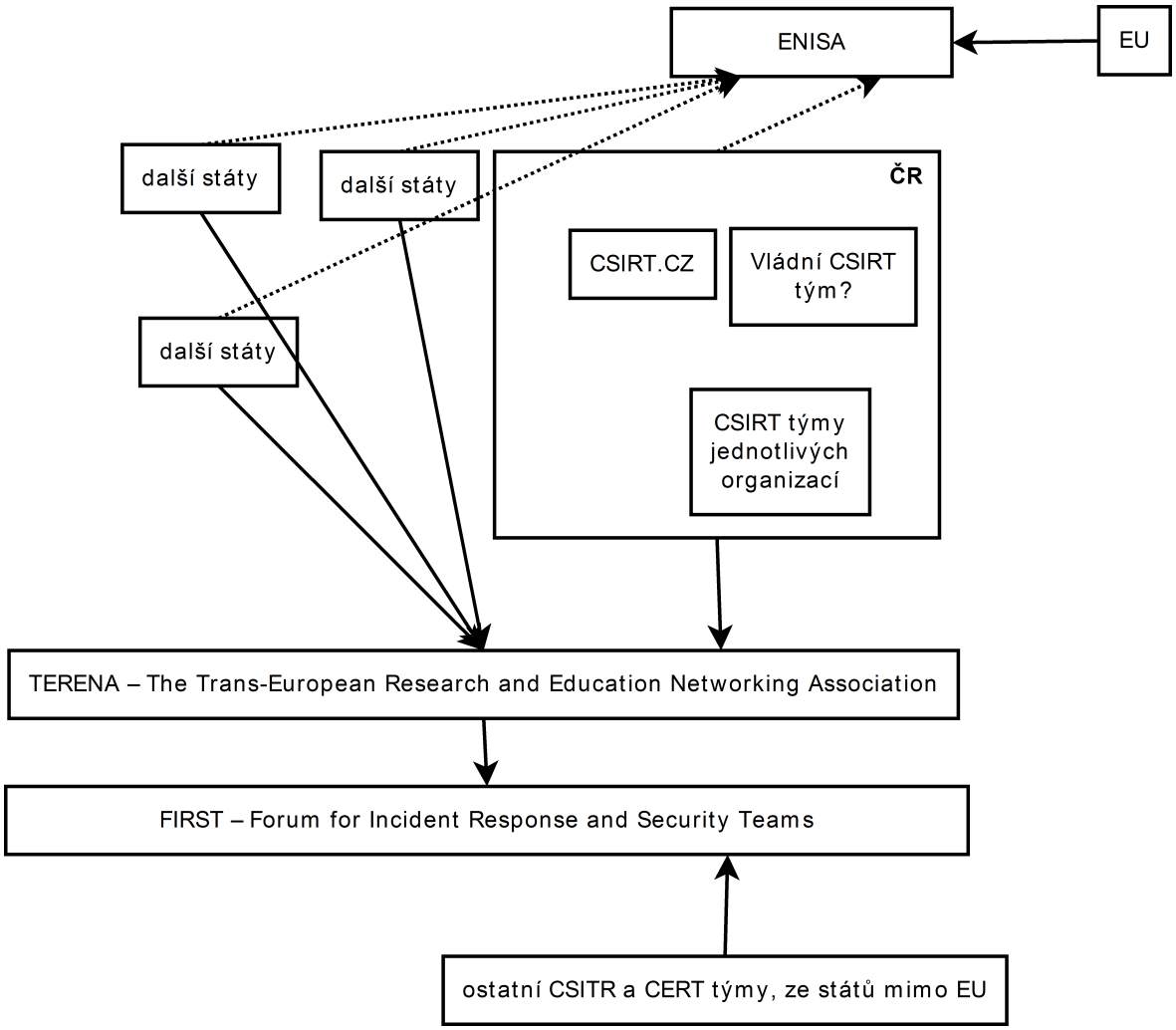
CSIRT týmy samotné se v Evropě sdružují do organizace The Trans-European Research and Education Networking (TERENA) [**?**] jako platformy zprostředkovávající výměnu bezpečnostně orientovaných informací, školení apod. mezi CSIRT týmy.

Samotná registrace je realizována pomocí mezinárodní organizace Forum for Incident Response and Security Teams (FIRST) [**?**]. Pro registraci je nutné, aby se za uchazeče o registraci zaručil nějaký již uznávaný člen fóra. Tímto způsobem se zajišťuje jeden z pilířů spolupráce – dobrá komunikace na mezinárodní úrovni. CSIRT tým tedy musí nejprve navázat „neformální“ spolupráci s jinými CSIRT týmy a teprve poté se může ucházet o registraci v rámci FIRST.

Schematicky si můžeme spolupráci na mezinárodní úrovni představit podobně jako na obr. 8.2.

K CERT/CSIRT týmům, lze také říci, že tvoří pouze část celkového řešení kybernetické bezpečnosti. Národní strategie kybernetické bezpečnosti [67] definuje celkový kontext kybernetické bezpečnosti podobně jako na obr. 8.3.

Pro plné rozebrání celkového obrazu zajištění kybernetické bezpečnosti v ČR, ale bohužel na těchto stránkách není dost prostoru.

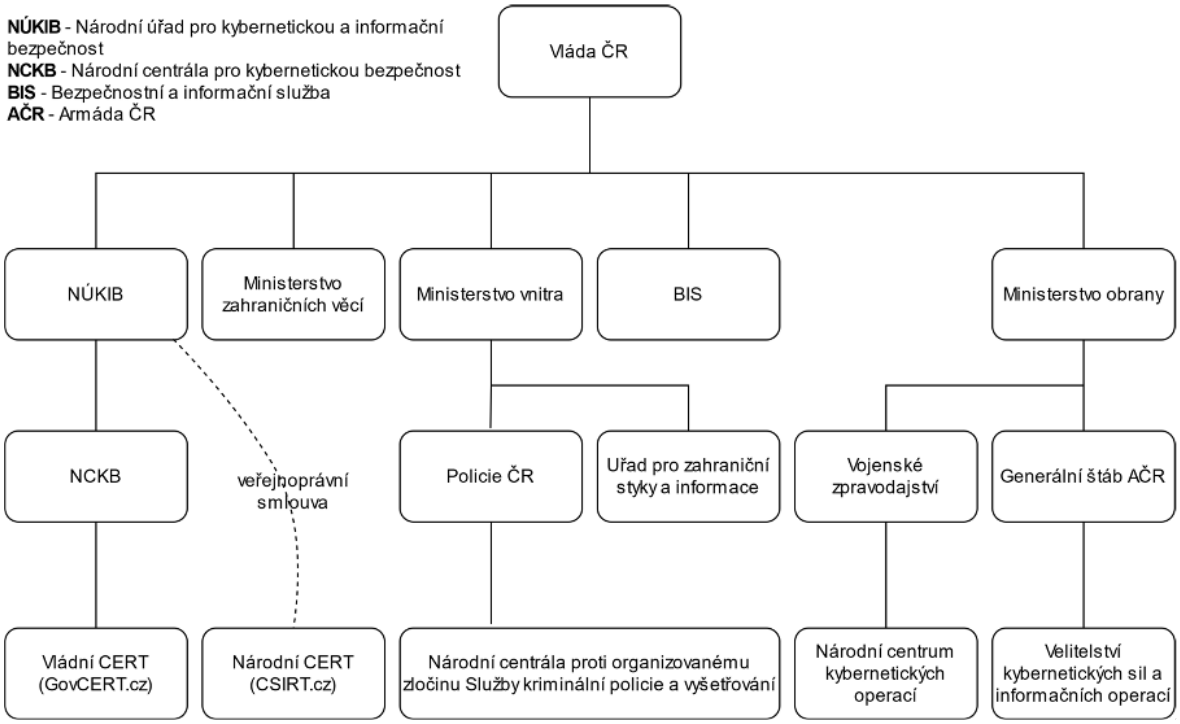


Obrázek 8.2: CSIRT týmy – mezinárodní spolupráce

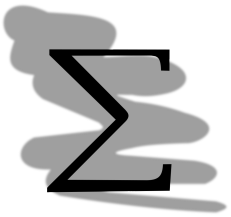
Národní vs vládní CSIRT tým

Národní CSIRT tým slouží pro řešení bezpečnostních incidentů na národní úrovni. Jeho uživateli tak mohou být soukromníci, firmy, ale také slouží jako kontaktní místo pro zahraniční CSIRT týmy, které řeší bezpečnostní incidenty s přesahem do ČR.

Funkce vládního týmu je ale definována mnohem úžeji. Slouží pro řešení bezpečnostních incidentů ve státní správě popř. samosprávě. Vládní CSIRT tým je obvykle provozován státem a jako takový má ve veřejném sektoru mnohem větší pravomoci než národní CSIRT tým vůči sektoru privátnímu.



Obrázek 8.3: Celkový kontext zajištění kybernetické bezpečnosti v ČR (adaptováno z [67])



Shrnutí

Problematika kybernetické bezpečnosti je z hlediska legislativního řešení relativně mladá. Zákon o kybernetické bezpečnosti vešel v platnost teprve počátkem roku 2015. Zakotvuje postavení národního (CSIRT.CZ) a vládního (GovCSIRT.CZ) CSIRT týmu. Vládní tým je provozován Národním centem pro kybernetickou bezpečnost (pod NBÚ).

Zákon dává možnosti NBÚ v případě ohrožení kritické informační infrastruktury popř. významných informačních systémů nařizovat opatření reaktivní a ochranná. V případě, že ohrožení přesáhne určitou mez, může být vyhlášen stav kybernetického nebezpečí dávající do rukou NBÚ možnost donutit ke spolupráci širší okruh zájmových osob. Tento stav může být vyhlášen maximálně na dobu jednoho měsíce.

Kontrolní otázky

1. Jaké jsou rozdíly v pravomocech národního a vládního CSIRT týmu?
2. Co rozumíme pojmem významný informační systém?
3. Co rozumíme pojmem významná síť?

Odpovědi

1. Národní CSIRT tým je primárně zaměřen na informování a spolupráci v oblasti běžných bezpečnostních incidentů, které nejsou zaměřeny např. na kritickou infrastrukturu. Národní CSIRT tým také nemá žádné faktické pravomoci.
2. Významným IS rozumíme, takové IS, bez kterých by veřejná správa nemohla vykonávat svou funkci (ve smyslu povinností uložených platnou legislativou).
3. Významnou sítí se rozumí takové sítě, které zajišťují připojení (datové, telekomunikace obecně) do zahraničí.

Kapitola 9

Rychlé informace

Náhled kapitoly
Problematikou rychlých informací vybočujeme lehce z oblasti informačních technologií a dostáváme se do mnohem obecnější oblasti. Rychlými informacemi máme na mysli použití barev, piktogramů apod., které na první pohled dávají informaci, která člověka nacházejícího se v dané oblasti nutná.

Po přečtení kapitoly budete
Vědět

1. jakým barvy se používají pro označování prostor a proč
2. proč jsou rychlé informace důležité
3. co všechno lze ještě zařadit mezi rychlé informace

Znát

1. vzhled nejběžnějších typů značek

Čas pro studium
Pro prostudování této kapitoly budete potřebovat přibližně 45 minut.

9.1 Úvod

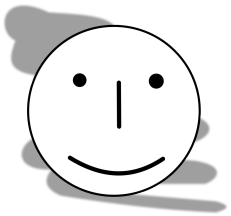
Koncepce rychlých informací vychází z toho, jakým způsobem člověk vnímá barvy, tvary a zvuky. Jedná se vlastně o přímé dědictví od našich zvířecích předků. Všechny tyto vjemy jsou vyhodnocovány jako signály o různé intenzitě. Na našich pudech popřípadě výcviku záleží, jak na tyto signály budeme reagovat.

Tyto vjemy lze rozdělit do několika kategorií podle smyslů, které je přijímají:

1. hmat
2. čich
3. sluch
4. zrak
5. chuť

Z hlediska rychlých informací, tedy alespoň jejich formalizované podoby bychom mohli takřka vyloučit čich a chuť.

Ačkoliv ani ten případ s plynem není úplně bez rychlých informací. Do zemního plynu se schválně z důvodu jednoduchosti detekce přimíchávají chemická látka thiol, jelikož zemní plyn samotný je bez



Přestávka
Poslední slova
. . . hele cítím plyn . . .
. . . jo, já ho taky cítím . . . počkej, škrtnu zápalkou, ať vidíme, odkud to jde . . .

nebo

Vidíš jak je ta smaženice dobrá? Ale je pravda, že ty žampiony vypadaly divně . . .

chuti a zápachu. Právě thiol zajišťuje typickou „vůni“ zemního plynu. Toto by že se dalo považovat za jistý druh rychlé informace.

Zbývá nám tedy zrak, sluch a hmat. Hmat se může zdát být podobně nepoužitelný jako chuť a čich, ale nevidomí nebo slabozrací spoluobčané jsou nuceni na něj spoléhat. Do této kategorie můžeme zařadit např. speciální dlažbu s výstupky označující, že se nevidomý nachází na chodníku, zvukovou signalizaci na přechodu pro chodce a podobně.

Z hlediska rychlých informací nás především bude zajímat zrak a sluch. V případě zraku je to pak zejména schopnost barevného vidění.

Například červená – barva krve, byla signálem, že na daném místě se něco a je třeba dávat vetší pozor popřípadě se místu kompletně vyhnout.

Z tohoto hlediska:
Červená barva – nebezpečná oblast
Žlutá barva – pozor, všimni si mě
Zelená barva – bezpečí, následuj mě a nic se ti nestane

9.2 Nařízení vlády 11/2002 Sb.

Pocity člověka z barev, které mohou být do značné míry individuální, nelze brát bez další normalizace. Právní předpis, který upravuje vzhled, umístnění značek je nařízení vlády 11/2002 Sb. [19]. Barvy a jejich významy viz. tab. 9.1.

Tabulka 9.1: Tabulka barev značek a světelných signálů (převzato z [19])

Barva	**Význam nebo účel**	**Pokyny a informace**
červená	Značka zákazu	Nebezpečné chování
	Signalizace nebezpečí	Zastavit přerušit práci bezpečnostní pojistka opustit prostor
	Věcné prostředky PO a bezpečnostně požární zařazení	Označení a umístnění
žlutá oranžová zelenožlutá	Značka výstrahy	Buď opatrný Připrav se Ověř si
modrá	Značka příkazu	Určité chování nebo postup Použij OOPP
zelená	Značka nouzového východu Značka první pomoci	Označení dveří, východů, cest, zařízení, vybavení
	Bezpečí	Návrat k běžnému stavu

V praxi by například značení nějaké překážky (schod, kanálek upevněný na zemi pro vedení elektrické sítě apod.) vypadal podobně jako na obr. 9.1.

Značky zákazu jsou vyvedeny v kruhovém tvaru s červeným okrajem a červeně přeškrtnutou činností, která je zakázána, viz například obr. 9.2.

Značky výstrahy jsou zpracovány v trojúhelníkovém tvaru se žlutým pozadím, černým okrajem se znázorněným symbolem nebezpečí, na které si takto značeném prostoru máme dát pozor (viz obr. 9.3).

Obrázek 9.1: Příklady použití barev pro značení

Obrázek 9.2: Příklady značek zákazu

Značky příkazu jsou kulovitého tvaru s modrým pozadím a graficky znázorněným co musí člověk udělat pro svou bezpečnost (viz obr. 9.4).

Informativní značky slouží pro označení únikových cest a nouzových východů nebo míst první pomoci a zařízení pro přivolání první pomoci (viz obr. 9.5).

Uvedené značky nejsou kompletním výčtem používaných značek, pouze jejich reprezentativním výběrem. Kompletní výčet je obsažen v přílohách nařízení vlády 11/2002 Sb. [19].

Bezpečnost ovšem není jediná oblast, kde se normalizované značení používá. Například protokol PECA (protokol k Evropské dohodě o posuzování shody a akceptaci průmyslových výrobků) ukládá výrobcům dávat na své výrobky značku CE jako rychlou informaci zákazníkovi, že daný výrobek splňuje základní požadavky nařízení vlády (viz. obr. 9.6).

Různých druhů značení je pravděpodobně stejně jako různých druhů lidské činnosti. Do kategorie rychlých informací bychom proto mohli zařadit například i značku Bio – označující ekologicky šetrně vyrobené potravinářské výrobky, nebo také punc vyražený na šperku pro rychlé určení drahého kovu, ze kterého byl vyroben.

Sluch je pro člověka stejně důležitý nebo možná důležitější smysl než zrak. Ucho jako sluchový orgán člověka je schopno ze zachycených zvuků zjistit směr odkud zvuk vychází a přibližnou vzdálenost zdroje zvuku. Člověk je také schopen si ve změti zdrojů vybrat jeden a ostatní zdroje „odfiltrovat“.

Zvukové signály jsou velmi často využívané pro poskytování rychlých informací. Klakson automobilu má jediný účel – říct tady jsem, dej na mě pozor. Mezi zvukové rychlé informace lze nepochybně zařadit například i sirény CO.

Je vědecky dokázáno, že člověk věnuje větší pozornost kombinovaným vjemům, tedy takovým vjemům, které zaznamenává více než jeden smysl. Na stejném principu je založeno i učení – je rozdíl, pokud si látku pouze čteme, a nebo zároveň k ní máme puštěnu audio nahrávku (např. výuka jazyků).

Tohoto principu využívají například i automobily záchranných služeb, které mají zároveň spuštěn maják i sirénu.

Obrázek 9.3: Příklady značek výstrahy

Obrázek 9.4: Příklady značek příkazu

Uvedené principy mají nepopiratelný význam pro návrh uživatelského rozhraní specializovaných systém, jejichž obsluha musí rychle reagovat na nějakou událost. Typicky se v průmyslu může jednat o vizualizace technologických procesů. Obsluha má k dispozici grafický výstup na obrazovku, který pro člověka přijatelným způsobem zobrazuje ukazatele sledovaného procesu. Přitom se neočekává, že by obsluha věnovala příliš pozornosti jednotlivým ukazatelům – sleduje pouze, zda se „nerozsvítila“ červená kontrolka signalizující, že něco není v pořádku.

V tomto okamžiku pracovník teprve studuje jednotlivé ukazatele a zjistí příčinu problému. Včasná indikace problému zabrání finančním ztrátám způsobeným například výpadky technologie apod.

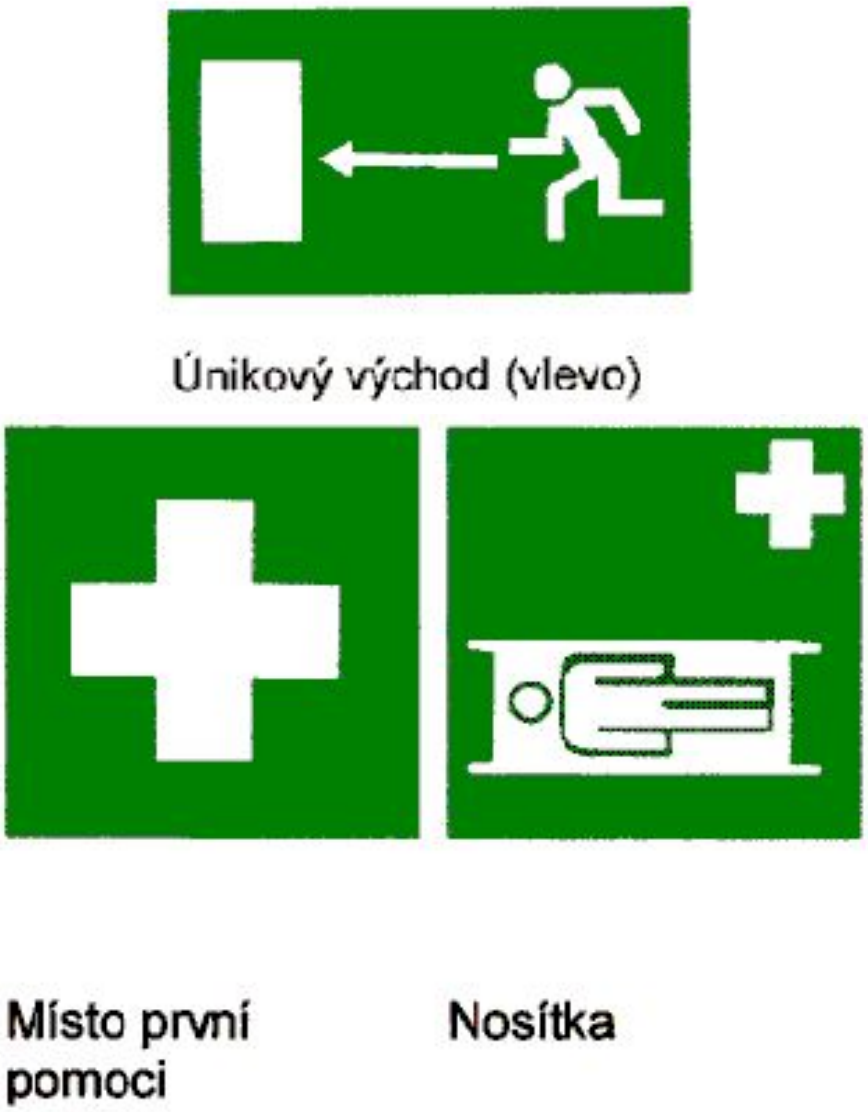
9.3 Nebezpečné látky – rychlé informace

Jako základní identifikátory slouží tři položky a to *CAS číslo*, *ES číslo* a *indexové číslo*. *Indexové číslo* se udává ve tvaru **ABC-RST-VW-Y**, kde číslo ABC udává atomové číslo prvku charakterizujícího látku. Číslo RST představuje pořadové číslo v sérii ABC a VW označuje formu v jaké je látka dodávána na trh. Poslední číslo Y plní kontrolní funkci – jedná se o kontrolní součet, vypočítaný metodou ISBN.

ES číslo neboli tzv. *Einecs číslo*, se přiděluje látkám, které jsou na seznamech látek, který v ČR ze zákona udržuje Ministerstvo životního prostředí. Konkrétně se jedná o tři rejstříky: seznam nových látek ELINCS (400-010-9 a vyšší), seznam látek, které nadále nejsou považovány za polymery NLP (500-001-0) a seznam obchodovatelných látek (200-01-8). ES číslo je přitom přidělováno látce bez ohledu na to zda je hydratovaná nebo ne.

Z předchozích odstavců vyplývá, že ani ES ani indexové číslo nemohou zajistit jednoznačnou identifikaci látky, lze je však použít lépe než např. *UN kód*. Látku jednoznačně identifikuje *CAS číslo*.

CAS číslo je unikátní číselný identifikátor chemických sloučenin. CAS čísla jsou přidělována divizí American Chemical Society, která se nazývá Chemical Abstract Service, s cílem jednoznačně identifikovat kteroukoliv chemickou látku, která kdy byla popsána. Počátkem prosince 2005 takto bylo přiděleno více než 27 miliónů čísel.



Obrázek 9.5: Příklady informativních značek

CAS číslo obsahuje tři části oddělené pomlčkou. První část se může skládat až z šesti číslic, druhá obsahuje dvě číslice a konečně třetí část obsahuje pouze jedinou číslici a slouží jako kontrolní součet.

UN číslo je čtyřciferný identifikátor nebezpečných látek a zboží v souvislosti s mezinárodní přepravou. UN čísla v intervalu 0001 – 3500 jsou přidělována výborem expertů pro přepravu nebezpečných materiálů při OSN (United Nations Committee of Experts on Transport of Dangerous Goods). Seznam UN čísel tito experti zveřejnili v tzv. Oranžové knize (Recommendations on the Transporttation of Dangerous Goods).

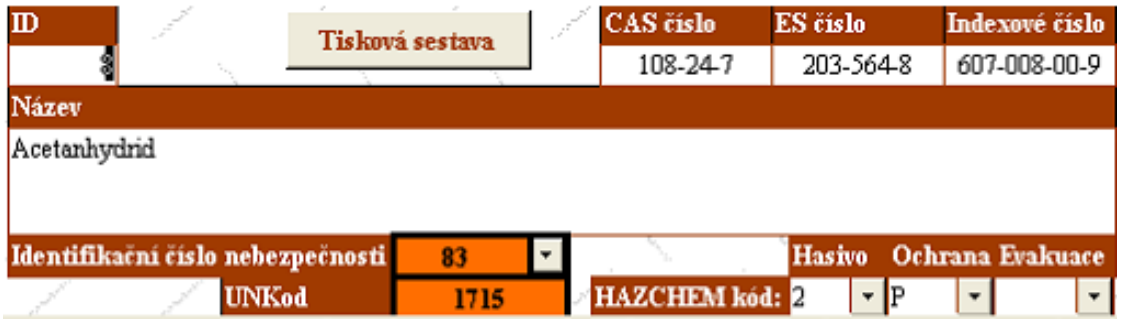
Kromě UN čísel se používají také tzv. NA čísla (North America (NA)), která jsou také známa pod označením DOT čísla. NA čísla přiděluje ministerstvo dopravy USA (Department of Transportation (DOT)). NA čísla jsou kompatibilní s UN čísly, v tom smyslu, že NA a UN čísla jsou totožná s výjimkou některých látek, které nemají UN číslo, ale mají NA číslo.

Identifikační číslo nebezpečnosti (dříve označováno jako tzv. *Kemler kód*), slouží k rychlému určení nebezpečí v případě havárie nebo požáru nebezpečných látek.

Tzv. *HAZCHEM* kód se používá zejména ve Velké Británii, ale pro jeho snadnou interpretovatelnost se postupně rozšířil i do dalších zemí. HAZCHEM kód je tvořen trojicí čísel udávajících hasivo – ochranu – evakuaci.

Značení prostřednictvím Diamantu prosadila v USA National Fire Protection Association (NFPA), vzhledem k tomu, že se jedná o jednoduchý a přitom spoustu informací poskytující systém, prosadil

Obrázek 9.6: Značka CE dle protokolu PECA



Obrázek 9.7: Příklad Identifikátorů nebezpečné látky – převzato z databáze Nebezpečné látky 2005 [86]

se tento způsob značení i mimo území USA.

Jednotlivé kvadranty Diamantu mají přitom následující význam:

1. modrá – zdraví
2. červená – nebezpečí požáru
3. žlutá – reaktivita
4. bílá – speciální ustanovení

Do každého kvadrantu s výjimkou bílého se přiřazuje číselné vyjádření nebezpečnosti, přičemž čím vyšší číslo, tím vyšší nebezpečí (ohrožení zdraví, požáru, ...).

V bílém kvadrantu jsou pak obsažena speciální ustanovení označovaná písmeny. Přeškrtnuté W (z technických důvodů v databázi pouze W) např. znamená zákaz použití vody pro sanaci látky.

ADR je Mezinárodní úmluva o pravidlech přepravy po silnici a *RID* je její obdoba pro železnici. Tato smlouva upravuje značení vybraných nebezpečných látek pro účely jejich přepravy.

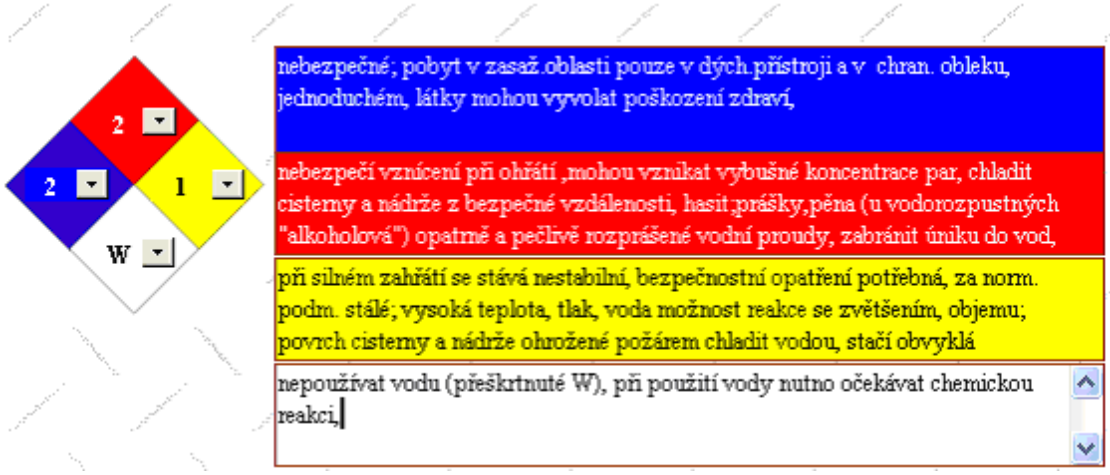
Definuje tzv. *třídy nebezpečnosti*, které jsou vizualizovány na přepravních kontejnerech, cisternách apod. prostřednictvím nálepek, viz. obr. 9.9.

Legislativa u nás i ve světě také upravuje oblast označování látek výstražných symbolů a R a S větami.

R věty slouží pro bližší specifikaci nebezpečí, které představuje nebezpečná látka (R = risk). Pro bližší specifikaci ochranných opatření se používají tzv. *S věty* (S = safety). R a S věty jsou tvořeny označením R resp. S a číslem. Ke každé kombinaci označení a čísla je přiřazen výklad, např. R1 – výbušný v suchém stavu. Existují i tzv. kombinované R a S věty, např. R14/15 – prudce reaguje s vodou za uvolňování extrémně hořlavých plynů.

R2 - Nebezpečí výbuchu při úderu, tření, ohni nebo působením jiných zdrojů zapálení.

S2 - Uchovávejte mimo dosah dětí.



Obrázek 9.8: Příklad Diamantu s vysvětlením významu – převzato z databáze Nebezpečné látky 2005 [86]

S9 - Uchovávejte obal na dobře větraném místě.

V souvislosti s postupným náběhem chemické legislativy REACH se budou zavádět různé změny v pro specifikaci nebezpečí a proto R a S věty budou do roku 2015 kompletně nahrazeny *H* (H = Hazard) a *P* (P = Protection) *větami*, kterých je více a jsou jiného znění, svým základním smyslem jsou ovšem stejné (R -> H, S -> P)[1].

Výstražné symboly jsou označeny písmenem, slovním popisem vlastnosti látky, která je považována za nebezpečnou a jejich grafickým znázorněním, např. E – výbušný. Platné výstražné symboly jsou zobrazeny na obr. 9.10.

Změně bude podroben i systém označování výstražných symbolů, viz. obr. 9.11. Tyto symboly budou univerzální a budou celosvětově platné celosvětově dohoda GHS, EU implementace je známa pod zkratkou CLP).

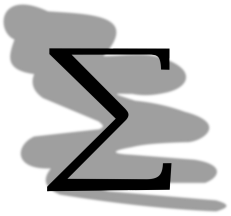
Systém rychlých informací může být součástí specializovaných informačních systémů např. pro záchranáře při zásahu pro zjištění vlivu uniklé chemické látky na zdraví apod.

[1] ačkoliv základní filozofie zůstává stejná, samotné znění jednotlivých vět se mění

Obrázek 9.9: Třídy nebezpečnosti

Obrázek 9.10: Výstražné symboly

Obrázek 9.11: Výstražné symboly dle legislativy CLP



Shrnutí

Z hlediska legislativy jsou rychlé informace řešeny např.:

1. nařízením vlády 11/2002 Sb.
2. Mezinárodní úmluvou o přepravě nebezpečných látek ADR, RID
3. a dalšími právními normami a mezinárodními úmluvami (např. dohoda PECA)

Nařízení vlády rozlišuje čtyři druhy značek

1. zákazu
2. výstrahy
3. příkazu
4. informativní

Jednotlivé značky se liší tvarem a barvami.
Pro identifikaci nebezpečných látek lze využít UN, ES, CAS, indexová čísla, přitom pouze CAS číslo poskytuje jednoznačnou identifikaci nebezpečné látky.
Z hlediska bezpečnosti jsou důležité vlastnosti a způsoby ochrany před účinky nebezpečných látek identifikovány pomocí R a S vět, identifikačního čísla bezpečnosti, výstražných symbolů a nálepek. Legislativa REACH a především CLP zavádí vlastní systém výstražných symbolů a používá H a P věty pro specifikaci ohrožení látkami a možností ochrany před jejich negativními účinky.

Kontrolní otázky

1. Jaké jsou barvy nebezpečí, výstrahy a bezpečí?
2. Co jsou to R a S věty?
3. Jaké informace poskytuje Diamant?
4. Jak se liší UN a DOT čísla?
5. Jaké rychlé informace mohu použít pro identifikaci škodlivých vlastností nebezpečných látek?

Správné odpovědi

1. nebezpečí – červená, výstrahy - žlutá, bezpečí – zelená
2. Identifikují riziko nebezpečné látky, S věty identifikují prostředky ochrany před účinky nebezpečné látky.
3. Ohrožení zdraví, nebezpečí požáru, reaktivita a speciální ustanovení (např. zákaz požití vody).
4. UN přijatá OSN, DOT přijatá Ministerstvem dopravy USA a obsahují UN čísla a některá další čísla pro další látky.
5. R nebo H věty, Diamant, HAZCHEM, identifikační číslo nebezpečnosti, výstražné symboly, třídy nebezpečnosti.

Test

1. Které z následujících čísel jednoznačně identifikuje nebezpečnou látku
   (a) CAS
   (b) ES
   (c) UN
2.  je značka:
   (a) zákazu
   (b) výstrahy
   (c) příkazu
3. Výstražné symboly obsahují
   (a) Obrázek
   (b) Písmeno nebezpečí, obrázek
   (c) Písmeno nebezpečí, obrázek, popis rizika
4. Diamant obsahuje barvy
   (a) Bílou, žlutou červenou, modrou,
   (b) Bílou, modrou, černou, červenou
   (c) Žlutou, červenou, fialovou, bílou
5. Číslo 0115 může být číslem
   (a) CAS
   (b) ES
   (c) UN

Správné odpovědi

1. a), 2. b), 3. b), 4. a), 5. c)

Kapitola 10

Budoucnost výpočetní techniky aneb počítáme netradičně

Náhled kapitoly
V této kapitole se seznámíte s možnou budoucností IT. Budeme hovořit zejména o pokročilých výpočetních systémech na bázi DNA a kvantových počítačů.

Po přečtení kapitoly budete
Vědět

1. co znamenají pojmy DNA počítač a kvantový počítač a proč se o nich má vůbec smysl bavit

Čas pro studium
Na prostudování této kapitoly budete potřebovat přibližně 30 minut.

10.1 DNA počítače

Výkladem o možné budoucnosti informačních technologií zakončíme exkurzi do světa informatiky. V kapitole 1 jsme si něco pověděli o informačním nárůstu a jeho limitujících faktorech. Jedním z těchto faktorů je hranice technologických možností. Z dnešního pohledu se zdá, že touto hranicí bude miniaturizace tranzistorů v procesorech. Podle některých odhadů může být této hranice dosaženo někdy za 20 možná 30 let, tedy s vysokou pravděpodobností ještě za našich životů.

Vyvinutí a nasazení úplně nových technologií může být novým impulsem, který odstartuje nové kolo inovací. O některých „nadějných“ technologiích se dozvíte něco v následujících odstavcích.

Začneme DNA počítači. Při výzkumu v této oblasti se vychází z toho, že v živých organismech slouží ke kódování informací nukleové kyseliny. Vlákno nukleové kyseliny se skládá z několika složek, z našeho hlediska nás však zajímá především jedna a to je tzv. dusíkatá báze. U DNA jde o adenin, guanin, cytosin a thymin, u RNA je thymin nahrazen uracilem. Jednotlivé dusíkaté báze dále budeme označovat jejich počátečními písmeny.

Některé z těchto dusíkatých bází jsou vůči sobě komplementární, tzn. že se mezi nimi vytváří pevná vazba:
A A G
T U C

Atraktivita použití DNA počítačů spočívá v masivním paralelismu při řešení zadané úlohy. Průkopníkem v této oblasti profesor Leopard Aleman, který pomocí DNA počítače řešil celkem dvě úlohy.

V roce 1994 úspěšně vyřešil problém obchodního cestujícího a v nedávné době i problém výběru automobilu.

Problém obchodního cestujícího je následující: Obchodní cestující má předem stanovená města, která během své cesty navštíví, tuto návštěvu ale chce optimalizovat tak, aby přitom urazil co možná nejmenší vzdálenost.

Druhý Alemanův experiment se blíží svým zadáním běžnému lidskému myšlení. Mějme autobazar a zákazníka, který chce koupit auto. Zákazník má představu co chce přesně koupit, ovšem tato představa je velmi obtížně zpracovatelná pomocí standardních výpočetních prostředků: zákazník by chtěl cadillac nebo auto s odklápěcí střechou nebo auto červené barvy. Pokud by se jednalo o Cadillac, musel by mít čtyři sedadla nebo uzamykatelný uzávěr k nádrži. A nakonec pokud by se jednalo o auto s odklápěcí střechou, nemělo by se jednat o Cadillac nebo by měl mít dvě sedadla. Zákazník ze sebe vychrlí ještě dalších 21 podmínek, prodejce si teď musí sednout a porovnat tyto podmínky s 1 milionem aut, která má k dispozici a vybrat z nich auto nebo auta, která podmínkám nejlépe vyhovují.

Pro člověka je takový problém neřešitelný. V případě řešení pomocí DNA počítače, by se vytvořili pomocí nukleových bází reprezentanti jednotlivých aut i požadavků zákazníka. Zajistí se, aby konce těchto samostatných vláken byly komplementární dle požadavků zákazníka a aby všichni reprezentanti byli zastoupeni v roztoku dostatečně-krát. Potom se vše pečlivě promíchá, aby se komplementární báze spojily, a výsledek se odfiltruje magnetismem, elektrolýzou apod.

Tedy požadovaný výsledek můžeme dostat, ale nemusíme, je pouze pravděpodobné, že díky tomu že jednotlivé komponenty byly v roztoku redundantně, dostaneme požadovaný výsledek. V tom spočívá výše zmíněný masivní paralelismus.

Zde představený počítač je jednoúčelový a jednosměrný – musí se připravit vstupní látky a ty se během výpočtu znehodnotí. Po ukončení výpočtu se musí tedy všechny látky zahodit a začít znovu.

Přesto je zajímavé zamyslet se nad složitostí problémů řešitelných tímto způsobem a srovnat jej se způsobem klasickým. Oba řešené problémy se řadí do kategorie problému NP- kompletních. Takové problémy rostou kvadratickou řadou s počtem prvků. Představte ti složitost řešení problému obchodního cestujícího se sedmi městy a dvaceti městy. Pro paralelní počítače, kam se řadí i DNA počítače, se složitost problému zvyšuje pouze lineárně.

V Izraeli se pracuje na DNA počítači nové generace, který by dle požadavků byl schopen spojovat a rozpojovat jednotlivé báze tak aby k tomuto problému nedošlo, tento výzkum je však ještě v relativně raném stádiu.

Praktického nasazení DNA počítačů se nejspíše v příštích 20-ti letech nedočkáme.

10.2 Kvantové počítače

Kvantové počítače byly teoreticky odvozeny z kvantové fyziky někdy během 80. let minulého století. Se vznikem teoretických základů je spojováno jméno Richarda Feynmana. Další impuls pro výzkum se staly práce Petera Shora z Bellových laboratoří, který navrhl první algoritmu, který takový by takový počítač mohl zpracovávat. Algoritmus řešil faktorizaci velkých čísel na prvočísla. Prakticky se to samozřejmě vzhledem k neexistenci takového počítače nikdy nevyzkoušelo.

Kvantové počítače pracují na principu kvantové fyziky. Ta mimo jiné říká, že jakékoliv měření vyvolává v prostoru kvantových jevů nevratné změny. Z tohoto důvodu kvantový počítač musí být úplně izolován od okolí, které by ho jinak ovlivnilo.

Odlišný způsob konstrukce (ve srovnání s klasickými počítači) ale způsobuje, že tento typ počítačů se rozvíjí relativně pomalu a využití se tak soustředí především na proof of concept řešení, popř. na řešení některých specifických problémů, byť s možností použití experimentuje řada společností jako např. IBM, Google, NASA, Microsoft a řada dalších.

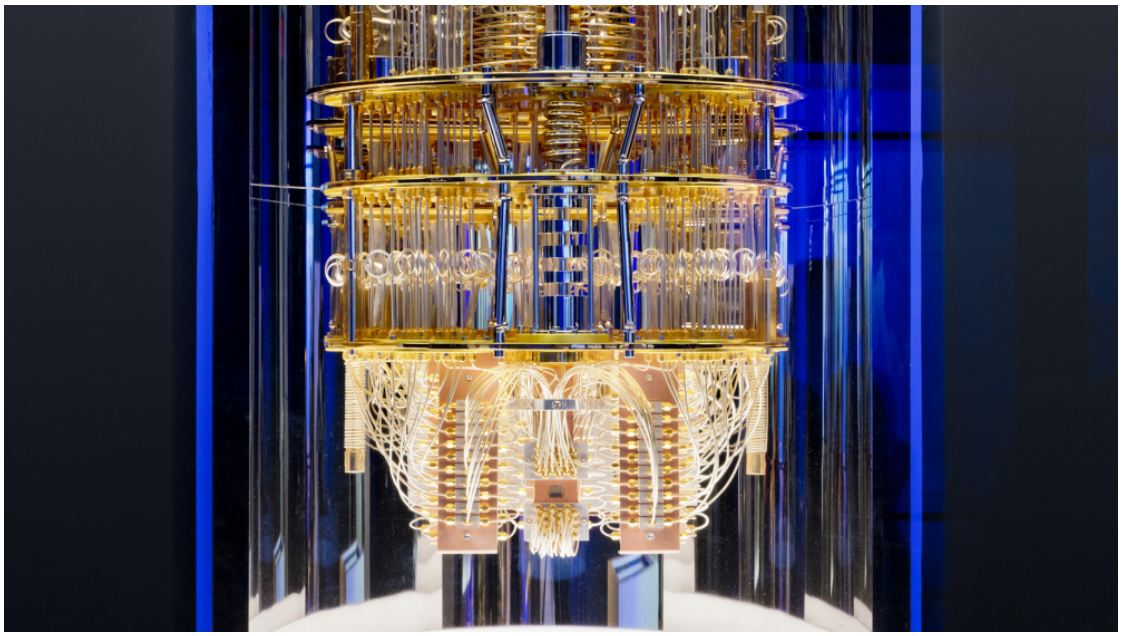
Podle kvantové fyziky totiž, dokud se na elektron nepodíváme, nevíme, kde se přesně nachází, ale což je závažnější, v určitém smyslu se nachází na více místech současně. V okamžiku, kdy se na něj podíváme, však tento zvláštní stav pomine a elektron uvidíme pouze na jednom z těchto míst.

Abychom se to shrnuli, klasický počítač pracuje se stavem se dvěma hodnotami 0/1. Přitom stav může mít pouze jednu hodnotu. Kvantová mechanika umožňuje elektronu, aby zaujal speciální stav, kterému se říká lineární superpozice obou stavů, který charakterizuje tzv. vlnová funkce. Zatímco tedy u klasických počítačů pracujeme s bity, u kvantových počítačů pracujeme s kvantovými bity neboli qbity. Díky tomu může celá soustava atomů ve všech 2N stavech současně, kde N je počet bitů. Je tedy možné najednou prozkoumat velké množství možností.

V praxi je kvantový počítač tvořen částicemi, připraví se do výchozí podoby a nechá se pracovat – v okamžiku kdy se na něj podíváme, dojde ke kolapsu systému, po kterém jsme schopni odečíst výsledek, ale počítač není schopen dál pracovat, musí se „opravit“ do původního stavu.

V současné době se s kvantovými počítači experimentuje intenzivně experimentuje. IBM v roce 2021 uvedla 127-mi qbitový kvantový počítač s plánem nasadit 433-mi qbatový počítač v roce 2022 a 1000 qbitový o rok později.

Dosažení superpozice stavů ale není v běžných podmínkách, především teplotních, možné. Kvantové počítače tak musí být provozovány při teplotách blízkých absolutní nule. Jistou představu o vzhledu je možno si udělat z obr. 10.1.



Obrázek 10.1: Systém IBM Q (převzato z [72])

Pro nasazování tohoto typu počítačů ale existuje celá řada dalších překážek, než pouze celkový počet qbitů, které jsou dostupné pro výpočet:

- fyzická škálovatelnost pro použití vysokého počtu qbitů
- možnost iniciovat qbity na určitou hodnotu
- kvantové brány, než čas dekoherence
- univerzální sada bran
- možnost snadného přečtení qbitů

Z hlediska škálovatelnost jsou počty uváděné IBM a zejména pak trajektorie rozvoje poměrně zásadní průlom. Velmi dlouhou dobu totiž kvantové počítače pracovaly pouze s jednotlivými qbity, najednou jich budou k dispozici stovky a v relativně blízké budoucnosti možná dokonce tisíce. Úroveň tisíců je přitom mezní pro (začátek) řešení problémů faktorizace pro řadu asymetrických šifrovacích algoritmů.

Pro pohodlné (řekněme horizont několika dní) řešení tohoto problému ale ale při současném stavu poznání předpokládána potřeba kvantového počítače disponujícího statisíci qbity.

Toto číslo ale není definitivní, protože výzkum v současnosti dosahuje také pokroku v oblasti efektivity Shorova algoritmu a také výběru částí algoritmu, na které se bude útočit. Lze proto předpokládat, že reálná výpočetní náročnost bude nižší. Jistou představu o stavu poznání této problematiky je možno si udělat z článku [60].

Do jisté míry vyřešen byl také problém tzv. kvantové nadvlády (quantum supremacy). Tento problém spočívá v demonstraci algoritmu, který kvantový počítač je schopen vykonávat řádově lépe než počítač klasický. V letech 2019 a 2020 se objevily první případy, které by tyto podmínky mohly splňovat, byť se vedou debaty o tom, jak ve skutečnosti velký případný náskok kvantového počítače je.

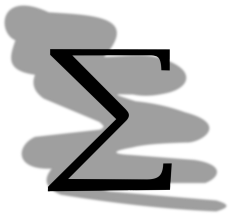
V oblasti aplikace kvantové mechaniky obecně došlo také k výraznějším pokrokům a dochází k nasazování tzv. kvantové kryptografie, která je svou fyzikální podstatou, alespoň dle současného stavu poznání, naprosto bezpečná.

Rozvoj v posledních letech prokazuje, že problematika kvantových počítačů se konečně přesunuje od akademických debat k praktičtějším aplikacím. Ruku v ruce s tím, ale je potřeba si pokládat také otázku co dál z pohledu bezpečnosti. Pokud víme, že v současnosti používané šifrovací algoritmy jsou náchylné k prolomení prostřednictvím kvantových počítačů, je potřeba hledat alternativní šifrovací schémata, která by naopak byla útokům realizovaných kvantovým počítačem odolná.

Takovým algoritmům říkáme post-kvantová kryprografie. V současnosti NIST organizuje soutěž z cílem vybrat a standardizovat algoritmy, které by byly kvantově odolné. Tuto snahu zahájil v roce 2016 a do dneška realizoval celkem tři kola soutěže, na základě kterých vybral několik finalistů, které považuje za nejnadějnější a také několik alternativních algoritmů. Ty budou ještě znova hodnoceny ve čtvrtém kole soutěže.

Výsledkem celé soutěže by měl být výběr jednoho algoritmu Public Key Exchange/Key Encapsulation Mechanism (PKE/KEM) a jednoho schématu elektronického podpisu. Lze ale předpokládat, že proces výběru algoritmů a jejich případná standardizace může trvat ještě léta. V současnosti není ani zaručeno, že navrhované algoritmy netrpí nějakou slabinou, která zatím zůstala neodhalena. Jisté obavy jsou spojovány také z licencování algoritmů, které je v některých případech sporné.

Každopádně je již dnes možno říci, že problematiku kvantových počítačů, ale také způsobu jakým bude reagovat zbytek IT sektoru na jejich nástup je potřeba sledovat tak, aby byla zajištěna



Shrnutí

Některé typy problémů, jsou pomocí současné výpočetní techniky špatně řešitelné, jedná se zejména o tzv. N:P kompletní problémy – třída problémů, jejichž složitost roste exponenciálně. Pro řešení takových problémů bude nutné vyvinout buď nové algoritmy řešení, nebo nový hardware.

Mezi nadějné počiny v oblasti hardware řadíme DNA počítače a kvantové počítače.

DNA počítače využívají tzv. masivního paralelismu, kterým rozumíme fakt, že jednotliví reprezentanti částí problému jsou v DNA počítači přítomni mnohokrát. Samotný výpočet tak probíhá najednou smísením všech těchto reprezentantů a následným filtrováním výsledků.

Kvantové počítače využívají pro výpočty kvantové mechaniky, která na rozdíl od klasické výpočetní techniky nepočítá s bity a qbity. V klasické mechanice stav nastane nebo nenastane (0/1), v kvantové mechanice funguje (0/1/0 a 1).

Všechny výše uvedené technologie, jsou bohužel zatím ve stádiu výzkumu a komerčně pravděpodobně nebudou nasazeny příštích deseti až dvaceti letech.

Kontrolní otázky

1. Co jsou to N:P kompletní problémy?
2. Co rozumíme pojmem masivní paralelismus DNA počítačů?
3. Proč říkáme, že kvantový počítač pracuje jako černá skříňka?
4. S jakými jednotkami pracuje kvantový počítač?

Správné odpovědi

1. Jsou to problémy, jejichž složitost roste minimálně exponenciálně.
2. Schopnost DNA počítačů provést výpočet najednou paralerně pro velké množství reprezentantů prvků problému.
3. Protože když se do ní podíváme, zhroutí se vlnová funkce a výpočet havaruje.
4. qbit

Test

1. DNA se skládá z následujících dusíkatých bází:
   (a) A, T, U
   (b) G, T, U
   (c) A, T, G
2. DNA počítače jsou
   (a) Jednoproblémové, jednorázové
   (b) Víceproblémové, jednorázové
   (c) Jednoproblémémové, stále použitelné
3. Speciálnímu případu nerozhodného stavu říkáme
   (a) Super pozice
   (b) Qbit
   (c) Vlnová funkce
4. DNA a kvantové počítače jsou
   (a) Běžně používány
   (b) Občas používány
   (c) Ve fázi vývoje

Správné odpovědi
1. c), 2. a), 3. a), 4. c)

Kapitola 11

Telekomunikace

Náhled kapitoly
V této kapitole se seznámíte s legislativním rámcem telekomunikací v České Republice a EU.

Po přečtení kapitoly budete
Vědět

1. Legislativní rámec telekomunikací v ČR a EU
2. Co znamenají pojmy ex ante, dominantní postavení, univerzální služba a řada dalších

Čas pro studium
Na prostudování této kapitoly budete potřebovat přibližně 60 minut.

11.1 Legislativní rámec EU

2002/21/ES – rámcová směrnice
Základní směrnicí v oblasti telekomunikací EU je směrnice European Parlament (EP) a rady 2002/21/ES o společném předpisovém rámci pro sítě a služby elektronických komunikací (rámcová směrnice).

Vzhledem ke konvergenci telekomunikací, medií a informačních technologií (IT) vyžadují jednotný předpisový rámec. Tento rámec se skládá ze čtyř základních směrnic:

1. 2002/20/ES o oprávnění pro sítě a služby elektronických komunikací - **autorizační směrnice**
2. 2002/19/ES o přístupu k sítím elektronických komunikací a přiřazeným zařízením a o jejich vzájemném propojení - **přístupová směrnice**
3. 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací - **směrnice o univerzální službě**
4. 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací - **směrnice o soukromí a elektronických komunikacích**

Všechny výše uvedené směrnice se zabývají technickou stránkou telekomunikací a nikoliv regulací jejich obsahu. Regulace obsahuje představuje pomerně komplexní téma, které vyžaduje samostatnou právní úpravu. Na úrovni EU můžeme jako zákld považovat směrnici 89/552/EHS a další směrnice od ní odvozené.

Legislativní rámec telekomunikací je relativně nový a právníci zabývající se touto oblastí uvádějí, že nová úprava podstatným způsobem zjednodušuje právní úpravu v této oblasti, nicméně, jak se ukáže v následujících odstavcích, to neznamená, že by právní úprava byla jednoduchá.

Z hlediska zařízení se směrnice také nevztahují na zařízení v oblasti platnosti směrnice 1999/5/ES o rádiových zařízeních a telekomunikačních koncových zařízeních a vzájemném uznávání jejich shody. Výše uvedené směrnice se však vztahují na zařízení pro digitální televizi.

Na služby v informační společnosti se vztahuje směrnice 2000/31/ES o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu na vnitřním trhu (směrnice o elektronickém obchodu).

Směrnice 98/34/ES o postupu při poskytování informací v oblasti norem a technických předpisů a pravidel pro služby informační společnosti – definuje jako první směrnice pojem služby informační společnosti. Většina z těchto služeb ale nespadá pod legislativní rámec telekomunikací, protože nespočívají zcela nebo převážně na přenášení signálů po sítích elektronických komunikací.

Právní rámec se tedy vztahuje na:

1. hlasové telefonní služby
2. služby přenosu elektronické pošty
3. přístup k internetu apod.

Do právního rámce naopak nespadá:

1. regulace obsahu (např. televizního vysílání nebo rozhlasu)
2. úprava služeb poskytovaných přes Internet apod.

Rámec jako takový stanovuje základní požadavky na úpravu telekomunikací, zejména s ohledem na podporu „zdravé“ hospodářské soutěže v tomto odvětví. Prvním z těchto požadavků je požadavek na existenci nezávislého regulátora na trhu. Nezávislostí se zde myslí zejména požadavek na možnost odvolat se k nějaké třetí straně. Dle směrnice jí může být i soud.

Regulace jako taková by měla být pokud možno technologicky neutrální.

Radiové frekvence, jejich přidělování a převod se řídí rozhodnutím Evropského parlamentu (EP) a rady 676/2002/ES o předpisovém rámci pro politiku rádiového spektra v Evropském společenství (rozhodnutí o rádiovém spektru).

Když se nad tím zamyslíme, EU vznikla původně za jediným účelem a to vytvoření společného trhu (EHP - Evropský Hospodářský Prostor). Základem správného fungování trhu je férový přístup k jednotlivým účastníkům na trhu. Tato férovost vyžaduje, aby jednotlivé státy zasahovaly do fungování trhu co možná nejméně. Každý zásah totiž na jedné straně zvýhodňuje jisté účastníky trhu, zatímco znevýhodňuje jiné.

Každý zásah má tedy potenciál ovlivnit trh. Takové ovlivnění ale nemusí být žádoucí. Regulace je proto možná pouze v případě, kdy na trhu dochází k tzv. *tržnímu selhání*. Tržním selháním se rozumí jakákoliv anomálie ve fungování trhu, která brání volné soutěži na trhu. Jedním z nejčastějších příčin je situace, kdy na trhu jeden nebo více účastníků trhu získá tzv. *významnou tržní sílu*.

Jako první se tento pojem vyskytnul v 97/33/ES o propojení v odvětvích telekomunikací s cílem zajistit univerzální službu a interoperabilitu. Uplatněním zásad otevřeného přístupu k síti (ONP). Mnohem častěji se však využívá pojem vycházející z juridikátů soudního dvora a soudu prvního stupně ES – *dominantní postavení*.

Dominantní postavení může nabývat podoby monopolu nebo třeba oligopolu. *Monopolní* postavení získá firma ovládnutím trhu. V takovém případě firma z trhu úspěšně vytlačí všechny své konkurenty. Následně pak na trhu sama poskytuje výrobky nebo služby. Jelikož v tomto případě neexistují konkurenti, nenutí organizaci nic k inovacím výrobků a nebo služeb, investicím k podpoře efektivity fungování služeb apod. V důsledku toho postupně trh začíná stagnovat, včetně možnosti postupného navyšovaní cen.

Oligopol je jiný v tom, že dominantního postavení nedosahuje jediná firma, ale několik firem. Tyto firmy si v podstatě rozdělí trh. Rozdělení může být na bázi regionální nebo třeba v typologii poskytovaných služeb. V okamžiku dosažení oligopolu ztrácejí účastníci na trhu motivaci k soutěžnímu chování. Jednotliví účastníci trhu se přestávají chovat konkurenčně a to opět vede k stagnaci na trhu, zvyšování cen, omezení tempa inovací, ale také rozvojových investic.

Dle platné legislativy má právě regulátor povinnost *analyzovat trh* za účelem detekce tržních selhání a navržení takových opatření, které by trh z hlediska jeho fungování vrátily do rovnovážné pro-soutěžní pozice. Odborně tento požadavek označujeme jako tzv *ex ante* princip.

Výraz ex ante pochází z latiny a bylo by jej možné volně přeložit „jako předtím“. Z hlediska regulace to znamená, že regulační opatření musí směřovat na vrácení situace na trhu do podoby jako před tím, než došlo k tržnímu selhání. To, že došlo k tržnímu selhání musí být prokazatelné provedenou

Vysvětlení
Dominantní postavení má jedna nebo více firem pokud mezi nimi existuje strukturální nebo jiné vazby nebo také tehdy pokud struktura trhu vede ke koordinačním účinkům a tedy podporuje souběžné (spojené) protisoutěžní chování na trhu.

analýzou trhu. Navržená opatření pak musí být opět zdůvodněna tak, aby se účinně vypořádala s příčinou tržního selhání.

Dobrý příkladem z poslední doby může být pokus ČTÚ regulovat ceny mobilních dat. ČTÚ za tímto účelem provedl v polovině roku 2021 analýzu trhu a na základě ní rozhodl o nutnosti regulovat ceny. Toto rozhodnutí, ale odmítla počátkem roku 2022 Evropská komise z důvodu neprokázání, že by současní tři síťoví mobilní operátoři v Česku ve shodě omezovali konkurenci na trhu. Analýza nebere dostatečně v úvahu dopady podmínek aukce tzv. 5G kmitočtů.

Bez souhlasu Komise ČTÚ nemůže svá regulační opatření nasadit. Nasazení regulace tedy podléhá přezkumu. Rozhodnutí Evropské komise ve skutečnosti neznamená nutně, že nedošlo k tržnímu selhání, pouze, že zdůvodnění analýzou takové selhání neprokazuje a není tedy důvod pro nasazení regulace. Národní regulátor pak může provést novou analýzu trhu a případně znovu rozhodnout o (ne-)potřebnosti regulace. To je také cesta, kterou se pravděpodobně vydá ČTÚ vzhledem k cenám datových přenosů. V době psání těchto řádek textu ale nová analýza trhu dosud nebyla k dispozici.

Všimněte si také, jakým způsobem je definice dominantního postavení sestavena, uvažuje totiž nejen se situací, kdy některý z účastníků získá dominantní tržní podíl, ale také situací, kdy dominantní postavení je založeno např. na vlastnění telekomunikační infrastruktury. K takové situaci dochází velmi často z historických důvodů.

I v tomto případě lze nalézt dobrý příklad v ČR a to konkrétně v oblasti přístupu k metalickým rozvodům telefonních sítí. Většina těchto rozvodů byla realizována v druhé polovině 20. století za účelem provozu pevných telefonních linek. Nástup mobilních telefonů a mobilních sítí sice výrazně zmenšil atraktivitu těchto sítí pro realizaci telefonních hovorů, ukázalo se však, že tuto metalickou síť je možno využít také k realizací vysokorychlostního připojení k Internetu pomocí technologie VDSL.

Vzhledem k tomu, že převážná část sítě byla vybudována v totalitní ČSSR, byla celá vlastněna jedinou společností - Telecomem, který se tak ocitl v pozici monopolu. To jak víme je možné klasifikovat jako tržní selhání a dává regulátorovi šanci začít regulovat, což se stalo. Regulátor stanovil velkoobchodní podmínky pro Telecom pro zpřístupnění své infrastruktury svým konkurentům, kteří pak mohou službu nabízet koncovým zákazníkům pod vlastní značkou.

Vlastník infrastruktury je ale samozřejmě za takové zpřístupnění finančně kompenzován.

Zavedená regulace vedla k tomu, že část infrastruktury se postupem času vyčlenila do samostatné společnosti (CETIN), která funguje jako velkoobchod poskytující přístup k infrastruktuře pro jednotlivé poskytovatele připojení k Internetu. CETIN je v současnosti (2022) vlastně společností PPF.

EU jako celek bude v budoucnu zřizovat skupinu evropských regulačních orgánů pro sítě a služby elektronických komunikací jako vhodnou metodu spolupráce jednotlivých národních regulátorů a pokud možno jednotné regulační úpravě trhu EU jako celku.

Z výše uvedeného vyplývá, že regulační orgán má významné postavení na trhu. Zkusmě formálněji definovat jaké úkoly by takový orgán měl plnit.

Vnitrostátní regulační orgány mají povinnost podporovat hospodářskou soutěž s cílem, aby všichni uživatelé včetně např. tělesně postižených) měli maximální výhody výběru z hlediska služeb, ceny a kvality. Regulátor také může investičně podpořit rozvoj infrastruktury nebo inovací pokud by bez této podpory inovace nebyla realizována vůbec nebo se zpožděním. Regulátor také podporuje účinné využívání radiových frekvencí a zdrojů číslování a zajišťuje jejich účinnou správu.

Regulátor kromě řešení tržních selhání má i úlohu v rozvoji vnitřního telekomunikačního trhu EU a to zejména v oblasti odstraňování překážek pro zajišťování sítí elektronických komunikací na evropské úrovni. Zde patří i různá přeshraniční spolupráce, podpora zřizování a rozvoje transevropských sítí, zajišťování interoperability celoevropských služeb apod.

V oblasti rádiového spektra musí jednotlivé státy zajistit přidělování a kontrolu radiových frekvencí a to v souladu s rozhodnutím 676/2002/ES (viz výše).

Členské státy zajistí přidělování čísel, jmen a adres a to na základě tzv. národních číslovacích plánů. Tyto národní číslovací plány mají členské státy povinnost zveřejňovat, výjimky jsou možné pouze z

důvodu možného ohrožení národní bezpečnosti.

2002/20/ES – autorizační směrnice
Cílem této směrnice je vytvořit právní rámec pro volné zajišťování sítí a poskytování služeb elektronických komunikací. Zabývá se požadavky pro získání oprávnění pro veškeré sítě a služby elektronických komunikací bez ohledu na to zda jsou poskytovány veřejnosti nebo ne.

Tato směrnice se nevyužívá pro přidělování rádiových frekvencí s výjimkou zajišťování sítí nebo poskytování služeb elektronických komunikací (obvykle za úplatu), které se radiových frekvencí nebo provozu na nich týkají.

Využívání rádiových vln (např. pro radioamatéry) upravuje směrnice 1999/5//ES.

Ustanovení upravující volný pohyb systému podmíněného přístupu a volného poskytování chráněných služeb, které jsou na takových systémech založeny, upravuje 98/84/ES o právní ochraně služeb s podmíněným přístupem a služeb tvořených podmíněným přístupem.

Udělování zvláštních práv může být nadále nezbytné pro užívání rádiových frekvencí a čísel národního číslovacího plánů včetně tzv. zkrácených kódů. Práva k číslům mohou být předělována i z evropského číslovacího plánu, včetně virtuálního kódu země „3883“, který byl přidělen členským státům Evropské konference správ pošt a telekomunikací (CEPT).

2002/19/ES – Přístupová směrnice
Předmětem úpravy jsou mobilní telefonní sítě, sítě kabelové televize, sítě pro pozemní vysílání družicových sítí a sítí Internetu (používané pro přenos hlasu a obrazu, dat nebo faxu). Pro sítě takového typu musí být uděleno povolení dle autorizační směrnice nebo předchozích regulačních opatření.

Tato směrnice se vztahuje na dohody o přístupu a propojování mezi dodavateli služeb. Na neveřejné sítě (sítě, které neposkytují služby veřejnosti, např. vnitropodnikové) se tato směrnice nevztahuje, stejně jako na služby poskytování obsahu.

Regulační rámec má zajistit pokud možno kulturní rozmanitost, mediální pluralitu v oblasti telekomunikací. Počáteční předpisový rámec pro digitální televizi stanovuje směrnice 95/47/ES. Ustanovení v něm obsažená, se mají přezkoumávat na úrovni států s cílem zjistit, zda je důvod pro rozšíření povinnosti na zřizování nových bran (gateway), jako jsou elektronické programové průvodce (EPG) nebo rozhraní pro aplikační programy (API), tak aby se služby dostaly bez problému ke koncovému uživateli.

Směrnice také upravuje podmínky poskytnutí přístupu k infrastruktuře a to zejména u firem, které mají dominantní postavení na předmětném trhu. Povinnost zpřístupnit infrastrukturu je odůvodnitelná jako prostředek pro zachování hospodářské soutěže v daném segmentu trhu (žádná infrastruktura konkurence = žádná soutěž).

Regulátor při stanovení povinnosti však musí brát v úvahu i práva vlastníka infrastruktury, který do jejího vybudování a údržby investoval nějaké finanční prostředky. Tedy zpřístupnění by se mělo dít pouze s finanční nebo jinou náhradou. Vlastník infrastruktury by také měl mít možnost využívat tuto infrastrukturu v přiměřené míře ve svůj prospěch.

Regulace cen je možná pouze za předpokladu, že analýza trhu prokáže, že hospodářská soutěž je v určitém segmentu trhu neúčinná. Stanovené ceny by měly být přiměřené (dle směrnice 97/33/ES).

2002/22/ES – Směrnice o univerzálních službách

Náhled kapitoly
Univerzální službou se rozumí minimální rozsah služeb, které má možnost používat každý občan, včetně např. tělesně postižených.

Státy EU přijaly závazky v této oblasti v souvislosti s dohodou o základních telekomunikacích Světové obchodní organizace (WTO). Každý stát má podle této dohody vymezit druh povinnosti univerzální služby dle svých potřeb. Tyto povinnosti pak nebudou považovány za protisoutěžní. V zásadě tedy může stát určit monopolního dodavatele univerzální služby.

Základním požadavkem, je poskytnout uživatelům na jejich žádost připojení k veřejné telefonní síti v pevném místě (jsou tedy vyloučení mobilní operátoři), za dostupnou cenu. Požadavek se omezuje

na úzkopásmovou přípojku, je z ní tedy vyloučeno ISDN nebo třeba DSL. Důvod je jednoduchý - širokopásmové připojení prostřednictvím metalických rozvodů je omezeno vzdáleností koncového místa od tzv. DSLAM (DSL Access Multiplexer). S rostoucí vzdáleností klesají přenosové rychlosti. Zejména v okrajových částech republiky pak vysokorychlostní internet zajištění touto technologií není možný.

Přístup k telefonní síti by měl umožnit bezproblémový přístup k on-line službám, zejména pro komunikaci s orgány státní správy a samosprávy.

Původně byl součástí univerzální služby také zajištění provozu telefonních automatů a telefonních budek. Ukázalo se však, že o automaty mají zájem pouze vandalové a tak už v průběhu roku 2021 byla slavnostně zrušena poslední telefonní budka v ČR. Původní myšlenka pro provoz automatů bylo zajistit obyvatelstvu schopnost v případě potřeby zavolat si pomoc na tísňových linkách. Rozšíření mobilních telefonů ale dalo tuto schopnost obyvatelstvu přímo do kapsy. Tady je ale potřeba říci, že přístup k mobilnímu telefonu není součástí univerzální služby.

Mobilní telefony a tarify k přístupu do sítě si tak obyvatelstvo musí hradit samo. Použití tísňové linky samotné je ale bezplatné.

Účastnické seznamy a informační služba o účastnických číslech (telefonní seznam a informační linka) představují základní prostředek pro přístup k telefonní službě a jsou součástí povinnosti univerzální služby.

Směrnice také upravuje přenositelnost telefonního čísla. Dnes již takovou službu považujeme za standard, ale ne vždy tomu tak bylo. Tato služba pro mobilní telefonní čísla byla zprovozněna teprve v roce 2006. Důvodem pro zavedení byl fakt, že bez přenosu čísla je přechod k jinému operátorovi poměrně komplikovaný, neboť je spojen se změnou telefonního čísla. Informování kontaktů o změně telefonního čísla je pak zdlouhavé a vždy se na nějaký kritický kontakt zapomene... To ve finále způsobovalo, že klienti zůstávali u svých operátorů, ačkoliv z pohledu ceny, kvality a rozsahu služeb by pro ně bylo lepší přejít ke konkurenci.

Zajímavá je také koncepce tísňového čísla 112. V minulosti byl medializován spor mezi pražskými hasiči a zdravotní záchrannou službou o reklamní kampani na číslo 112, kdy hasiči podporují 112 a záchranná služba naopak existenci národních tísňových linek 15x. Záchranná služba argumentuje tím, že v případě, že se uživatel dovolá na číslo 112 a potřebuje okamžitou lékařskou pomoc, bude operátorem na čísle 112 přepojen na záchrannou službu a tam se mu teprve dostane pomoci. Doba přepojení přitom trvá 1 – 2 minuty. Jde o to, že na specializované lince se uživatel může dozvědět informace např. o resuscitaci, než dorazí záchranka.

Z hlediska směrnice je však číslo 112 prioritní s tím, že jednotlivé státy mohou, ale nemusí, používat národní tísňové linky. Z tohoto pohledu je tedy přístup HZS správný a problém časové prodlevy by se měl tedy řešit jinak, např. technickým opatřením, slučováním dispečinků apod.

V současnosti také došlo k posunu v příjmu tísňových volání jako takových. Řada krajů provozuje pro své obyvatele Integrované bezpečnostní centrum (IBC), které shromažďuje dispečery tísňových linek jednotlivých složek integrovaného záchranného systému (IZS) pod jednu střechu. Pro zajištění plynulosti provozu jsou pak jednotliví operátoři vyškoleni na příjem tísňových volání všech složek IZS. To zajišťuje jednak vysokou dostupnost služby, jednak také vysoký komfort jejího použití. Původní námitky 112 vs 15x tak pro velké části území již nejsou relevantní.

11.2 Zákon o elektronických komunikacích (127/2005 Sb.)

Zákon o elektronických komunikacích byl přijat v rámci harmonizace práva ČR s přepisovým rámcem EU.

Jako regulátor byl v ČR ustanoven Český telekomunikační úřad (ČTU) se sídlem v Praze. V plnění zásad stanovených regulačním rámcem spolupracuje ČTU s Ministerstvem vnitra, které přebralo prakticky celou gesci dnes již zrušeného Ministerstva informatiky.

Komunikačními činnostmi se dle zákona rozumí

1. zajišťování sítí elektronických komunikací
2. poskytování služeb elektronických komunikací
3. a provozování přístrojů dle §73 (problematika homologace zařízení pro použití na trhu)

Pro provoz komunikační činnosti musí fyzické osoby splnit následující podmínky: dosáhnout minimálně 18-ti let věku, být bezúhonné a být způsobilé k vykonávání právních úkonů. Fyzická osoba také nesmí mít závazky vůči orgánům státní správy.

Právnické osoby musí splňovat podobné podmínky jako fyzické osoby. Omezení bezúhonnosti a právní způsobilosti přitom platí pro osobu nebo osoby oprávněné jednat jménem právnické osoby.

ČTU uděluje tzv. *všeobecné oprávnění*. Jedná se o obecné opatření ČTU stanovující podmínky výkonu komunikační činnosti. Podmínky pro udělení všeobecného oprávnění se mohou týkat finančních příspěvků na provoz univerzální služby, požadavků na interoperabilitu, ochranu životního prostředí apod.

Pro podnikání v oblasti telekomunikací platí oznamovací povinnost.

Ze zákona také vyplývá povinnost ČTU spravovat rádiové spektrum. Rádiovým spektrem se přitom rozumí elektromagnetické vlnění o kmitočtech 9kHz – 3000GHz šířené prostorem bez zvláštního vedení (jinými slovy tedy vzduchem).

Správou se rozumí sestavování návrhu plánu přidělení kmitočtových pásem, přidělování volacích značek, identifikačních čísel a kódů a kontrola využívání rádiového spektra.

Kmitočty lze využívat pouze na základě individuálního oprávnění k využívání rádiových kmitočtů. Pro některé účely je k žádosti vyžadována licence dle zvláštního předpisu:

1. 231/2001 Sb. O provozování rozhlasového a televizního vysílání
2. 49/1997 Sb. O civilním letectví
3. 114/1995 Sb. O vnitrozemské plavbě
4. 61/2000 Sb. O námořní plavbě

Přestávka
Česká námořní plavba byla privatizována Viktoru Koženému.

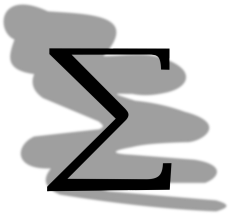
Úřad přednostně rozhoduje o udělování kmitočtů pro zajištění činnosti orgánů Ministerstva vnitra, BIS, Úřadu pro zahraniční styky a informace, Policie ČR, Vězeňská služba a justiční stráže ČR, HZS ČR a jednotek PO, Záchranné zdravotní službě a celním orgánům.

Kmitočtová pásma vyhrazená ministerstvu obrany pro vojenské účely mohou být pro tyto účely využívány bez nutnosti rozhodnutí o udělení oprávnění. Jinými slovy ministerstvu obrany se přidělují celé bloky rádiového spektra, aniž by ministerstvo muselo specifikovat, jaké služby na jakým kmitočtech bude provozovat. Jedná se o logické rozhodnutí, protože podrobnou specifikací kmitočtů a služeb by nepřátelský stát v podstatě dostal návod na vyřazení těchto služeb v případě válečného konfliktu. Blokové přidělení tak umožňuje armádě jednak udržovat způsob použití v tajnosti, jednak ji nechává otevřenou cestu přejít v případě potřeby na jinou frekvenci a zachovat tak kontinuitu služeb.

Za krizových stavů jsou podnikatelé zajišťující veřejné komunikační sítě povinní dle §12a zákona 240/2000Sb. a svých technicko – organizačních pravidel zabezpečit přístup k veřejné telefonní síti. Tento přístup je samozřejmě zpoplatněn. Pravidla, která si organizace přijímá sama, slouží k určení doby, za kterou je možno poskytnou přístup k síti a i ceny, která bude za využití sítě zaplacena.

Ministerstvo informatiky (MI) v oblasti elektronických komunikací předkládá vládě návrh státní politiky elektronických komunikací a po jejím schválení dohlíží nad její realizací. MI zabezpečuje mezinárodní vztahy v této oblasti na úrovni vlád, vládních i nevládních organizací s výjimkou těch, kde tímto úkolem byl pověřen ČTU. MI zodpovídá za plnění závazků vyplývajících z mezinárodních smluv a konečně vykonává státní statistickou službu.

Jelikož ministerstvo informatiky koncem roku 2007 zaniklo, přešly všechny jeho práva a povinnosti do gesce ministerstva vnitra.



Shrnutí

Telekomunikace jsou řešeny se na území EU jednotnými pravidly vymezenými směrnicemi EP a rady: rámcové, přístupové, autorizační, zvláštní směrnice a směrnice o univerzální službě.
Právní rámec se vztahuje na hlasové telefonní služby, služby přenosu elektronické pošty, přístup k internetu a podobně.
Regulace obsahu je spravována samostatnými pravidly.
Hlavním úkolem tohoto rámce je zajistit přístup k základním službám (univerzální služba), a zajistit, že trh se chová transparentně z hlediska hospodářské soutěže. Dalším cílem je zajistit plynulou přeshraniční spolupráci v této oblasti.
V ČR jsou tyto směrnice implementovány do zákona o elektronických komunikacích (127/2005 Sb.). Jako regulátor byl pro ČR stanoven Česky telekomunikační úřad (ČTU). Z hlediska spolupráce na legislativě a mezinárodní spolupráce vstupuje do telekomunikací i Ministerstvo informatiky (MI).

Kontrolní otázky

1. které úřady mají povinnosti na úseku elektronických komunikací v ČR
2. Vyjmenujte zkrácené názvy alespoň dvou směrnic EU z oblasti elektronických komunikací
3. Pokuste se stanovit co je to univerzální služba.
4. Která čísla mají z hlediska práva větší význam 112 nebo 15x?
5. Co je přístup ex ante.

Správné odpovědi

1. ČTU, MI
2. Autorizační, přístupová, o univerzální službě, speciální
3. Základní hlasové a datové služby umožňující komunikaci s úřady.
4. 112, EU to tak chce a EU to tak bude mít i u nás
5. Překlad: Jako předtím – reguluje se s cílem dosáhnout stavu jako před dosažení dominantního postavení účastníka trhu nebo obecně nějakého tržního selhání.

Test

1. Které frekvence a telekomunikační služby schvaluje ČTU
   (a) Všechny
   (b) Žádné
   (c) Všechny kromě armádních
2. Spolupracovat se zahraničními partnery na úseku telekomunikací má ze zákona povinnost
   (a) Evropská komise
   (b) MI
   (c) ČTU
3. Univerzální služba obsahuje
   (a) ISDN
   (b) ADSL
   (c) Základní hlasové a datové služby
4. Regulačním přístupem, kterým se snažíme dosáhnout situace na trhu předcházející tržnímu selhání, nazýváme
   (a) Ex jure
   (b) Ex ante
   (c) Ex libris
5. Důvodem zavádění přenositelnosti telefonních čísel je
   (a) Dobrá vůle operátorů
   (b) Snaha pomoci koncovým zákazníkům
   (c) Snaha otevřít rigidní trh konkurenci

Správné odpovědi
1. c), 2. b), 3. c), 4. b) 5. c)

Literatura

[1] AV-Test.

[2] CCSDS 650.0-m-2 - reference model for an open archival information system (OAIS).

[3] CESNET Komunikační infrastruktura.

[4] Common Criteria.

[5] Csirt.cz.

[6] Enigma.

[7] ETSI TS 101 733 v2.2.1 - electronic signatures and infrastructures (ESI); CMS advanced electronic signatures (CAdES).

[8] Farbar recovery scan tool.

[9] The hash function RIPEMD-160.

[10] ISO 14721:2012 - space data and information transfer systems – open archival information system (OAIS) – reference model.

[11] ISO/IEC 10118-3:2004 - information technology – security techniques – hash-functions – part 3: Dedicated hash-functions.

[12] ISO/IEC 18033-4 information technology — security techniques — encryption algorithms — part 4: Stream ciphers.

[13] ISO/IEC 29192-3 information technology — security techniques — lightweight cryptography — part 3: Stream ciphers.

[14] Jiří peterka.

[15] Keylength - NIST Report on Cryptographic Key Length and Cryptoperiod (2012).

[16] Konsolidované znění Smlouvy o fungování Evropské unie.

[17] Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.

[18] Nařízení vlády 432/2010 Sb., o kritériích pro určení prvků kritické infrastruktury.

[19] Nařízení vlády č. 11/2002 sb. kterým se stanoví vzhled a umístění bezpečnostních značek a zavedení signálů.

[20] Návod na vytvoření logu z DDS.

[21] Návod na vytvoření logu z RSIT.

[22] OpenPGP.

[23] OpenSSL.

[24] Ova.net.

[25] RFC 1918 - Address Allocation for Private Internets.

[26] ROZHODNUTÍ KOMISE 2011/130/eu ze dne 25. února 2011, kterým se stanoví minimální požadavky na přeshraniční zpracování dokumentů elektronicky podepsaných příslušnými orgány podle směrnice 2006/123/ES evropského parlamentu a rady o službách na vnitřním trhu.

[27] Skytale.

[28] TVS-671 :: QNAP.

[29] Uznesenie vlády slovenskej republiky č. 479/2009 k návrhu organizačného, personálneho, materiálno-technického a finančného zabezpečenia na vytvorenie špecializovanej jednotky pre riešenie počítačových incidentov (csirt.sk) v sr.

[30] Zákon 111/2009 sb. o základních registrech.

[31] Zákon 480/2004 sb., o některých službách v informační společnosti.

[32] Zákon č. 227/2000 sb., o elektronickém podpis.

[33] *Specification for the Advanced Encription Standard (AES)*. NIST, Springfield, VA, 2001.

[34] FIPS PUB 180-4 - secure hash standard (SHS), 2012.

[35] FIPS PUB 186-4 digital signature standard (DSS), 2013.

[36] Android OS, 2022.

[37] AV Comparatives. Independent Tests of Anti-virus software, 2022.

[38] AV-TEST. Malware Statistics & Trends Report, 2022.

[39] Avast. Testování počítače na přítomnost virů pomocí Záchranného disku aplikace Avast Antivirus, 2022.

[40] Kalid Azad. Understanding the birthday paradox.

[41] William C. Barker and Elaine Barker. NIST SP800-67 recomendation for triple data encryption algorithm (TDEA) block cipher, 2012.

[42] Martin Beltov. Karma Lockscreen Ransomware — How to Remove It, April 2019. Section: Ransomware.

[43] M. Boesgaard, M. Vesterager, and E. Zenner. A description of the rabbit stream cipher algorithm, 2003.

[44] Petr Bouška. Víte, jak pracuje switch?

[45] Augusto Buonafalce. Image of an Alberti Cipher Disk, March 1467.

[46] Business Wire. Strategy Analytics: Internet of Things Now Numbers 22 Billion Devices But Where Is The Revenue?, 2019.

[47] CERT.GOV.PL. Arakis agregacja, analiza i klasifikacja incidentów sieciowych.

[48] CERT.GOV.PL. Cert.gov.pl - domácí stránky.

[49] CESNET. Topologie sítě CESNET2, 2018.

[50] Comodo. Antivirus For Servers Alerts, Comodo Antivirus | Comodo Client Security | COMODO, 2022.

[51] CSIRT.CZ. Incident handling statistics.

[52] CZ.NIC. Datovka 4.

[53] CZ.NIC. DNSSEC/TLSA Validator add-in for Web Browsers.

[54] CÚZK. Veřejný dálkový přístup k datům registru územní identifikace, adres a nemovitostí, 2020.

[55] Hans Dobbertin. Cryptanalysis of MD4. *Journal of Cryptology*, 11(4):253–287.

[56] Robert Eisele. Caesar cipher decryption tool - Code is poetry.

[57] EK. Overview of pre-notified and notified eID schemes under eIDAS - eID User Community, 2022.

[58] ESET. ESET SysRescue, 2022.

[59] ETSI. ETSI TS 119 312 V1.4.1 (2021-08) Electronic Signatures and Infrastructures (ESI); Cryptographic Suites, 2021.

[60] Tommaso Gagliardoni. Quantum Attack Resource Estimate: Using Shor's Algorithm to Break RSA vs DH/DSA VS ECC, August 2021.

[61] John Gantz and David Reinsel. *Extracting Value from Chaos*. IDC, 2011.

[62] Burt Kaliski. PKCS #1: RSA Encryption Version 1.5. Request for Comments RFC 2313, Internet Engineering Task Force, March 1998. Num Pages: 19.

[63] Vlastimil Klíma. Tunnels in hash functions: MD5 collisions within a minute.

[64] M. Matsui, J. Nakajima, and S. Moriai. RFC 3713 a description of the camellia encryption algorithm.

[65] NIST. FIPS 140-2 - security requirements for cryptographic modules.

[66] NIST. *FIPS PUB 202 SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*. NIST, Gaithersburg,, 2015.

[67] NÚKIB. *Národní strategie kybernetické bezpečnosti České republiky na období let 2021 - 2025*. NÚKIB, Brno, 2020.

[68] NÚKIB. Doporučení v oblasti kryptografických prostředků 2.0. page 8, 2022.

[69] P. Oorschot and M. Wiener. Parallel collision search with applications to hash functions and discrete logarithms. In *ACM Conference on Computer and Communications Security*, pages 210–218. ACM Press, 1994.

[70] Patch My PC. Patch My PC - Patch Management Made Easy, 2020.

[71] C. E. Shannon. A mathematical theory of communication. *The Bell System Technical Journal*, 27(3):379–423, 1948.

[72] Sherbrooke. IBM Q Hub - L'Institut quantique at Université de Sherbrooke joins IBM Q Network, 2020.

[73] Nigel P. Smart, Vincent Rijmen, Bogdan Warinschi, and Gaven Watson. *Algorithms, Key Sizes and Parameters Report*. ENISA, Brusel, 2013.

[74] Marc Stevens, Pierre Karpman, and Thomas Peyrin. Freestart collision for full SHA-1. Technical Report 967, 2015.

[75] Nick Sullivan. A (relatively easy to understand) primer on elliptic curve cryptography, 2013.

[76] Evan Sultanik, Trent Brunson, Mike Myers, Alexander Remie, Sam Moelius, Talley Amir, Felipe Manzano, Eric Kilmer, and Sonya Schriner. Are Blockchains Decentralized?, 2022.

[77] Svět sítí. Základy počítačových sítí.

[78] Jordan Tuwiner. 5 Best Bitcoin Mining Hardware ASICs 2020 (Comparison), 2019.

[79] US-CERT. National cyber awareness system.

[80] US-CERT. Us-cert - domácí stránky.

[81] Virus Bulletin. VB100 comparative testing.

[82] Kishan Vyas. Google releases updated Android Distribution numbers for 2021, November 2021.

[83] Xiaoyun Wang, Dengguo Feng, Xuejia Lai, and Hongbo Yu. Collisions for hash functions MD4, MD5, HAVAL-128 and RIPEMD, 2004.

[84] Česko. 297/2016 Sb. Zákon o službách vytvářejících důvěru pro elektronické transakce.

[85] ČR. Elektronická identita | Informační web elektronické identity, 2021.

[86] Pavel Šenovský. *Databáze nebezpečných látek 2005 - Příručka uživatele.* SPBI, Ostrava, 2005.

[87] Pavel Šenovský. *Počítačové sítě a ochrana dat.* VŠB-TU Ostrava, Fakulta bezpečnostního inženýrství, Ostrava, 2015.

[88] Pavel Šenovský. *Bezpečnostní informatika 1 - Návody do cvičení.* VŠB-TU Ostrava, Fakulta bezpečnostního inženýrství, Ostrava, 2017.

[89] Pavel Šenovský. *Bezpečnost informačních systémů.* VŠB-TU Ostrava, Fakulta bezpečnostního inženýrství, Ostrava, 2 edition, 2018.

Slovník

AACS Advanced Access Content System.

AD Active Directory.

AdES Advanced Electronic Signature.

ADSL Asymmetric Digital Subscriber Line.

AES Advanced Encryption Standard.

API Application Programming Interface.

ARPA Advanced Research Projects Agency.

ARPANET Advanced Research Projects Agency Network.

ASCII American Standard Code for Information Interchange.

AWS Amazon Web Services.

BI1 Bezpečnostní informatika 1.

BI3 Bezpečnostní informatika 3.

BIOS Basic Input Output System.

BOINC Berkeley Open Infrastructure for Network Computing.

BSD Berkeley Software Distribution (též Berkeley Unix).

C & C Command and Control Infrastructure.

CAD Computer Aided Design.

CASE Computer Aided System Engineering.

CC Common Criteria.

CCSDS Consultative Committee for Space Data Systems.

CD Compact Disc.

CEN Comité Eurioéen De Normalisation (Evropská normalizační komise).

CERN Organisation européenne pour la recherche nucléaire.

CERT Computer Emmergency Response Team.

CLP Classification, Labelling and Packaging (klasifikace, označování a balení).

CMCKG-PP Cryptographic module for CSP key generation services protection profile.

CMCSO-PP Cryptographic module for CSP signing operations - Protection profile.

CMCSOB PP Cryptographic module for CSP signing operations with backup - Protection profile.

CRC Cyclic redundancy check (kontrolní součty).

CRYPTREC Cryptography Research and Evaluation Comittees.

CSIRT Computer Security Incident Response Team.

CSS Content Scrambling System.

CWA CEN Workshop Agreement.

DARPA Defence Advanced Research Project Agency.

DDoS Distributed Denial of Services.

DES Decryption Encryption Standard.

DHCP Dynamic Host Cache Protocol.

DHT Distributed Hash Table.

DLP Discrete Logarithm Problem.

DNS Domain Name Server.

DOS Desktop Operating System.

DOT Department of Transportation.

DRM Digital Rights Management.

DSA Digital Signature Algorithm.

DSS Digital Signature Standard.

DTP Desktop Publishing.

DVD Digital Versatile Disc.

EAL Evaluation Assurance Level.

ECDLP Elliptic Curves Discrete Logarithm Problem.

ECDSA Elliptic Curves Digital Signature Algortithm.

ENISA European Union Agency for Network and Information Security Agency.

eOP elektronický občanský průkaz.

EP European Parlament.

ETSI European Telecomunication Standards Institute.

EU Evropská unie.

EULA End User Licence Agreement.

FIPS Federal Information Processing Standard.

FIRST Forum for Incident Response and Security Teams.

FRST Farbar Recovery Scan Tool.

FTP File Trasfer Protocol.

GIF Graphics Interchange Format.

GPL General Public License.

GPRS General Packet Radio Service.

GSM Global System for Mobile Communications.

GUI Graphical User Interface.

HIPS Host Intruder Prevention System.

HTML Hyper Text Markup Language.

IDM Identity Management.

IDS Intruder Detection System.

IETF Internet Engineering Task Force.

IIS Internet Information Service.

IMP Interface Message Processor.

INWG International Network Working Group.

IoT Internet of Things.

IPS Intruder Prevention System.

IRC Internet Relay Chat.

IS Informační systém.

ISDN Integrated Services Digital Network.

ISDS Informační systém datových schránek.

ISMS Information Security Management System.

ISP Internet Service Provider.

IST Information Society Technologies.

ISVS informační systémy veřejné správy.

IT Informační technologie.

JRE Java Runtime Environment.

KI kritická infrastruktura.

KII kritická informační infrastruktura.

LAN Local Area Nework.

LGPL Lesser GPL License.

Linux Linux is not Unix.

MAC Media Access Control.

MAN Metropolitan Area Network.

MD Message Digest.

MISTY Mitsubishi Improved Security Technology.

MP3 MPEG-2 Audio Layer III.

MS Microsoft.

NA North America.

NAS Network Attached Storage.

NASA National Aeronautics and Space Administration.

NAT Network Address Translation.

NATO North Atlantic Treaty Organization.

NBU Národní bezpečnostní úřad.

NCKB Národní centrum kybernetické bezpečnosti.

NCP Network Control Protocol.

NESSIE New European Schemes for Signatures, Integrity and Encryption.

NFPA National Fire Protection Association.

NFS Network File System.

NIPS Network Intruder Prevention System.

NIST National Institute for Standards and Technology.

NSA National Security Agency.

NSF National Science Foundation.

NTT Nipon Telegraph and Telephone Corporation.

NUKIB Národní úřad pro kybernetickou a informační bezpečnost.

OAIS Open Archival Information System.

OS Operační systém.

P2P peer to peer.

PARC Palo Alto Research Center.

PC Personal Computer.

PCS Poskytovatel Certifikačních Služeb.

PDF Portable Document Format.

PKE/KEM Public Key Exchange/Key Encapsulation Mechanism.

POSIX Portable Operating System Interface [for Unix].

QES Qualified Electronic Signature.

RAID Redundant Array of Independent Disks.

RFC Request for Comment.

RIPE Race Integrity Primitives Evaluation.

RPC Remote Procedure Call.

RSIT Random's System Information Tool.

RSS RDF Site Summary.

SAGE Security Algorithms Group pf Experts.

SHA Secure Hash Algorithm (bezpečný hašovací algoritmus).

SHS Secure Hash Standard.

SOGIS Senio Official Group Information Systems Security.

SOHO Small Office Home Office.

SQL Structured Query Language.

STP Shielded Twisted Pair.

SŘBD Systém řízení báze dat.

TDEA Triple Data Encryption Algorithm.

TDES Triple DES.

TERENA The Trans-European Research and Education Networking.

TIFF Tagged Image File Format.

TLS Transport Layer Security.

UAC User Access Control.

UCS Universal Character Set.

UD United Devices.

UMTS Universal Mobile Telecomunications System.

URL Universal Resource Locator.

USA United States of America.

UTF-8 UCS Transformation Format.

UTP Unshielded Twisted Pair.

VDSL Very High Speed DSL.

VIS veřejný informační systém.

W3C World Wide Web Consorcium.

WAN Wide Area Network.

WU work unit.

WWW World Wide Web.

XML Extensive Markup Language.

ÚOOU Úřad pro ochranu osobních údajů.

ČR Česká republika.

[title=Seznam zkratek]

Rejstřík