doc. Ing. Pavel Šenovský, Ph.D.

Počítačové sítě a ochrana dat

skripta

Ostrava, 2015

Počítačové sítě a ochrana dat
tento text neprošel jazykovou úpravou

Vysoká škola báňská - Technická univerzita Ostrava, Fakulta bezpečnostního inženýrství

Obsah

Seznam obrázků **5**

Seznam tabulek **7**

Úvod **9**

1 Úvod do počítačových sítí **13**
1.1 Rozdělení sítí . . . 13
1.2 Kabeláž sítí . . . 15
1.3 Síťová architektura ISO/OSI . . . 17
1.4 Ostatní síťová zařízení . . . 20

2 Perimetr sítě a jeho ochrana **27**
2.1 Vnější perimetr sítě . . . 27
2.2 Vnitřní perimetr sítě . . . 30
2.3 Mobilní zařízení - ztráta . . . 31

3 Autentizace a autorizace v počítačových systémech **35**
3.1 Autentizace a autorizace . . . 35
3.1.1 Autentizace znalostí . . . 36
3.1.2 Autentizace vlastnictvím . . . 39
3.1.3 Autentizace vlastností . . . 40
3.2 Identity management . . . 44

4 Ochrana dat **47**
4.1 Zálohování . . . 47
4.1.1 Kam zálohovat . . . 48
4.1.2 Náročnost záloh . . . 50
4.2 Klonování disků . . . 51
4.3 RAID . . . 52

5 Lidský činitel **57**
5.1 Útoky zvenčí . . . 58
5.2 Útoky zevnitř . . . 59

6 Typy útoků a jejich provedení **63**
6.1 Útoky DoS a DDoS . . . 63
6.2 DNS spoofing, DNS cache poisoning . . . 64
6.3 SQL injection . . . 65
6.4 Sociální inženýrství . . . 66

7 Systémy řízení informační bezpečnosti **69**
7.1 Politika ISMS . . . 72
7.1.1 Obsah politiky ISMS . . . 72
7.1.2 Formulace bezpečností politiky ISMS . . . 73
7.2 Bezpečnostní politika IT aktiva . . . 74
7.3 Případová studie Politiky ISMS . . . 75

7.3.1 Úvod . . . 75
7.3.2 Slovník pojmů . . . 75
7.3.3 Bezpečnostní politika . . . 76
7.3.4 Organizace informační bezpečnosti . . . 77
7.3.5 Aktiva a jejich bezpečnost . . . 78
7.3.6 Závěrečná ustanovení . . . 79
7.4 Případová studie Bezpečnostní politiky IT aktiva . . . 79
7.4.1 Úvod . . . 79
7.4.2 Definice a pojmy . . . 79
7.4.3 DMS . . . 80
7.4.4 Organizace systému DMS . . . 80
7.4.5 Závěrečná ustanovení . . . 81
7.4.6 Přílohy . . . 81

Literatura **84**

Seznam zkratek **86**

Rejstřík **87**

Seznam obrázků

1.1 Sběrnicová topologie počítačových sítí . . . 14
1.2 Topologie počítačových sítí token ring . . . 14
1.3 Hvězdicová topologie počítačové sítě . . . 15
1.4 Nejčastěji používané typy kabeláže v počítačových sítích (převzato z [45]) . . . 16
1.5 Komunikace v síti - pohled referenční model ISO/OSI . . . 18
1.6 Switch Cisco Catalyst 2950 . . . 19
1.7 Nastavení formáty data a čísel ve Windows 7 . . . 21
1.8 Příklad NAS TVS-671 od společnosti QNAP (převzato z [43]) . . . 23

2.1 WiFi Analyzer (převzato z [27]) . . . 29
2.2 AP přípojné body Linksys WAP54G (převzato z [37]) a ASUS RT-AC3200 (převzato z [2]) . . . 29
2.3 Vnitřní perimetr sítě . . . 31

3.1 Odemčení telefonu gestem (převzato z [39]) . . . 37
3.2 Výkon louskání hesel pro MS Office 2013 pomocí ElcomSoft Distributed Password Recovery (převzato z [34]) . . . 39
3.3 Zadní strana občanského průkazu (převzato z [42]) . . . 39
3.4 Průkazka studenta (převzato z [47]) . . . 40
3.5 RSA SecurID SID800 token bez USB konektoru (převzato z [30]) . . . 40
3.6 Apple iPhone 5s (Touch ID) vs skaner otisku prstu Samsung Galaxy S5 . . . 41
3.7 Čtečka otisků prstů v notebooku Lenovo ThinkPad 430 (převzato z [15]) . . . 41
3.8 Snímače žilkování na dlani v zařízeních společnosti Fujitsu . . . 42
3.9 Kontrola identity členů městské rady Bagdádu pomocí skenu oční duhovky (převzato z [44]) . . . 43
3.10 SSO pro webové aplikace na VŠB-TU Ostrava . . . 45

4.1 Struktura DVD-R média (převzato z [9]) . . . 48
4.2 RAID-0 se dvěma disky tvořící jeden logický disk (převzato z [19]) . . . 52
4.3 RAID-1 se dvěma disky tvořící jeden logický disk (převzato z [20]) . . . 53
4.4 RAID-5 se čtyřmi disky tvořící jeden logický disk (převzato z [21]) . . . 53
4.5 RAID-6 se pěti disky tvořící jeden logický disk (převzato z [?]) . . . 54

5.1 Působení zaměstnance ve firmě . . . 60

6.1 Příklad bezpečného spojení pomocí WWW prohlížeče Chrome 45 na web ČSOB . . . 65
6.2 Drahoušek zákazník - jeden z prvních zaznamenaných phishingových útoků v ČR . . . 67

7.1 Proces zavedení ISO 27 000 v organizaci . . . 71
7.2 Organizace informační bezpečnosti ve společnosti XYZ . . . 77

Seznam tabulek

3.1 Možný počet kombinací - gesta vs PIN (převzato z [39]) 36
3.2 Možný počet kombinací pro útok hrubou silou na vybrané hashovací funkce 37

4.1 Rychlost zápisu na optická média (převzato z [29]) 48

Úvod

Vážený studente, dostává se Vám do rukou učební text předmětu *Počítačové sítě a ochrana dat*. Tento text je především určen studentům třetího, popř. čtvrtého ročníku Fakulty bezpečnostního inženýrství, předmětu *Počítačové sítě a ochrana dat* v oborech Havarijní plánování a krizové řízení (HPKR) a Technická bezpečnost osob a majetku (TBOM). Svým obsahem skripta navazují na předměty *bezpečnostní informatika 1* a také *Bezpečnostní informatika 2*, kde byla probírána témata relevantní k problematice počítačové bezpečnosti. Jedná se především o problematiku:

- elektronického podpisu (BI1),
- šifrování - symetrického i asymetrického (BI1)
- bezpečné hashovací funkce (BI1)
- kritéria pro hodnocení bezpečnosti systémů (BI2)

Mým cílem při psaní tohoto textu bylo, aby čtenář získal základní přehled v oblasti počítačové bezpečnosti Text samotný svou náplní není zaměřen přímo na informatiky, proto se v jednotlivých probíraných tématech nejde příliš do hloubky. Cílem předmětu (a tohoto textu) proto není vytvořit plnohodnotného IT bezpečnostního pracovníka, ale spíše poučeného uživatele, který bude schopen součinnosti s IT specialisty při koordinaci fyzické a IT bezpečnosti.

Poznatky získané v tomto předmětu jsou také přímo aplikovatelné pro zajištění základní IT bezpečnosti domácích počítačů zapojených v menší (domácí) počítačové síti.

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.

V tomto 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 zkratek (které informatici tak milují) a ona by mě přesměrovala automaticky na seznam zkratek“? 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.

Pro zjednodušení orientace v textu jsem zavedl systém ikon:

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.

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

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 První vydání vydání skript předmětu *Počítačové sítě a ochrana dat*. Přestože se jedná o vydání první navazují tato skripta velmi úzce na dnes již nevyučovaný předmět *Počítače a ochrana dat*

Novinky v 1. vydání skript (proti skriptům Počítače a ochrana dat, 2. vydání)

1. sazba v LaTeX
2. přepracována kapitola věnována počítačovým sítí
3. doplněny informace k zajištění ochrany perimetru sítě
4. kapitola věnována bezpečnostním politikám byla přepracována aby korespondovala s kodexem norem ISO 27 000
5. do kapitoly věnované ochraně dat byly přidány informace o diskových polích RAID
6. řada dalších drobných doplnění a oprav

Kapitola 1

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
3. jaké otázky je potřeba zohlednit při návrhu domácí sítě

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

1.1 Rozdělení sítí

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

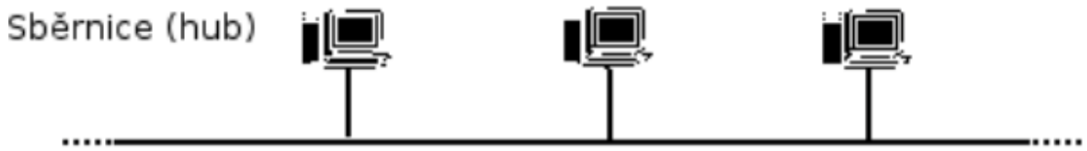
- topologie
- charakteru komunikace
- oblasti, kterou síť pokrývá
- apod.

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 do jisté míry (alespoň ve své čisté podobě). V rámci této topologie se koncová zařízení připojují ke sběrnici. Vizuálně si lze tuto topologii představit jako na obr. 1.1.

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 je pak hlavní kabel zakončen tzv. terminátory, jejichž účelem je pohlcování volných signálů pohybujících se v síti.

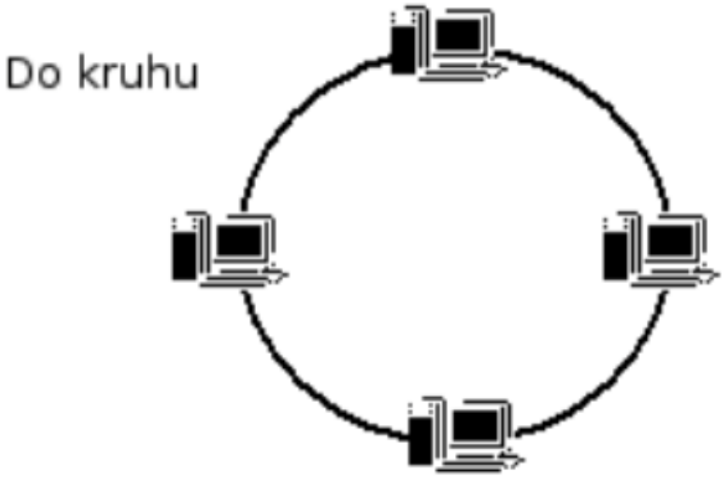


Obrázek 1.1: Sběrnicová topologie počítačových sítí

Použití koaxiálního kabelu znamená 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.

Sítě typu **token ring** jsou z hlediska topologie zajímavé. Vizuálně si je lze představit jako na obr. 1.2. 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 1.2: Topologie počítačových sítí token ring

Fungování těchto sítí si lze představit tak určíme zdroj komunikace na síti a na jeho umístění položíme značku (token). Tuto značku postupně posunujeme v kruhu 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.

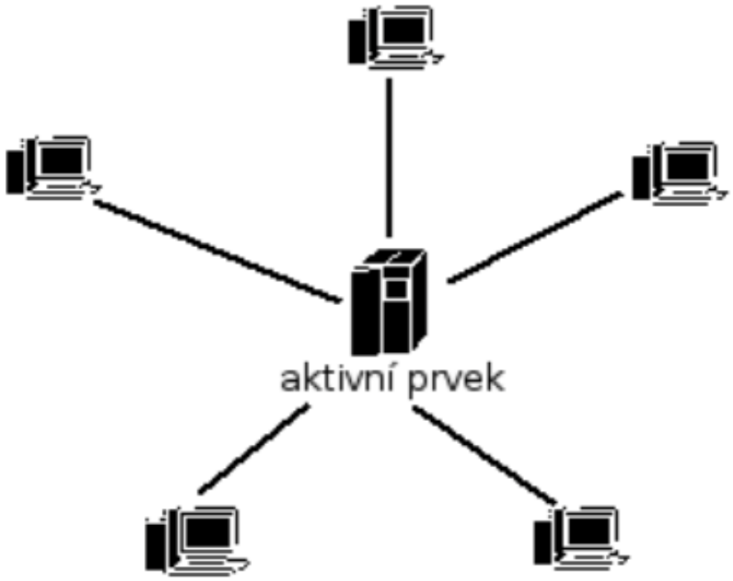
Vizuálně je možné si **hvězdicovou topologii** představit podobně jako na obr. 1.3.

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).

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 jsou ale zapojovány pomocí sběrnicové topologie (pomocí zařízení nazývaných hub). Účelem hybridních topologií je umožnit stavbu rozsáhlejších sítí.

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



Obrázek 1.3: Hvězdicová topologie počítačové sítě

- 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 a Fakulta bezpečnostního inženýrství jsou fyzicky v odlišných částech města. Každá odlehlá lokace proto realizuje vlastní LAN a tyto jsou pak propojeny do rozsáhlejší WAN sítě.

Propojování odlehlejších lokací může být realizováno různým způsobem, lze využít veřejné infrastruktury telefonního vedení, pokud nejsou požadovány 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) nebo Intruder Prevention System (IPS). Tímto způsobem je možné včas detekovat, popř. zabránit šíření virových infekcí nebo propagaci útoku hackerů mezi jednotlivými lokalitami organizace.

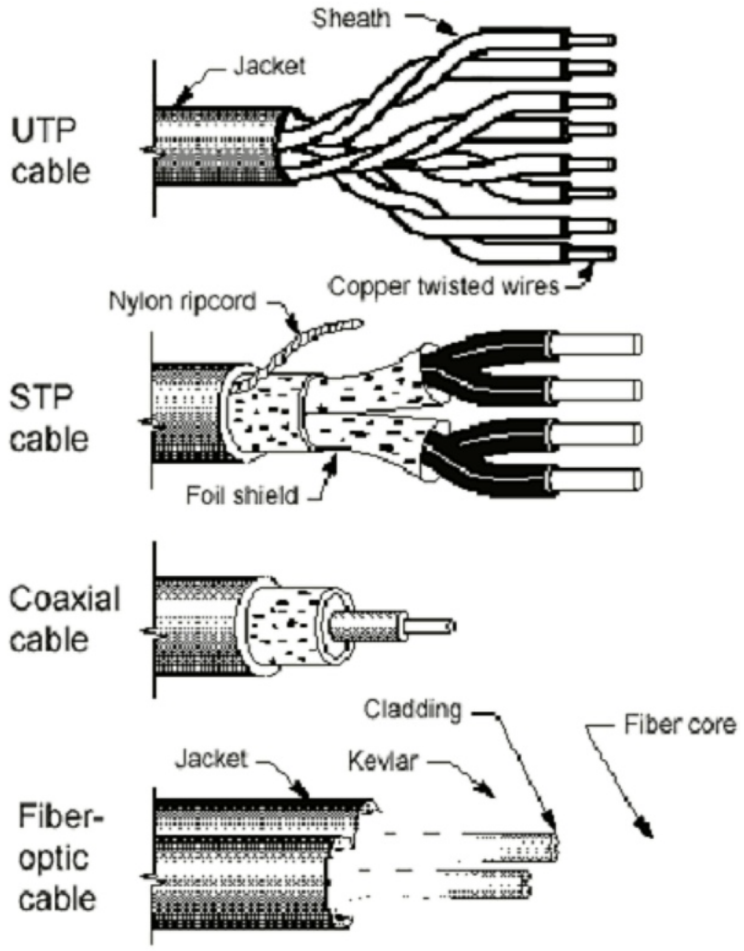
Sítě **MAN** je možno do určité míry připodobnit k veřejným infrastrukturám typu vodovody, kanalizace apod. Města si od budování metropolitních sítí slibují zajímavost pro větší investory, kteří se mohou na takovou síť připojit a získat tak vysokorychlostní připojení k Internetu, samozřejmě za úplatu. Fyzicky jsou takové sítě realizovány pomocí optických kabelů a zřizováním Wi-Fi hot spotů. Organizačně města tuto problematiku řeší zřízením dceřiných firem (s plným vlastnictvím města). Např. v Ostravě funguje tímto způsobem společnost Ova.net [17].

Představitelem **kontinentálních** sítí je např. sdružení CESNET. Jeho hlavním úkolem je výzkum v oblasti a vývoj v oblasti informačních a komunikačních technologií. Toto sdružení také buduje a provozuje síť CESNET2 [5], která propojuje pomocí vysokorychlostního připojení vzdělávací a výzkumné instituce v ČR a je připojena k podobně řešeným sítím zahraničím, zejména síť GÉANT, kterou lze považovat za evropskou páteř výzkumu, vývoje a vzdělávání.

Typickým představitelem celosvětové sítě je pak Internet.

1.2 Kabeláž sítí

Schématické znázornění nejčastěji používaných typů kabeláže je dostupné na obr. 1.4.



Obrázek 1.4: Nejčastěji používané typy kabeláže v počítačových sítích (převzato z [45])

Začít výklad můžeme u kabelu **koaxiálního**, tento kabel se v praxi pro počítačové sítě 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 varianty kabelu, která se použije.

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.

Kabely typu **kroucená dvojlinka** (twisted pair) je v současnosti nejpoužívanějším síťovým kabelem. Kabel tvoří celkem 8 kabelů které jsou zkrouceny po dvou - odtud název kroucená dvojlinka. Zkroucení kabelů není samoúčelné, ale plní velmi důležitou funkci, zmenšuje totiž přeslechy mezi jednotlivými kabely a omezuje též elektromagnetické vyzařování kabelu do okolí.

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 se také rozlišuje podle tzv. *kategorie*. Kategorie se označuje CatX, kde X představuje číslo kategorie. Vyšší čísla v pořadí odpovídají novějším kategoriím. V současnosti je v praxi nejrozšířenějším druhem kabeláže typu Cat5 s přenosovými rychlostmi 100 Mbps (mega-bit za sekundu), popř. 1 Gbps (gigabit za sekundu). Hodnota 1 Gps je na horní hranici možností kabelu.

Nové sítě jsou pak konstruovány pomocí kabeláže Cat6 nebo Cat7 umožňující přenosové rychlosti

až 10 Gbps, ve vývoji je pak kabeláž umožňující ještě vyšší přenosové rychlost (Cat8 až 40 Gbps). Skutečná rychlost sítě však není determinována pouze kvalitou kabeláže, ale také aktivními síťovými prvky, které síťový provoz řídí. Proto pokud např. switch podporuje přenosové rychlosti pouze 100 Mbps, vyšší rychlosti z něj skutečně nedostanete, byť by to kabeláž třeba podporovala.

Z hlediska fyzických vlastností je maximální délka kabelu 100 m a není z něj možné provádět odbočky.

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.

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 nebo stovky 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, kterou je možné překlenout, 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.

1.3 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* [45] nebo články na specializovaných serverech, např. [32].

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.

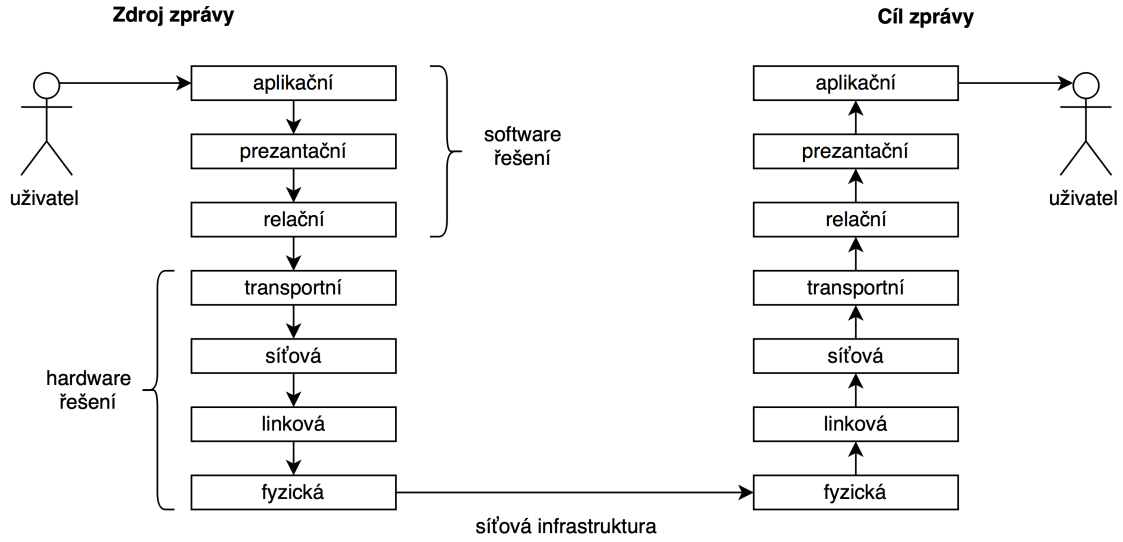
Referenční model se skládá ze sedmi na sebe navazujících vrstev:

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 dodržují. Důvod odhalíme relativně jednoduše při pohledu na seznam vrstev, první vrstvy jsou spojeny s více s hardware. Odchylky v jejich realizaci by proto způsobily 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. 1.5.



Obrázek 1.5: Komunikace v síti - pohled referenční model ISO/OSI

Jak z obr. 1.5 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 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 různých typů kabelů, 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 od použití postupně upouští, jelikož přeposílání komunikace do všech portů představuje neúměrně vysoké zatížení sítě, zejména tam, kde je do sítě zapojeno větší množství zařízení. Alternativu k použití hubu představují zařízení typu *switch*, tato zařízení fungují ale až na vyšší vrstvě počítačové sítě.

Linková vrstva 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 *switche* (přepínače), na která jsme narazili již při výkladů významu hubů.

Switch v zásadě vypadá (viz obr. 1.6) a plní funkci jako hub, činí tak ale inteligentním 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 v násobcích osmi (tedy 8, 16, ..., 48). Počet 48 portů již lze pro praktické nasazení možno považovat za mezní.

[1] v praxi se používají spíše anglické názvy zařízení, než jejich české ekvivalenty

Obrázek 1.6: 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 se nachází cílové zařízení komunikace. Tímto způsobem se výrazně omezí síťový provoz.

Další výhodou je, že switch pracuje transparentně. Transparentností rozumíme to, že z hlediska funkce sítě se jedná o zařízení, které nemění data, která jím procházejí, funguje automatizovaně a proto není potřeba v rámci komunikace switch adresovat (přímo oslovovat).

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 pracuje v současnosti pracuje 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 používá pro adresu čtveřici čísel v intervalu 0 - 255. 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 s jednou 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.

Prudký rozvoj Internetu, ale jasně ukázal, že tento počet je absolutně nedostatečný - definitivní řešení pro představitelnou budoucnost představuje IPv6. Předtím, než se trošku podíváme na novější IPv6, se podívejme ještě na některé adresy, 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 musí se k němu připojit pomocí dalšího zařízení, jako je např. sítová maškaráda (Network Address Translation (NAT)) apod.

Rozsahy adres privátních sítí jsou definované standardem RFC 1918 [22]:

- 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:

- jumbo packety - podpora pro efektivní přenos větších souborů, popř. streamování
- podpora pro elektronické podepisování jednotlivých uzlů v síti (mělo by být obtížnější pro útočníka vydávat se za jiné zařízení)

- podpora šifrování komunikace
- a řada dalších

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.

Přenosová 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, která činí tento typ služeb zajímavých pro aplikace zaměřené čistě na datové přenosy (např. Bittorent). Kontrolu kvality, v případě potřeby, lze realizovat na vyšších vrstvách síťové architektury - především v aplikační vrstvě.

Typickým představitelem nespojových služeb je protokol *UDP*.

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
- Structured Query Language (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 (akupunktura), speciálních znacích apod.

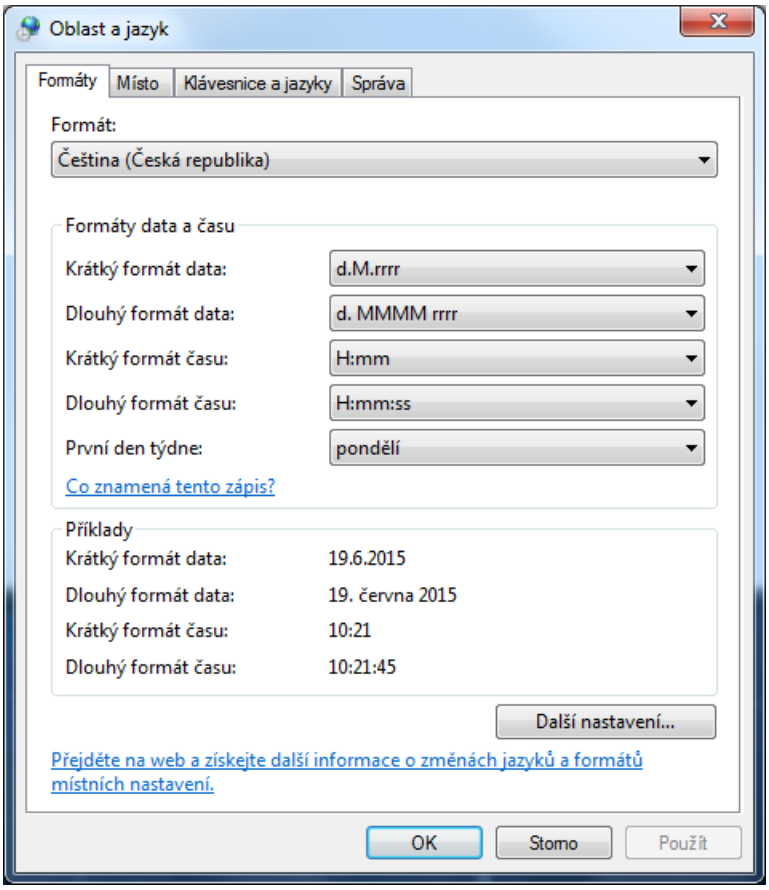
Tyto rozdíly nevznikly přes noc - jsou výsledkem dlouhodobého vývoje jazyků. Problémem je, že počítače nejsou vnitřně navrženy tak, aby se dokázaly s takovými rozdíly samy vypořádat. Uznávají pouze jednu definici čísla, data apod. Prezentační vrstva se proto stará o překlad údajů v těchto striktních 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. 1.7.

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 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.

1.4 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



Obrázek 1.7: 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.

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.

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 virtuální. 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 lépe škálovat.

Lepším zabezpečením máme na mysli především to, že lze mnohem lépe specifikovat okruh uživatelů a způsobu užití serveru - zmenší se tak prostor zneužitelný pro případnou kompromitaci serveru pomocí malware nebo útokem hackera. Škálováním rozumíme přizpůsobení výkonu požadavkům uživatelů.

Službu z tohoto pohledu lze provozovat na jediném serveru nebo v případě potřeby zátěž rozložit na cluster 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.

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.

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. 1.8.

NAS zařízení se vyznačují použitím více disku (dva a více), které je možno propojit do diskového pole. 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:

- 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 počítače. Tento způsob práce je, dalo by se říci, tradiční, je s ním ale spojena také řada nevýhod, zejména v okamžiku kdy takových klientu organizace provozuje stovky nebo tisíce a všechny je musí udržovat. Jakákoliv změna v aplikační logice se v takovém případě vyžádá provedení změn (distribuci upraveného programu) na všech

Obrázek 1.8: Příklad NAS TVS-671 od společnosti QNAP (převzato z [43])

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 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.

Na síti se nachází také celá řada dalších zařízení, které plní různé funkce, některá z nich tady proto ještě zmíníme. První z nich je DynamicHost 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.

Posledním typem zařízení, které v této podkapitole zmíníme je **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 tan osloví cílové zařízení na Internetu.

NAT si pamatuje odkud požadavek vzešel a směřuje tam odpovědi ze zařázení 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 nasadí IPv6, 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 2

Perimetr sítě a jeho ochrana

Náhled kapitoly
V této kapitole bude probrána realizace okraje (perimetru) sítě. Zabývat se přitom budeme jak vnějším perimentrem, který odděluje síť např. podniku od Internetu, tak perimetr vnitřní, kterým jsou oddělovány jednotlivé segmenty sítě.

Po přečtení kapitoly budete
Vědět

1. co je to vnější a vnitřní perimetr sítě
2. co je demilitarizovaná zóna
3. něco málo o Wi-Fi sítích.

Čas pro studium
Pro prostudování této kapitoly budete potřebovat přibližně 2 hodiny.

2.1 Vnější perimetr sítě

Vnějším perimetrem sítě rozumíme rozhraní mezi podnikovou sítí a dalšími sítěmi, obvykle Internetem. Z minulé kapitoly máme určitou představu o některých zařízením, která nám mohou posloužit pro nastavení a řízení síťového provozu provozu přes toto rozhraní. Jedná se o zařízení:

- router (gateway)
- firewall
- systémy IDS nebo IPS

Připomeňme si, že *router* slouží pro směřování síťového provozu, firewall pak slouží pro jeho filtraci. Z hlediska ochrany sítě je firewall základním nástrojem ochrany, který umožňuje nastavit která zařízení (IP adresou) mohou komunikovat a pomocí jakých služeb (nastavením portů).

Teoreticky tedy lze poměrně přesně nastavit pravidla komunikace. Problémem je, že takové nastavení je obvykle poměrně generické. Pracovní stanice v počítačové síti podniku často potřebují využívat celou řadu služeb. Upřesnění nastavení na firewallu by pak vyžadovalo zavádění velkého množství pravidel na firewallu, přičemž platí, že čím více je pravidel, tím je těžší je udržet v aktuální (bezpečné) podobě.

Z tohoto důvodu firewall na vnějším perimetru sítě je doplňován řadou dalších nástrojů, které pak tvoří celkový obraz bezpečnosti v dané organizaci a kromě vnějšího perimetru sítě pak často budujeme také perimetr vnitřní.

Existuje tedy výrazný rozpor mezi požadavky uživatelů na užití služeb počítačové sítě a bezpečnostními aspekty takového použití. Koncoví uživatelé obvykle požadují, aby mohli používat maximum existujících služeb sítě, obvykle bez ohledu na to, jestli pracují přímo v této síti (např. v kanceláři) nebo z nějaké vzdálené lokace (domov, služební cesta, apod.).

V případě, že by síťoví administrátoři pouze povolili dostupnost takových služeb odkudkoliv - mělo by to výrazný dopad na bezpečnost, protože by zároveň tyto služby zpřístupnili komukoliv. Většina služeb v sobě sice má implementován nějakou formu autentizace, avšak její pouhopouhé vystavení umožní případnému útočníkovi, aby hledal chyby v jeho implementaci a pokusil se službu kompromitovat.

Pro vyřešení tohoto rozporu se v praxi využívají zařízení **Virtual Private Network (VPN)**. Úkolem těchto zařízení je zajistit bezpečnou komunikaci mezi vzdáleným koncovým zařízením (např. notebookem) a počítačovou sítí. Bezpečnost je zajištěna tak, že koncový uživatel se autentizuje pomocí klienta VPN proti tzv. VPN koncentrátoru a ten připraví šifrované spojení mezi vzdáleným zařízením a počítačovou sítí podniku. Vzdálený uživatel pak může využívat služeb sítě stejně, jako kdyby seděl ve své kanceláři.

VPN tedy poskytuje velmi cenné služby, ale jak už to bývá, není to zadarmo. Už víme, že veškerá komunikace pomocí je šifrovaná. Toto šifrování musí provádět, jak koncové zařízení uživatele, tak koncentrátor VPN. Koncové zařízení z tohoto pohledu nepředstavuje problém - zabezpečuje komunikaci pouze jednoho člověka. VPN koncentrátor musí ale zajistit připojení celé řady takových vzdálených uživatelů. Každé připojení je přitom šifrováno vlastním klíčem, aby se zajistila odolnost proti odposlechu napříč připojeními. VPN koncentrátor proto představuje určité *úzké hrdlo* komunikace. Aby jej bylo možné efektivně využívat, jsou kladena na jeho uživatele obvykle některá omezení:

- Uživatel se připojuje k VPN pouze v případě, že potřebuje využívat služeb sítě organizace
- délka spojení by měla být co možná nejkratší (udělat, co je potřeba a odpojit se od VPN)
- uživatel by svou činnost vyžadující přenosovou kapacitu sítě měl omezit pouze na pracovní činnosti (tedy žádné videa na YouTube apod.).

Je potřeba mít také na paměti, že VPN chrání pouze datový přenos, pokud tedy bylo koncové zařízení kompromitováno např. virovou infekcí, šifrování datového přenosu už pro ochranu přenášených dat nebude stačit. Ochrana vnějšího perimetru se tedy nemůže omezovat pouze na prostředky managementu sítě, musí pracovat také s ochranou koncových zařízení, především pokud se tato zařízení nacházejí fyzicky mimo objekty organizace.

K ochraně se pak nabízí celá řada nástrojů, jako je:

- proškolování uživatelů
- šifrování disků
- konfigurace koncových zařízení a další.

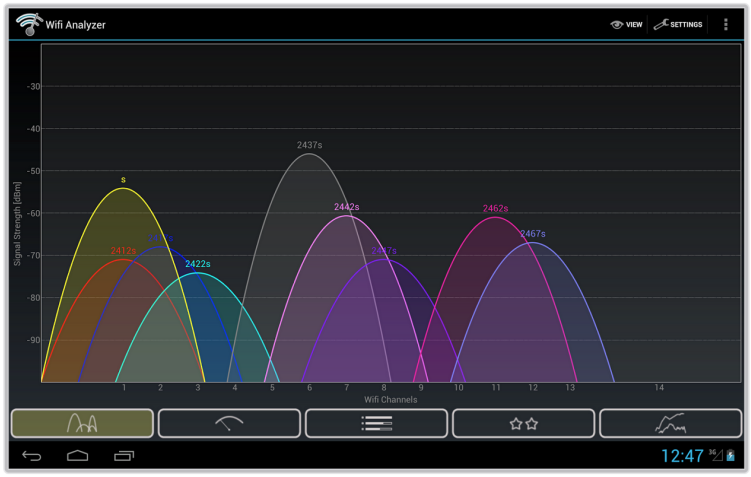
Některými z výše uvedených opatření se budeme věnovat v dalších kapitolách. Předtím, než se tak stane se ale ještě podíváme na další zařízení, která mohou tvořit vnější perimetr sítě. Prvním z těchto zařízení bude Wi-Fi Access Point (AP), tedy přístupové body pro připojení se do sítě Wi-Fi.

Wi-Fi je ve skutečnosti obchodní značka, pod kterou se skrývá celá řada standardů pro bezdrátové připojení. Tyto standardy se skrývají pod označením IEEE 802.11, po kterém následuje písmeno označující verzi standardu. Aktuálně se v praxi využívají standardy 802.11n (pro starší sítě) a 802.11ac (pro novější sítě). Společným prvkem standardů je využití nelicencovaných pásem 2,4 a 5 GHz.

Dosah AP se liší podle použité frekvence a také prostoru, ve kterém je bezdrátová síť provozována. Dosah se výrazně snižuje uvnitř budov využívajících ve větší míře materiálu s horší propustností jako je beton, ocelové konstrukce apod. Velký dopad na dosah má také výběr kanálu, na kterém bude AP vysílat a také další schopnosti AP, jako schopnost směrového vysílání signálu. Vzhledem k tomu, že maximální „síla“ vysílaného signálu je stanovena a její dodržovaní je vymáháno úřadem (Český telekomunikační úřad (CTU)), je použití směrového vysílání jedinou možností jak dosáhnout většího dosahu signálu.

Z hlediska výběru kanálů, je vhodné přihlédnout k bezdrátovým sítím provozovaným v okolí. Vybíráme takový kanál, v nejož okolí nejsou ideálně provozovány žádné bezdrátové sítě. V opačném případě budou interference v signálu způsobovat zmenšení dosahu signálu vysílaného z našeho AP.

Existuje celá řada aplikací pro mobilní telefony nebo tablety, které umožní pohodlné zmapování využití Wi-Fi spektra v dané lokalitě. Výstup z populární aplikace WiFi Analyzer pro zařízení s operačním systémem Android je znázorněn na obr. 2.1.



Obrázek 2.1: WiFi Analyzer (převzato z [27])

(a) Linksys WAP54G (b) ASUS RT-AC3200

Obrázek 2.2: AP přípojné body Linksys WAP54G (převzato z [37]) a ASUS RT-AC3200 (převzato z [2])

Na obr. 2.1 jsou jasně patrné, jak síla signálu bezdrátové sítě (výška paraboly) a také přesah do sousedních kanálů. Pro novou síť hledáme kanály které jsou pokud možno volné a pokud to není možné, je v nich alespoň signál cizích sítí slabý.

Špičková zařízení mají schopnost vysílat najednou v několika směrech a několika frekvencích, aby se maximalizovala přenosová kapacita AP. Rozdíl mezi jednotlivými AP je přitom patrný často na první pohled, srovnejte např. v domácnostech běžně používané zařízení společnosti Linksys s nedávno představeným (VIII 2015) špičkovým zařízením společnosti ASUS RT-AC3200 na obr. 2.2. AP volíme obvykle podle toho, v jakém prostředí má být AP nasazeno a také našich finančních možností.

Z hlediska dosahu platí směrové vysílání má větší dosah než všesměrové vysílání. Z hlediska přenosových rychlostí je teoretickým maximem 802.11n 450 Mbps (Megabit per second), pro 802.11ac pak 1300 Mbps. Takových rychlostí však bývá v praxi dosahováno spíše zřídka. Reálně tak lze očekávat rychlost 240 Mbps pro verzi n standardu a 720 Mbps pro ac verzi standardu.

Co do dosahu lze verzi n pokrýt v ideálních podmínkách venku maximálně 200 m a uvnitř budov pak za ideálních podmínek 60 m. V husté zástavbě se saturovaným spektrem může být problém jeden rodinný domek běžné velikosti (do 150 m^2). Tyto vzdálenosti je však potřeba brát pouze orientačně. Např. Švédská kosmická agentura při svém experimentování s bezdrátovými sítěmi byla schopna při použití nestandardního hardware navázat spojení s AP ve vzdálenosti 420 km.

Prakticky to pro ochranu perimetru sítě znamená, že se nelze spoléhat na pevné hranice sítě, které

je možno ztotožnit z hranicí budovy nebo pozemku ve vlastnictví organizace. Dosah bezdrátových sítí může tuto hranici překonat. Z tohoto důvodu je nutno věnovat nastavení sítě zvýšenou pozornost.

Každá Wi-Fi síť je identifikovaná pomocí tzv. Service Set Identifier (SSID). Toto SSID ale nutně nemusí AP vysílat. Případný uživatel tak musí znát SSID sítě, aby se mohl připojit. Z pohledu bezpečnosti se jedná spíše o bezpečnostní placebo - případný útočník je schopen toto SSID rychle zjistit, jelikož síť samotná je běžně viditelná na analyzátorech provozu sítě.

AP v domácnostech a ve firmách (středních a větších) se liší podporou různých mechanismů autentizace a šifrování síťového provozu. V domácnostech se tak používají:

- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)
- WPA2

Z výše uvedených protokolů je v současnosti možno považovat za **bezpečný pouze WPA2**. Problémem WEP je trojího druhu, prvním je vetšinou šifrování klíčem o délce pouze 128 bitů a dále to, že šifrování je prováděno pro všechny uživatele stejným klíčem - tedy všichni připojení uživatelé mohli sledovat komunikaci ostatních a konečně protokol samotný obsahoval chyby umožňující připojení se bez znalosti autentizačních údajů takřka v reálném čase (bez časové prodlevy).

Bezpečnost WPA je lepší, podporuje šifrování 256-ti bitovým klíčem a využívá také některé další mechanismy pro ochranu přenášených dat, jako je např. separace uživatelů apod. Přesto si WPA zachovává některé aspekty WEP, které z něj činí z hlediska bezpečnosti problematickou záležitost.

WPA2 bylo navrženo tak, aby bylo odolné vůči známým útokům na WEP a WPA. Implementuje uznávaný šifrovací algoritmus AES s dostatečnou délkou klíče. Samozřejmostí je separace uživatelů a řada dalších bezpečnostních mechanismů. Pro domácí použití by proto WPA2 mělo být standardem.

Extensible Authentication Protocol (EAP) Protected EAP (PEAP) Pro podnikové nasazení se používá většinou některá z rozšíření WPA2, konkrétně EAP nebo PEAP. EAP je autentizační rámec. To znamená, že zajišťuje sjednání autentizačních metod (metody EAP) a některé další obecné činnosti. V současnosti je definováno okolo 40-ti metod EAP, jejich název je většinou složeninou EAP a použité autentizační metody např. TTLS, tedy dohromady EAP-TTLS.

PEAP funguje podobně jako EAP, ovšem s tím, že nepřijímá stejné bezpečnostní předpoklady jako EAP. EAP předpokládá, že jsou použity chráněné komunikační kanály, PEAP toto nepředpokládá a zapouzdřuje EAP pomocí šifrované komunikační vrstvy.

Použití EAP nebo PEAP je ve firmách velmi rozšířené, zejména díky možnosti integrovat autentizaci do bezdrátových sítí společnosti s centralizovanými systémy řízení uživatelských účtů ve společnostech a tedy získáním určité kontroly nad tím, kdo se do bezdrátové sítě autentizuje a co na ní dělá.

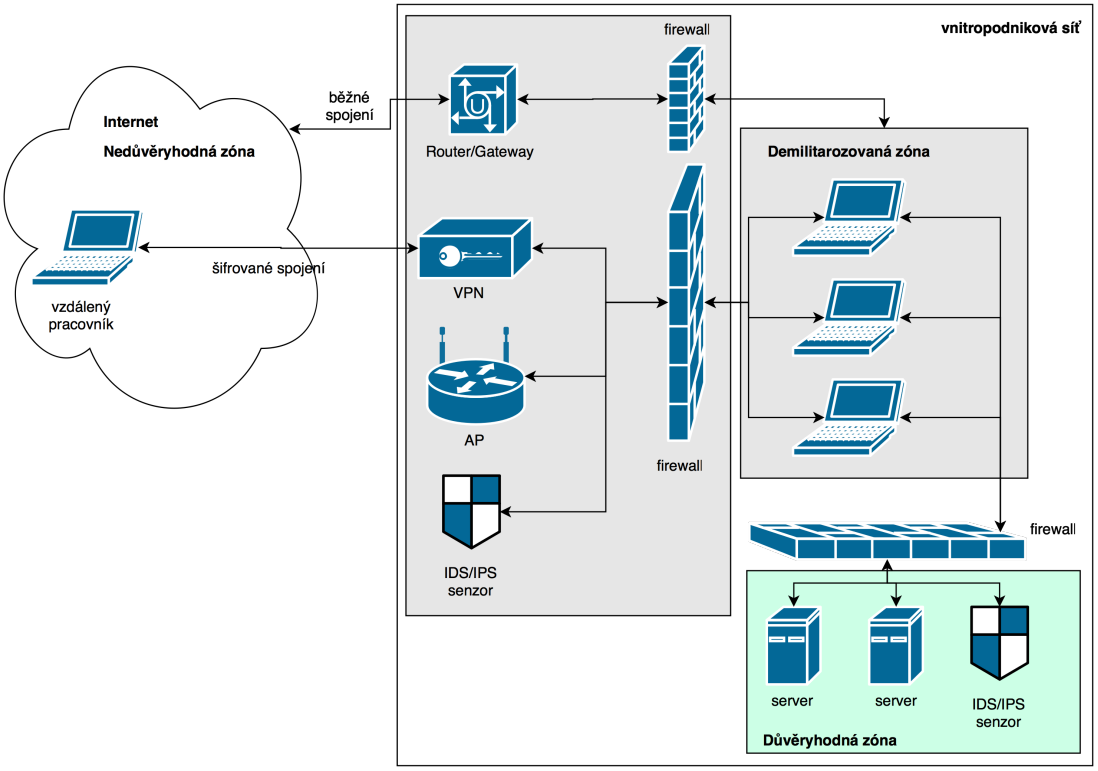
Autentizačním mechanismům je věnována samostatná kapitola.

Připojení WiFi na Fakultě bezpečnostního inženýrství
Prozkoumejte možnost připojení se k WiFi síti v prostorách Fakulty bezpečnostního inženýrství. Použijte `http:\\idoc.vsb.cz` pro zjištění pravidel a použitých mechanismů pro autentizaci do sítě.

2.2 Vnitřní perimetr sítě

Vnitřním perimetrem sítě rozumíme prostředky nasazované uvnitř počítačové sítě organizace pro oddělení obzvláště cenných zařízení od zbytku sítě (ve smyslu řízení síťového provozu z a do nich. Vychází se z toho, že na síti existují zařízení, jako jsou např. servery, pro které je možno velmi přesně stanovit jaká zařízení a jakým způsobem s nimi budou komunikovat. To je velký rozdíl oproti běžným počítačům, kde je obvykle velmi obtížné předem stanovit, jakých služeb bude uživatel využívat.

V souvislosti s budováním vnitřního perimetru často hovoříme o budování tzv. *demilitarizované zóny* (Demilitarizovaná zóna (DMZ)). Určitou představu možném o způsobu realizace si lze udělat z obr. 2.3.



Obrázek 2.3: Vnitřní perimetr sítě

Schéma na obr. 2.3 je pouze orientační. Možností, jak oddělení jednotlivých zájmových segmentů sítě realizovat je celá řada. Složitost pak roste úměrně s velikostí sítě a nároky na ni kladenými. V obecné rovině hovoříme o DMZ ve smyslu části sítě, kterou máme pod kontrolou ale není u ní možné plně kontrolovat bezpečnost. V zásadě se tedy jedná o zónu sítě, kde očekáváme, že mohou vzniknout, nebo se propagovat, problémy, tyto problémy jsme schopni detekovat a řešit.

Proti tomu důvěryhodná zóna je obvykle z pohledu použitých zařízení omezená, což umožňuje nastavení těchto zařízení a konfiguraci filtrace síťového provozu z a do nich směřujícího takovým způsobem, abychom tato zařízení mohli považovat za bezpečná a zónu sítě, ve které se nacházejí za důvěryhodnou.

Síť Internet je proti tomu zcela mimo naši kontrolu, proto všechna zařízení na ní se nacházející je nutno považovat za potenciálně nebezpečná, ovšem s tím, že na rozdíl od DMZ s případnými problémy (útoky) nebudeme schopni v místě jejich vzniku nic dělat. Z tohoto pohledu je tedy tato zóna nedůvěryhodná.

Vybrané činnosti řešitelné oddělením DMZ a důvěryhodné zóny (DZ)

- omezení poskytovaných služeb zařízení v DZ, pouze na ty žádoucí
- nastavení způsobu komunikace mezi důvěryhodnými zařízeními
- možnost omezení poskytování určitých služeb zařízení v DZ konkrétním zařízením v DMZ (např. pro účely správy)
- a další.

2.3 Mobilní zařízení - ztráta

Poslední položkou, kterou je potřeba probrat v souvislosti s perimetrem sítě jsou zařízení, která se mohou používat mimo tento perimetr. Jedná se především o zařízení jsou:

- notebooky,
- mobilní telefony a
- tablety.

Obecně se jedná o jakékoliv zařízení, u kterého se dá očekávat, že může opustit prostory dané organizace a zároveň jeho uživatel bude očekávat stejnou funkčnost jako v případě, že by je použil např. ve své kanceláři. Problém je v tom, že všechna řešení umožňující takovou práci realizovat (z nichž některá jsme si popsali v kapitolách výše) mají dva předpoklady - zařízení je fyzicky v držení oprávněného uživatele a zařízení nebylo kompromitováno.

Co přesně to znamená? Znamená to, že zařízení používá jen a pouze stanovená oprávněná osoba a ne oprávněná osoba, jeho manželka, dítě a náhodný kolemjdoucí jménem Ted. Toto omezení je pravděpodobně snadno pochopitelné, pokud zařízení nemáme pod kontrolou, těžko můžeme zaručit, co se s ním bude dít. Zároveň zaměstnance organizace je možno proškolit o bezpečném používání zařízení, jeho rodinné příslušníky však nikoliv. V praxi se ale takové pravidlo dodržuje poměrně obtížně, konečně co je špatného na tom, když si návštěva rychle něco vyhledá nebo vyřídí na vašem notebooku?

Zapůjčení zařízení lze považovat za první krok k jeho kompromitaci. Mnohem závažnější je však ztráta nebo odcizení zařízení. Tímto způsobem se zařízení dostane zcela mimo kontrolu oprávněného uživatele. Metod jak zajistit ochranu údajů v těchto zařízeních obsažených je celá řada, typově lze zmínit dva:

1. šifrování
2. vzdálený výmaz systému (wipe systému)

V tento text není zaměřen na rozebírání jednotlivých šifrovacích schémat, konečně předpokládá se, úspěšné absolvování předmětu *Bezpečnostní informatika 1*, které se touto problematikou poměrně podrobně zabývá. Zde se proto omezíme spíše na možnosti, které nám v tomto ohledu nabízejí jednotlivé operační systémy.

Windows ve verzích určených pro podniky (enterprise verze) poskytují nástroj *Birlocker*, který slouží pro šifrování disků nebo diskových oddílů. Toto šifrování je relativně rychlé a především bezpečné, takže si nezapomeňte zálohovat (a bezpečně uschovat) šifrovací klíče, protože bez nich není šifrované disky možné dešifrovat.

Alternativně je možno použít řadu dostupných softwarových nástrojů pro šifrování, ať už komerčních nebo open source. Za krále nástrojů pro šifrování disků byl dlouhou dobu považován *True Crypt* [24], v květnu 2014 však tento nástroj přestal být dále vyvíjen a na jeho stránkách se objevilo upozornění, že True Crypt nemusí být bezpečný a řada migračních návodů pro použití alternativních šifrovacích nástrojů. Existuje celá řada projektů, které mají ambici TrueCrypt nahradit. Zmínit lze např. CipherShed [6], VeraCrypt [25] a další. Ovšem žádná z těchto náhrad není bez problémů.

VeraCrypt je možno vnímat jako snahu pokračovat ve vývoji původního True Cryptu. VeraCrypt vychází z kódu True Cryptu, opravuje některé chyby a postupně uvádí i některé novinky zvyšující výkon šifrování nebo jeho bezpečnost. Problémem tohoto programu je, že dnes není úplně jisté jak moc bezpečné jsou vlastně kódy True Cryptu. Během posledního roku sice proběhly dva bezpečnostní audity tohoto software, které neodhalily nějaké kritické nedostatky, přesto není možné zaručit, že implementace zvolených šifrovacích schémat je správná. Což podrývá důvěryhodnost VeraCryptu. Přesto je pravděpodobně lepší použít VeraCrypt než TrueCrypt, už jen proto, že VeraCrypt je stále podporován.

CipherShed také vychází z kódů True Cryptu, ale jeho cíle jsou trochu jiné. Vývoj je zaměřen na udržení plné kompatibility s disky šifrovanými pomocí True Crypt, patrné je také extenzivní zaměření na auditování změn v softwaru. Oproti VeraCrypt dosud (září 2015) nebyla uvolněna použitelná verze software. Podrobnější popis rozdílů mezi výše uvedenými softwarovými balíky je možno nalézt na stránkách lze nalézt v diskuzních fórech TCnext [26].

V případě operačního systému Linux je kromě možnosti použití výše uvedených programů (kromě Bitlocker) zapnout podporu šifrování oddílů přímo v jádru operačního systému. Šifrování disků je také dostupné v OS X, formou nástroje *FileVault*. Od verze OS X 10.10 se je přitom šifrování disku implicitní volbou (předvoleno šifrování disku, které musíte vypnout, pokud jej nechcete).

Na úrovni tabletů a mobilních telefonů se šifrování postupně stalo standardem, který podporují prakticky všichni výrobci těchto zařízení. Standardem se bohužel ale nestalo bezpečné uzamčení těchto zařízení (pomocí hesla, PIN nebo ověření biometrických údajů), bez kterého silné šifrovací algoritmy nemohou poskytnout požadovanou ochranu.

V oblasti vzdáleného výmazu jsou možnosti většiny zařízení omezené - dobře tuto oblast mají vyřešené zařízení společnosti Apple (počítače, notebooky, tablety i mobilní telefony). V jejich případě je možné vzdálený výmaz provést pomocí služby iCloud. Na koncových zařízeních musí být povolena služba najít MůjMac. Alternativně je možno zařízení vyhledat pomocí vestavěného sledování polohy.

V případě zařízení dalších výrobců je situace složitější. V případě počítačů s operačním systémem Windows a Linuxu je potřeba s touto možností počítat předem a nainstalovat specializovaný software, který tuto funkčnost zajistí. Podobně je V případě mobilních telefonů s Windows (od verze 7) je možno provést vzdálený wipe systému, pokud se telefon synchronizuje proti Active Directory (viz kapitola věnovaná autentizaci). Telefony a tablety s operačním systémem Android je možno vzdáleně blokovat, smazat nebo hledat, pokud je toto zařízení připojeno ke Google účtu (Android zařízení prakticky vždy je připojeno k nějakému účtu Google).

Shrnutí

Úvahy okolo bezpečnosti *vnějšího a vnitřního perimetru sítě* tvoří základ většiny úvah o počítačové bezpečnosti. Perimetrem se rozumí okraj, který je potřeba řídit. Základním zařízením pro tento účel jsou firewally. V počítačové síti podniku často vytváříme vnitřní perimetr, abychom vytvořili důvěryhodnou zónu obsahující servery a další obvzláště cenná IT aktiva společnosti a zónu demilitarizovanou, kde očekáváme vznik problémů (v síti společnosti).

Kromě úvah o řešení perimetru jako takového je potřeba věnovat pozornost také jednotlivým zařízením, které lze použít pro připojení se do počítačové sítě organizace, nebo které mohou obsahovat citlivé údaje. Jedná se především o notebooky, tablety a mobilní telefony. Pro taková zařízení je potřeba předem rozhodnout, jakým způsobem budou chráněna, přičemž základními prostředky ochrany je šifrování a nastavení možnosti vzdáleného výmazu systému, aby se předešlo kompromitaci zařízení. Koncový uživatel zařízení by měl být také poučen (proškolen) o bezpečném používání svěřeného zařízení a o postupu, který má použít v případě jeho ztráty nebo odcizení.

Kontrolní otázky

1. Co je vnější perimetr sítě?
2. Co je vnitřní perimetr sítě?
3. Je možno demilitarizovanou zónu považovat za bezpečnou a proč.
4. Co rozumíme dálkovým výmazem (wipe) systémů?
5. Jaký je poslední standard pro Wi-Fi?
6. Jaký systém zabezpečení domácí WiFi sítě je možno bezpečně použít?
7. Jaký je rozdíl v nasazování WiFi v domácnostech a středních/velkých podnicích?

Odpovědi

1. Vnější rozhraní (síť organizace - Internet)
2. Rozhraní mezi zájmovými segmenty sítě, obvykle s různou úrovní důvěryhodnosti)
3. Ne. Demilitarizovaná zóna je tvořena běžnými počítači v síti, pro které obvykle není možné provést výrazné omezení přijímaných a poskytovaných síťových služeb, proto nelze řídit bezpečnost tak dobře jako v případě např. serverů.
4. Rozumíme tím dálkové spuštění výmazu systému (službou k tomu určenou) s cílem zabránit zneužití informací obsažených na daném zařízení. Dálkový výmaz obvykle spouštíme po ztrátě nebo odcizení zařízení.
5. WPA2
6. V podnikovém nasazení je často připojení do bezdrátové sítě je spojeno s autentizací proti jednotnému systému řízení identit uživatelů.

Kapitola 3

Autentizace a autorizace v počítačových systémech

Náhled kapitoly
Prokázání identity systému (autentizace) a potvrzení činnosti v systému (autorizace) jsou základní obranné mechanismy, které lze nasadit softwarově pro ochranu dat a služeb poskytovaných IT aktivy organizace.

Po přečtení kapitoly budete
Vědět

1. jaký je rozdíl mezi autentizací a autorizací
2. jaké druhy autentizace se používají a jak jsou spolehlivé
3. co jsou systémy řízení identit uživatelů a jak fungují

Čas pro studium
Pro prostudování této kapitoly budete potřebovat přibližně 2 hodiny.

3.1 Autentizace a autorizace

Procesem **autentizace** rozumíme postup, kterým automatizovanému systému prokazujeme identitu. Existují přitom tři základní možnosti jak identitu prokázat:

1. znalostí
2. vlastnictvím
3. vlastností

Identifikace *znalostí* předpokládá, že svou identitu prokážete systému tím že víte něco, co můžete vědět právě jen a pouze Vy (např. heslo). *Vlastnictvím* prokazujeme identitu vlastnictvím nějakého fyzického předmětu, který je pro nás unikátní, např. čipová karta. Konečně *vlastností* prokazujeme identitu systému tím, čím jsme - tedy fyzickou vlastností tělesné části (např. otisk prstu, sken sítnice apod.).

Alternativně je možno k autentizaci použít kombinaci výše uvedených postupů, tedy např. vlastnictvím a znalostí (kreditní karta + PIN).

Autorizace v systému proti tomu probíhá jinak. Autorizace přichází na řadu teprve po autentizace - uživatele tedy úspěšně prokázal systému svou identitu, ale vykonal v systému činnost takové závažnosti, že se navíc vyžaduje autorizace této činnosti. Nejjednodušší příklad, se kterým máme

všichni zkušenosti, je použití elektronického bankovnictví. Do bankovnictví se hlásíme pomocí svého uživatelského jména a hesla, pro provedení transakce jsme ale obvykle vyzváni k zadání kontrolního kódu, který banka zašle pomocí SMS na mobilní telefon uživatele.

Autorizace je tedy krok navíc, v rámci kterého prokazujeme identitu odlišným způsobem než v případě autentizace. Použití odlišného mechanismu prokázání identity vychází z toho, že pokud byl jeden autentizační mechanismus kompromitován, je naivní očekávat, že jej útočník nepoužije opakovaně. Odlišný mechanismus ověření identity zajišťuje, že pravděpodobnost současné kompromitace různých ověřovacích mechanismů je menší.

Podívejme se podrobněji na jednotlivé typy autentizace.

3.1.1 Autentizace znalostí

Nejčastěji používanou metodou ověření identity je pomocí určité znalosti určité, kterou má pouze oprávněný uživatel. Autentizace znalostí může nabývat různých podob:

- hesla
- PIN
- pass fráze
- kombinace uživatelského jména a hesla
- gesta (pro odemčení např. tabletu nebo mobilního telefonu)

Z hlediska bezpečnosti jsou poměrně problematická gesta. Odemykání pomocí gest funguje tak, že uživateli se zobrazí obrázek a ten odemkne zařízení pohybem po určitých částech takového obrázku. Nedávné studie o použití takových metod však odhalily, že tento typ autentizace není možno považovat za bezpečný.

Prvním problémem je samotný display. Lidská kůže má totiž jednu nepříjemnou vlastnost - je mastná. Prakticky to znamená, že všechny dotykové displaye jsou do určité míry „zapatlané“. V těchto šmouhách je pak často možno identifikovat vzory, které pak lze využít pro odemknutí.

Schválně otřete pečlivě display display svého mobilního telefonu a následně na něj napište nějaké písmeno - stopu Vašeho prstu se pokuste na ztmaveném displayi najít.

Druhým problémem je to, že pohyb gesta samotného není náhodný, lze jej také odpozorovat a počet kombinací není nevyčerpatelný, viz srovnání počtu možných kombinací gest a čísel PIN viz tab. 3.1. Z bezpečnostního hlediska proto není možné použití gest doporučit jako plnohodnotnou náhradu PIN nebo hesel (pass frází). Určitou představu o fungování gest je možné učinit z obr. 3.1.

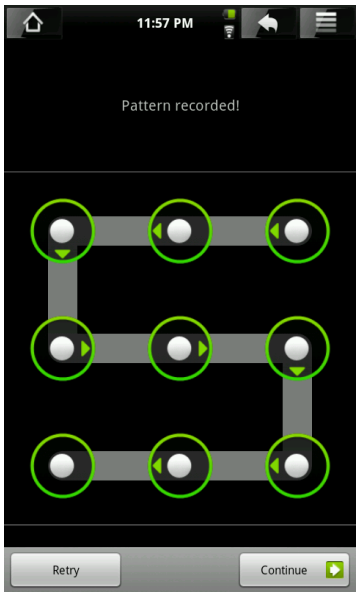
Tabulka 3.1: Možný počet kombinací - gesta vs PIN (převzato z [39])

N	**spojení N bodů**	**PIN používající N čísel**
2	56	100
3	360	1 000
4	2 280	10 000
5	14 544	100 000
6	92 448	1 000 000
7	588 672	10 000 000
8	3 745 152	100 000 000

Výše uvedené metody autentizace jsou všeobecně známé snad s výjimkou *pass fráze*. Základním předpokladem bezpečnosti hesla je, že heslo musí být relativně dlouhé a také silné - tedy odolné proti odhadnutí nebo tzv. slovníkovým útokům (o těch později). Ideálně by tedy heslo mělo být náhodným shlukem alfanumerických znaků a délce 10 - 16 znaků. Takové heslo je ale velmi obtížně zapamatovatelné. Člověk má ale schopnost zapamatovat si lépe celou větu. Takovým větám, které používáme místo hesla, říkáme pass fráze.

Vztah mezi délkou hesla a jeho bezpečností lze poměrně jednoduše odvodit. Podle způsobu, jakým je heslo v systému uloženo je možno k výpočtu složitosti útoku hrubou silou (vyčerpání všech možných hesel) přistoupit dvěma různými způsoby. V případě, že heslo je v systému chráněno šifrováním. Celkový prostor nutný prohledat je možno v takovém případě odhadnout pomocí vzorce (3.1):

$$k = p^m \tag{3.1}$$



Obrázek 3.1: Odemčení telefonu gestem (převzato z [39])

kde k ... celkový počet možných hesel, p ... počet písmen ve zvolené abecedě, m ... počet znaků hesla.

Ze vzorce (3.1) vyplývá, že složitost útoku hrubou silou v takovém případě roste lineárně s velikostí použité abecedy a exponenciálně s délkou hesla. Můžeme si to demonstrovat na několika jednoduchých příkladech:

1. anglická abeceda (24 písmen), délka hesla 5 znaků - $k = 24^5 = 7\ 962\ 624$
2. anglická abeceda, velká a malá písmena, délka hesla 5 znaků - $k = 48^5 = 254\ 803\ 968$
3. + čísla, další znaky a česká diakritika, délka hesla 5 znaků - $k = 99^5 = 9\ 509\ 900\ 499$
4. abeceda, jako v případě 3., délka hesla 8 znaků - $k = 99^8 = 9\ 227\ 446\ 944\ 279\ 201$

Alternativou k šifrování hesla je uložení hesla formou hashe - tedy výsledku jednocestné matematické kryptografické funkce. Jednocestnost zaručuje, že takto uložené heslo nepůjde dešifrovat. Rozdílem proti šifrování je také to, že délka šifrovaného textu (hesla) proporcionálně odpovídá délce hesla, u hashovaného hesla tomu tak není - výsledkem je vždy textový řetězec o přesně stanovené délce odpovídající použitém algoritmu.

Složitost útoku se proto odvozuje trochu jinak, viz (3.2).

$$k = 2^m \tag{3.2}$$

kde k ... složitost útoku, m ... délka hashe v bitech.

V tab. 3.2 je k dispozici vypočtená složitost útoku hrubou silou pro vybrané populární hashovací algoritmy.

Tabulka 3.2: Možný počet kombinací pro útok hrubou silou na vybrané hashovací funkce

algoritmus	**délka hashe [bit]**	**složitost útoku**
MD5	128	$3,4 \cdot 10^{38}$
SHA-1	160	$1,5 \cdot 10^{48}$
RIPEMD-160	160	$1,5 \cdot 10^{48}$
SHA-512	512	$1,34 \cdot 10^{154}$

Počet kombinací pro útok hrubou silou je tedy v tomto případě velmi problematický (přesahuje možnosti současné výpočetní techniky). Existuje několik možností, jak se k tomuto problému postavit. Lze analyzovat samotný použitý algoritmus a hledat slabiny v jeho implementaci. Tímto způsobem lze výrazně omezit prostor, který v rámci útoku bude potřeba prohledat. I tak však tento prostor

zůstává, při současné úrovni poznání, příliš veliký pro to, aby takový útok byl efektivní. Útočníci se proto obvykle zaměřují na účty chráněnými tzv. *slabými hesly*.

Slabé heslo je takové, které je možno jednoduše odhadnout a to buď na základě znalosti dané osoby a nebo hrubou silou pomocí tzv. slovníkového útoku. Obětí znalosti se v roce 2005 stal např. účet Paris Hilton u společnosti T-Mobile. Jako spousta webových aplikací i ta od T-Mobile má kontrolní otázky pro ověření identity v případě, že uživatel zapomene heslo. Jednou z takových otázek byla také otázka na jméno psa. Problém je, že toto jméno bylo všeobecně známé: *Tinkerbell* a průnik na účet byl hotový.

Slovníkový útok využívá toho, že náhodně generovaná (bezpečná) hesla se špatně pamatují, proto řada uživatelů volí hesla, která nejsou náhodná, dávají tedy smysl. Z jazykového pohledu se obvykle jedná o slova, každý jazyk má omezenou slovní zásobu.Ačkoliv je takových slov obvykle velké množství, v žádném případě se tento počet ani vzdáleně neblíží počtům uvedeným tabulce 3.2.

Útočníkovi pro úspěšné proniknutí do systému stačí obvykle kompromitovat jediný účet a ten pak zneužít pro další průnik. V případě, že uživatelských účtů jsou tisíce, je šance, že alespoň jeden z nich bude zabezpečen slabým heslem poměrně velká.

Pokud jsou místo šifrování hesel použity hashe, je možné použít také tzv. *rainbow tables* (duhové tabulky). Pokud je znám algoritmus, kterým je vypočítáván hash, je možno vytvořit předem tabulku hashů a jim odpovídajících hesel, tak že hesla postupně proženeme hashovací funkcí a hash prostě spočítáme. Pokud pak útočník získá databázi hashů hesel systému, kam chce proniknout - stačí mu porovnat hashe hesel s předpřipravenou rainbow table a hledat takové hashe, které se v ní vyskytují. K takovým hashům pak jednoduše odečte z tabulky. Vyhodnocení i tisíců účtů může pomocí takových tabulek proběhnout během pár sekund.

Existuje metoda, kterou se lze použití rainbow tables bránit - jmenuje se *solení hesel*. Solení hesla spočívá v tom, že k heslu přidáme náhodně vygenerovaný řetězec a teprve takto upravené heslo proženeme hashovací funkcí. Heslo samotné pak představuje pouze část potřebné informace k průniku do systému. Solení hesel by v dnešní době mělo představovat standard v zabezpečení hashem chráněným účtům.

Silná hesla a možnost jejich ztráty

Už víme, že silné heslo je obtížněji zapamatovatelné než heslo slabé. Jedou z metod, které lze použít pro předcházení problémů z toho plynoucích je heslo si někam zapsat. Zapsání hesla však samo o sobě může představovat bezpečnostní riziko, pokud se neudělá správně. V zásadě existují dvě možnosti, jak postupovat a přitom zůstat v bezpečí:

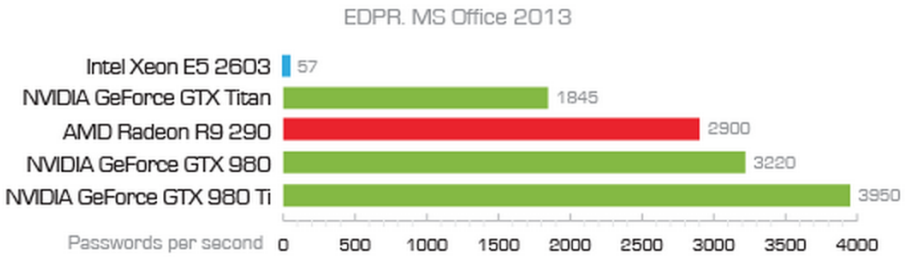
- *zapsání na papír* - je možno provést, pokud místo kam bylo heslo zapsáno je bezpečné - např. papír s heslem se zalepí do obálky a uzamkne v trezoru, skříně (nebo někde jinde) podle citlivosti chráněných údajů
- *použití specializované aplikace* v počítači nebo na mobilním telefonu - hesla k účtům jsou přitom chráněna jedním heslem do aplikace, po jeho zadání je možno uložená hesla zobrazit. Při použití je nutno dát pozor, aby byl program instalován z oficiálního zdroje, byl aktuální a pokud má online komponentu např. synchronizovanou do cloudu je nutné také sledovat informace o bezpečnosti a v případě průniku na servery služby hesla změnit.

Poslední otázkou, kterou v této podkapitole je potřeba zodpovědět je, jak rychle dnešní počítače jsou schopné útoky hrubou silou provádět. Odpověď na tuto otázku není vůbec jednoduchá, protože útok lze realizovat pomocí běžného procesoru (CPU), grafické karty (GPU), je možno si pronajmout virtualizované výpočetní prostředí jako je např. Amazon EC2. V případě, že je útok prováděn na vzdálený systém, úzkým hrdlem nemusí být výkon hardware, ale přenosovou kapacitou síťového připojení, popř. schopností cílového systému vyřizovat požadavky.

Velké rozdíly jsou také v efektivitě implementace jednotlivých kryptovacích algoritmů a algoritmů bezpečných hashovacích funkcí. Obecně se dá říci, že použití grafických karet (pokud je jejich nasazení technicky možné) výrazně urychluje proces prolamování hesel.

Určitou představu si lze udělat z grafů společnosti Elcomsoft, která se zabývá vývojem software pro prolamování hesel do různých systémů, viz obr. 3.2.

Na obr. 3.2 je jediným běžným CPU Intel Xeon E5 2603, ostatní zařízení jsou high-endové herní grafické karty společností AMD a NVidia. Hlavním důvodem výkonnostního rozdílu jsou rozdíly v architektuře mezi CPU a moderními GPU. Např. výše uvedený procesor Intel Xeon má 4 jádra, NVidia



Obrázek 3.2: Výkon louskání hesel pro MS Office 2013 pomocí ElcomSoft Distributed Password Recovery (převzato z [34])

GeForce GTX 980 Ti má ale k dispozici více než 2 800 výpočetních jader. Problém prolamování hesel je přitom velmi dobře zpracovatelný pomocí paralelních výpočtů a odtud pak pochází tento ohromný výkonnostní rozdíl.

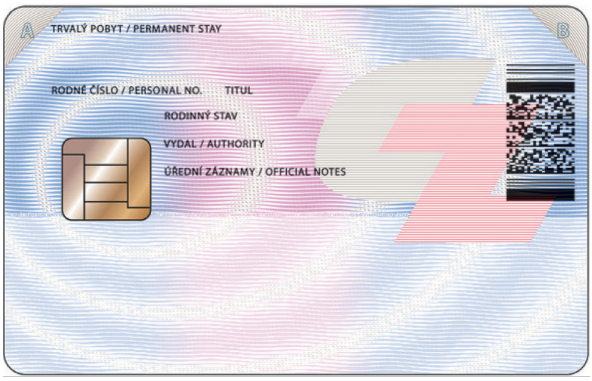
Na stránkách společnosti Elcomsoft [34], lze najít další benchmarky pro různé typy problémů. Benchmarky pro různé konfigurace hardware, ale i software je možné nalézt také pro open source nástroj John the Ripper [14] a řadu dalších.

3.1.2 Autentizace vlastnictvím

Autentizace vlastnictvím umožňuje prokázat identitu pomocí vlastnictví nějakého předmětu. Pro tento účel se používají nástroje jako jsou:

- čipové karty (karty s magnetickým páskem)
- čipy (např. RFID)
- průkazy s elektronicky čitelnými údaji
- tokeny
- a další

Příkladem **průkazu se strojově čitelnými údaji** je např. občanský průkaz. Strojově čitelná zóna je na zadní straně průkazu vpravo, viz obr. 3.3. V případě občanského průkazu může být vydávána také varianta s čipem. Praktické použití tohoto čipu je však dosud velmi omezeno, viz Peterka [42].



Obrázek 3.3: Zadní strana občanského průkazu (převzato z [42])

Dobrým příkladem **čipové karty** karta studenta. Tato karta obsahuje čip, který na rozdíl od čipů na kreditních kartách nebo občanském průkazu není viditelný, kterým se může student autentizovat do řady systémů na univerzitě (systém stravování, počítačové kiosky, celoškolské počítačové učebny dostupné volně studentům v hlavní budově univerzity apod.).

Náhled vzhledu průkazu je na obr. 3.4.

Čipové karty se často používají pro kontrolu vstupu a obdobné aplikace, použití pro autentizaci do běžných počítačových systémů, jako je např. PC je ale spíše neobvyklé (byť technická řešení existují), protože vyžaduje přítomnost specializované čtečky. Naopak velmi populární je použití **tokenů**, popř. možnost použití mobilního telefonu s nainstalovanou bezpečnostní aplikací.

Obrázek 3.4: Průkazka studenta (převzato z [47])

Představu o vzhledu tokenu je možno si udělat z obr. 3.5. Na obr. je znázorněn RSA SecurID token generující bezpečnostní kód použitelný v kombinaci s uživatelským jménem a heslem pro autentizaci do systému. Použití je tedy v rámci multifaktorové autentizace.

Obrázek 3.5: RSA SecurID SID800 token bez USB konektoru (převzato z [30])

Tokeny mohou být kombinovány s USB portem a flash pamětí. Většinou jsou opatřeny karabinkou umožňující připnutí je svazku klíčů, což výrazně zmenšuje šanci, že token bude ztracen.

Všechny metody autentizace pomocí vlastnictví předmětu má jednu závažnou vlastnost - je možno je relativně jednoduše odcizit. To je důvod proč se tyto nástroje často nepoužívají samostatně. Pro kontrolu vstupu může kontrolovat ostraha, zda vlastník karty, která byla použita pro vstup do objektu odpovídá člověku, kterému byla vydána.

3.1.3 Autentizace vlastností

Autentizace vlastností umožňuje prokázat identitu systému pomocí vlastností lidského těla. Existuje celá řada metod, které spolehlivě umožní identifikovat člověka. Např. DNA je jednou z nejspolehlivějších metod. Vyhodnocování DNA je však drahé a trvá opravdu dlouho. Experti na forenzní vědy jsou schopni spolehlivě identifikovat člověka podle chůze, pro účely autentizace ale nemůžeme např. po zaměstnanci očekávat, že před zahájením práce na počítači projde kanceláří třikrát tam a zpátky aby mohla být zhodnocena jeho chůze.

Pro autentizaci se proto volí takové vlastnosti, které je možno rychle, levně a spolehlivě měřit. Požadavkem zároveň je, že snímací senzor by neměl zabírat příliš mnoho místa. Tedy jaké typy autentizace vlastností se v praxi používají:

- sken siluety ruky
- snímání otisku prstu
- sken žilkování na dlani

(a) Touch ID v iPhone 5s (převzato z [23] (b) Samsung Galaxy S5 snímač (převzato z [12])

Obrázek 3.6: Apple iPhone 5s (Touch ID) vs skaner otisku prstu Samsung Galaxy S5

- skenování oční duhovky
- skenování oční sítnice

Jednotlivé typy snímačů se liší výrazně cenou, svou velikostí, přesností a také způsobem použitím. Jeden z nejstarších typů snímačů je snímač umožňující sejmutí vlastností ruky. Ruka je přitom tradiční a logickou volbou. Evoluce dala v ruce člověku do vínku nástroj se kterým se snadno manipuluje, je přiměřeně velký a zároveň existují signifikantní rozdíly v populaci v tom jak ruka vypadá.

Prvotní snímače se zaměřovaly na snímání základních vlastností ruky - tedy počet prstů, jejich délka a šířka, velikost dlaně apod. V malých skupinách osob je tento působ rozlišení mezi osobami možno akceptovat, u větších skupin se ale výrazně zvyšuje riziko shody vlastností ruky mezi různými lidmi. Právě tento problém vedl k tomu, že se snímače ruky braly spíše jako doplňující prvek ochrany, než jako hlavní způsob ochrany, zejména v okamžiku, kdy se začaly ve větší míře prosazovat skenery otisků prstů.

Otisk prstu je znakem, který byl zkoumán již od starověku (první zmínky lze nalézt ve textech ze starověké Asýrie). Moderní pojetí zkoumání otisků prstů ale položily až vědecké práce publikované v průběhu 19. století, jako např. Jana Evangelisty Purkyně, který se zabýval papilárních linií (nikoliv však možností jejich použití pro identifikaci člověka) nebo Josepha T. Jamese, který formoval některé základní postuláty daktyloskopie o neměnnosti otisků prstů v průběhu života a jejich unikátnosti, čímž byly položeny základy oboru, který označujeme názvem *daktyloskopie*.

Identifikace pomocí otisku prstu vychází ze zkoumání vzhledu papilárních linií. V rámci tohoto zkoumání jsou v otisku identifikovány markanty a jejich orientace a vzájemná poloha. Na otisku prstu člověka je možno obvykle identifikovat 8 - 17 takových markant. Pro účely identifikace člověka je pak vyžadována shoda s 10 - 15-ti znaky. Vzhledem k tomu, že pro autentizaci do systémů pracujeme s menšími vzorky populace není obvykle taková přesnost vyžadována. Na obr. 3.6 jsou znázorněny příklady nejčastěji použitých snímačů v mobilních telefonech a noteboocích (viz obr. 3.7).

Obrázek 3.7: Čtečka otisků prstů v notebooku Lenovo ThinkPad 430 (převzato z [15])

Problém relativně malého rozměru řeší zařízení různě, např. Touch ID Applu, při vytváření záznamu o otisku, opakovaně snímá různé části prstu tak, aby z nich postupně sestavilo pokud možno

(a) PalmSecure Mouse (převzato z [35] (b) Fujitsu Lifebook S935 (převzato z [10])

Obrázek 3.8: Snímače žilkování na dlani v zařízeních společnosti Fujitsu

úplný otisk prstu a bylo tak jedno kterou částí prstu se snímače dotknete. Snímač Lenova má výšku pouze několik milimetrů, předpokládá proto, že po senzoru přejedete pomalu prstem.

Vzhledem v velikosti senzoru, není vyhodnocení dokonalé, ale pro účely autentizace spolehlivost a rychlost vyhodnocení lze hodnotit jako dostatečnou.

Dlouhou dobu byl problémem s použitím těchto senzorů pro účely autentizace absence podpory ze strany operačního systému (především MS Windows). Pro použití proto bylo vyžadována instalace dodatečného software, který použití senzoru pro tento účel umožňují. Moderní operační systémy tento problém, ale poměrně efektivně řeší a také proto se čtečkami otisků prstů můžeme setkat ve velkém množství různých zařízení.

Jako alternativu k snímání otisku prstu je možnost **snímání žilkování na dlani**. Výhodou je, že žilkování na dlani je biometrickým údajem, který se během života nemění a žilkování je také rozdílné i pro jednovaječná dvojčata. Jedná se o metodu optickou, která snímá strukturu žilkování na dlani. Snímkování probíhá v infračerveném světle, protože okysličený hemoglobin v krvi pohlcuje infračervené záření, což umožňuje optické zvýraznění struktury žilkování.

Senzor samotný je relativně malý a je možné jej použít buď samostatně, nebo jako součást jiných zařízení jako např. myši nebo notebooku, viz obr. 3.8. Průkopníkem v nasazování tohoto typu řešení v praxi je společnost Fujitsu.

Oční duhovka poskytuje poměrně přesnou metodou identifikace člověka. V určitém smyslu pracuje podobně jako vyhodnocování otisků prstů. Snímání se provádí opticky. Na sejmutém obrázku oční duhovky se vyhledávají markanty a ty jsou pak srovnávány s uloženými záznamy. Oproti otisku prstu je obvykle možno v oční duhovce identifikovat okolo 200 markant. Tento biometrický údaj je proto pro identifikaci člověka spolehlivější než otisk prstu.

Způsob snímání i velikost celého zařízení v současnosti, ale není úplně příznivý pro účely autentizace k počítačovým systémům, viz obr. 3.9. Existují již ale implementace této technologie pro účely autentizace k použití mobilního telefonu. Tato technologie je podporována např. telefonem ARROWS NX F-04G společnosti Fujitsu, který byl do prodeje uvolněn v květnu 2015 [36]. Tento mobilní telefon je však dostupný pouze v Japonsku.

Ještě větší spolehlivost zaručuje použití **skenování oční sítnice**. Tento druh skenování snímá struktury cév na pozadí lidského oka. Běžně používané skenery jsou obdobného rozměru jako skenery oční duhovky. Podobně jako v předchozím případě existují komerční pokusy nasadit tuto technologii do širší praxe. Tento způsob autentizace podporuje např. mobilní telefon ZTE Grand SIII [31], který je však v současnosti komerčně dostupný pouze v Číně.

Z výše uvedeného vyplývá, že skenování oční duhovky a sítnice jsou vysoce progresivní technologie, kde vývoj v senzorech a algoritmech vyhodnocování nasnímaných údajů do budoucna umožní mnohem širší nasazení těchto velmi bezpečných autentizačních mechanismů, než jak je tomu v současnosti.

Poslední otázkou, kterou zbývá zodpovědět, je spolehlivost jednotlivých metod. V případě autentizace vlastností se obvykle řeší dva typy problémů: 1) odmítnutí oprávněného uživatele a 2) přijetí

Obrázek 3.9: Kontrola identity členů městské rady Bagdádu pomocí skenu oční duhovky (převzato z [44])

neoprávněného uživatele. První problém nepředstavuje bezpečnostní riziko. Odmítnutí je obvykle způsobeno chybným sejmutím údaje a je možné jej jednoduše opravit opětovným sejmutím sledovaného údaje. Druhý problém je mnohem závažnější, protože umožní využít systém osobě, které měla být odmítnuta - což je bezpečnostní problém. Zároveň tento problém není jednoduše odstranitelný, je totiž záležitostí použitého senzoru a vyhodnocovacího algoritmu.

Z výše uvedených údajů lze odvodit několik metrik pro hodnocení kvality [41]:

- Míra správného přijetí (True Acceptance Rate (TAR)) / Míra správného ztotožnění (True Match Rate (TMR)) - poměr reprezentuje schopnost biometrického systému správně identifikovat oprávněného uživatele (výrobci zařízení se snaží maximalizovat)
- Míra chybného přijetí (False Acceptance Rate (FAR)) / Míra chybného ztotožnění (False Match Rate (FMR)) - reprezentuje frekvenci s jakou se chybně sejmuté údaje v systému ztotožní s některým z existujících oprávněných uživatelů (výrobci zařízení se snaží minimalizovat)
- Míra správného odmítnutí (True Rejection Rate (TRR)) / Míra správného neztotožnění (True Non-Match Rate (TNMR)) - reprezentuje frekvenci případů, kdy biometrické údaje není možné ztotožnit se uloženými záznamy, jelikož daná osoba není evidována (výrobci se snaží maximalizovat)
- Míra chybného odmítnutí (False Rejection Rate (FRR)) / Míra nesprávného neztotožnění (False Non-Match Rate (FNMR)) - reprezentuje frekvenci případů, kdy sejmuté biometrické údaje nebyly ztotožněny se záznamem o osobě v databázi, přestože se tak správně mělo stát (výrobci se snaží minimalizovat)

Pokud jednotlivé míry vyjádříme procentem, můžeme velmi jednoduše popsat vztah mezi sledovanými souvisejícími veličinami, rovnice (3.3 - 3.6).

$$TAR + FAR = 100\% \tag{3.3}$$

$$TMR + FMR = 100\% \tag{3.4}$$

$$TRR + FRR = 100\% \tag{3.5}$$

$$TNMR + FNMR = 100\% \tag{3.6}$$

Pro hodnocení řešení jednotlivých výrobců je potřeba použít výsledky benchmarků nezávislých hodnotících laboratoří jako je např. projekt Fingerprint Verification Competition (FVC)-onGoing [11], který v polovině roku 2015 zveřejnil více než 150 benchmarků pro více než 4 000 algoritmů vyhodnocování otisků prstů. Pro ostatní biometrické metody autentizace je ale nezávislé hodnocení poměrně obtížně dohledatelné. Uvádějí se pouze orientační údaje ukazující spíše potenciál jednotlivých metod než skutečnou chybovost:

- otisk prstu 1:500
- oční duhovka 1:100 000
- oční sítnice 1:10 000 000

3.2 Identity management

Identity Management System (IDM) je systém udržující veškeré informace o uživatelích na jednom místě. Účelem je sjednotit proces autentizace pro různé služby napříč systémy. IDM obvykle implementují větší organizace, které provozují vetší množství systémů.

Pro menší organizace může být výhodnější tuto problematiku neřešit a ponechat autentizaci na jednotlivých provozovaných systémech. V praxi to znamená, že uživatelé mají řadu samostatných účtů pro různé služby v rámci jedné organizace. Zkušenosti větších organizací ale ukazují, že čím větší množství uživatelských účtů každý uživatel má, tím větší šance je, že buďto zapomene heslo (což vyžaduje zásah administrátora), použije slabé heslo, které se dobře pamatuje (což vede ke zvýšení možnosti průniku do systému útočníkem). Sjednocení autentizace pomocí IDM tento problém poměrně elegantně řeší.

V souvislosti s IDM se velmi často používají další pojmy a zkratky, u kterých se na chvíli zastavíme. První dvě technologie se zabývají uchováváním informací o uživatelských účtech, jedná se o Active Directory (AD) a Lightweight Directory Access Protocol (LDAP). Co přesně to znamená, zejména s tím, že i o IDM jsme si řekli, že uchovává informace o uživatelích.

Problém je v tom, jak přesně chceme IDM použít. Jedná se o jediný systém, vůči kterému probíhá autentizace, nebo IDM slouží spíše jako synchronizační nástroj, který umožňuje informace o uživatelských účtech přenášet (synchronizovat) mezi jednotlivými autentizačními systémy? Pokud vnímáme IDM prvním způsobem, můžeme říci, že technologie jako je AD a LDAP jsou IDM. Pokud ho vnímáme spíše druhým způsobem, pak LDAP a AD jsou spíše klienty IDM. Co tedy přesně dělá IDM a proč vůbec takto komplikovaně k problematice řízení uživatelských účtů přistupovat?

Úkoly IDM v obecné rovině jsou následující:

1. poskytuje služby autentizace, popřípadě autorizace pro další systémy
2. podporuje role, jako normalizované skupiny činností, které uživatel může v systému provádět
3. delegování - práva k úpravám jsou delegována na lokálního administrátora služby využívající IDM (případné změny nemusí provádět globální administrátor IDM)
4. výměna dat mezi systémy - údaje o uživatelských účtech jsou synchronizovány napříč systémy připojenými k IDM.

LDAP vznikl v 70. letech minulého století jako nezávislý standard. Jedná se o aplikační protokol pro přístup a údržbu k distribuovaným informačním službám o adresářích. Základní funkcí LDAP je tedy vytváření objektů jako jsou uživatelé, úložný prostor na síti a práce s nimi. Prostřednictvím LDAP je proto možno sdružovat jednotlivé uživatele do skupiny a těmto skupinám přidělovat práva k systémům na síti.

LDAP se rychle rozšířil a byl implementován řadou různých výrobců síťových zařízení i operačních systémů. LDAP má však také jeden poměrně zásadní problém a tím jsou velké rozdíly v implementacích LDAP různých implementátorů standardu. Důvodem pro tyto rozdíly je fakt, že standard neřeší přesně způsob, jak má taková implementace přesně vypadat. Neřeší způsob jakým mají být ukládána data o objektech - mají být v nějaké databázi, nebo stačí textový soubor?

LDAP také neřeší širší problémy správy počítačových sítí v rozsáhlejších sítích. To je důvod, proč Microsoft účely správy uživatelských účtů vytvořil vlastní, zpětně nekompatibilní implementaci LDAP a nazval ji Active Directory (AD). AD oproti LDAP umožňuje navíc také objekty typu počítač, jejich

sdružování do skupin a především aplikaci *systémových politik* stanovujících, jak tyto počítače mají být nastaveny.

Právě politiky jsou tím nástrojem, pro který řada firem AD zvolila. Politiky je možno aplikovat pouze na počítače, které je připojeny do AD a mají nainstalovaný operační systém Windows. Systémové politiky se aplikují v okamžiku přihlášení uživatele na počítači do AD.

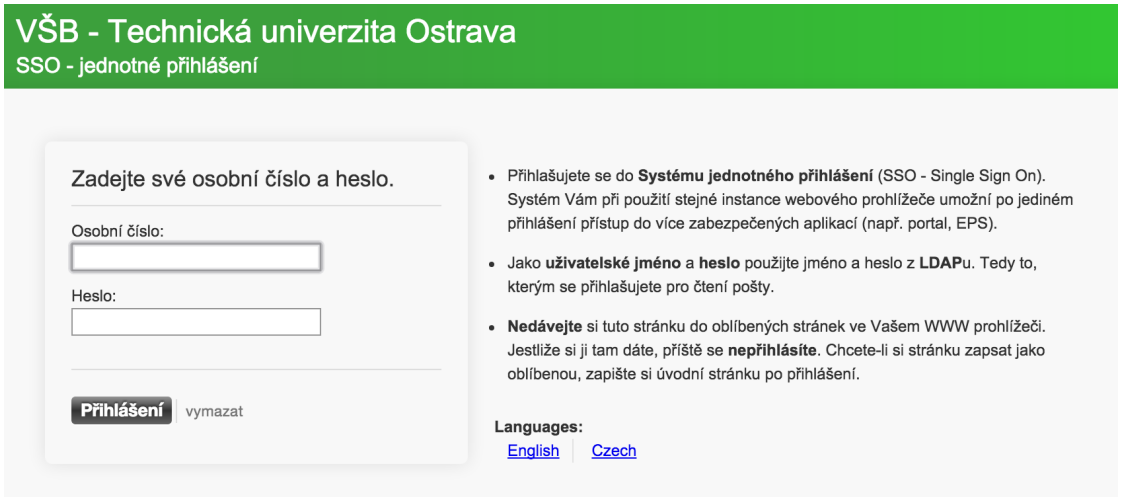
Tímto způsobem je možno efektivně spravovat v podstatě neomezené množství počítačů. Administrátoři se pak mohou zaměřit na řešení skutečných problémů (odpadá velké množství rutinní práce s nastavováním pracovních stanic). Systémové politiky jsou také základním nástrojem pro zajištění souladu nastavení počítačů s požadavky bezpečnostních politik.

Takže si to shrňme - máme tedy starší LDAP a mladší a v mnoha ohledech pokročilejší AD. Řada organizací proto v minulosti implementovala LDAP a později pak také AD, tím ale vznikla situace, kde v rámci jedné firmy fungují dva nezávislé systémy sloužící pro autentizaci uživatelů. Na oba systémy se pak obvykle navazují další služby a systémy (minimálně z pohledu autentizace), takže není možné jeden z nich jednoduše odstavit. Právě v takových situacích je vhodné nasazení IDM.

Druhým momentem hovořícím pro nasazením IDM je fakt, že AD ani LDAP nepodporují role. Role, ale mohou výrazným způsobem zefektivnit správu systémů, zejména z pohledu nastavování práv k systému.

Souvisejícím pojmem je Single-Sign On (SSO). Jedná se o prostředek, který společnosti používají, aby pod různými systémy probíhalo přihlašování vůči jednotnému IDM. SSO se extenzivně využívá především pro webové aplikace. Funguje to tak, že při pokynu pro přihlášení systém otevře formulář pro přihlášení SSO, ten autentizuje uživatele vůči IDM a pošle informaci o výsledku původnímu systému.

Tento způsob autentizace je bezpečný, pokud síťová komunikace probíhá šifrovaně (obvykle pomocí HTTPS), Příklad SSO pro webové aplikace na VŠB-TU Ostrava je na obr. 3.10.



Obrázek 3.10: SSO pro webové aplikace na VŠB-TU Ostrava

Shrnutí

Autentizací se rozumí prokázání identity uživatele systému. Autentizace je možná znalostí (např. uživatelské jméno a heslo), vlastnictvím (např. čipová karta) a vlastností (např. otisk prstu). Pro zvýšení bezpečnosti je možno metody autentizace kombinovat (multifaktorová autentizace).

Některé činnosti v systémech jsou natolik závažné, že pouhá autentizace nepostačuje - v takovém případě může systém požadovat autorizaci takové činnosti. Autorizace funguje jako bezpečnostní nadstavba pro autentizované uživatele a obvykle využívá jinou metodu než byla použita pro autentizaci. Příkladem autorizace je potvrzení platby v elektronickém bankovnictví zadáním kódu zaslaného bankou pomocí SMS na mobilní telefon.

Informace o uživatelských účtech jsou ukládány obvykle centralizovaně v systémech LDAP nebo AD popř. v systému, který sjednocuje přihlašování napříč různými systémy používanými v organizaci. Takovým systémům obecně říkáme IDM. Úkolem IDM je evodivat na jednom místě uživatele, informace o nich a role, které v jednotlivých systémech zastávají.

Kontrolní otázky

1. Co je multifaktorová autentizace?
2. Seřaďte různé metody autentizace vlastností podle spolehlivosti od nejspolehlivějšího: otisk prstu, žilkování na dlani, obraz duhovky, obraz očního pozadí.
3. Co je to role v systému IDM?
4. Co je politika v AD?

Odpovědi

1. Autentizace využívající více než jeden typ autentizačního mechanismu.
2. žilkování na dlani, oční pozadí, obraz duhovky, otisk prstu
3. Soubor pravidel (popř. politik) vztahující se k určité typu prováděných činností v systému.
4. Nastavení spojená s uživatelskými účty nebo počítači v AD, která se aplikují při přihlášení do systému.

Kapitola 4

Ochrana dat

Náhled kapitoly
Organizace, ale také jednotlivci zpracovávají velké množství údajů různého charakteru a zároveň jsou data obvykle to nejcennější, co organizace vlastní a proto je potřeba je efektivně chránit. Hardware je možno koupit, software přeinstalovat, ale data, pokud o ně přijdeme, nahradit je jednoduše není možné. V této kapitole se proto zaměříme na možnosti jak postupovat v jejich ochraně.

Po přečtení kapitoly budete
Vědět

1. jak funguje zálohování
2. jak funguje a k čemu se používá klonování disků
3. jaký je účel RAID a jaké jsou mezi nimi rozdíly

Čas pro studium
Pro prostudování této kapitoly budete potřebovat přibližně 2 hodiny.

Jelikož data není možné v případě ztráty data jednoduše nahradit, je nutné ztrátě dat pokud možno zabránit. Nabízejí se tři způsoby ochrany:

1. zálohování
2. klonování disků
3. RAID pole

4.1 Zálohování

Základní metodou ochrany dat je jejich **zálohování**. Zálohováním rozumíme proces, v rámci kterého kopírujeme zálohovaná data z místa jejich běžného užití do místa odlišného. Při úvahách o způsobu zálohování je nutno rozhodnout:

- co zálohovat
- kam zálohovat (volba média)
- jak často zálohovat
- jak budou zálohy chráněny
- jak bude realizována obnova dat ze zálohy

Odpovědi na výše uvedené otázky tvoří tzv. *zálohovací strategii* zálohovaného systému.

4.1.1 Kam zálohovat

Identifikace dat k zálohování je prvním krokem ke stanovení zálohovací strategie. Množství dat, ve smyslu velikosti, může výrazně omezit výběr média. Pokud je objem dat opravdu velký odpadá v zálohování řada možností. Menší objemy dat je ale možno zálohovat na mnoho různých médií. Zkusme projít různá média a popsat jejich výhody popř. nevýhody.

Z přenosných médiích se nabízí zálohování na optické Compact Disc (CD) (700 MB), Digital Versatile Disc (DVD) (1 vrstva 4,7 GB, DL 8,5 GB), Blu-ray Disc (BD) (BD-R 1 vrstva 25 GB, 2 vrstvy 50 GB, BD-XL 3 vrstvy 100 GB). CD je zde uvedeno spíše pro úplnost, v praxi se pro zálohování na optická média používá spíše DVD nebo BD, přičemž mechaniky podporující třívrstvé BD-XL se prodávají více méně pouze v Japonsku.

O zálohování na optická média lze říci, že se jedná o proces relativně pomalý. Pro porovnání je v tab. 4.1 základní rychlost zápisu na média a maximální dosažitelný rychlost zápisu v době vzniku těchto skript.

Tabulka 4.1: Rychlost zápisu na optická média (převzato z [29])

médium	1x [Mbit/s]	max. rychlost	max. rychlost [Mbit/s]
CD	1,229	52x	63,91
DVD	11,08	16x	177,28
BD-R	36	12x	432

V tab. 4.1 uvedené rychlosti je potřeba brát jako orientační. Aktuální rychlost vypalování je determinována použitým vypalovacím zařízením, médiem (a rychlostí zápisu, kterou podporuje) a také schopnosti dostatečně rychle číst zálohována data z původního umístění. Např. udržení uvedené rychlosti BD-R při zálohování po síti vyžaduje minimálně gigabitový ethernet. Řada organizací přitom má realizován pouze 100 Mbit ethernet nebo používá bezdrátovou síť, kde dosahování takových rychlostí není prakticky možné.

Druhou otázkou spojenou s optickými médii je jejich životnost - jak dlouho po vypálení budou data na disku čitelná? To je poměrně složitá otázka, pro její zodpovězení se podrobněji podívejme na strukturu DVD-R média, viz obr. 4.1.

Obrázek 4.1: Struktura DVD-R média (převzato z [9])

Všimněte si na obr. 4.1 kovové AZO vrstvy, na kterou probíhá samotný zápis. Všechny ostatní vrstvy mají zajistit ochranu proti nežádoucím vlivům. Problém je v tom, že kov je pouze jednou ze tří možností, kterou lze pro tuto vrstvu použít:

- lisovaný hliník
- organické barvivo
- fázi měnící film

Ne kovové vrstvy jsou náchylnější k poškození vlivem změn teplot, ale slunečním svitem (UV zářením) apod. Za ideálních podmínek skladování může DVD vydržet v použitelné podobě až 100 let. V praktických podmínkách bude ale životnost pravděpodobně výrazně nižší zejména vlivem povrchového poškrábání povrchu disku a změnách na vrstvě nesoucí záznam vlivem stárnutí a působení vnějšího prostředí.

Pro účely dlouhodobého zálohování obzvláště cenných dat existují speciální média jako je Data Trescor Disc [8], kde výrobce díky použití speciální kovové vrstvy uchovávající data předpokládá životnost 160 let, za ideálních podmínek. Za delší životnost média si uživatel samozřejmě připlatí.

Výhodou záloh na optické disky je jejich malý rozměr a relativně dlouhá životnost, což umožňuje takto vytvořené zálohy dlouhodobě archivovat. Zálohování na bázi magnetického pole (běžné HDD, pásky apod.) přitom postupem času se pomalu demagnetizují, čímž může dojít k postupné ztrátě dat. Tato přirozená demagnetizace je ale velmi pomalá (přibližně 20 let).

Po uběhnutí tak dlouhé doby ale může být vůbec problém nalézt počítač, ke kterému by bylo možné takový disk připojit. Pokud se zaměříme na na pevné disky (Hard Disc Drive (HDD)) používající magnetický zápis, jako hlavní typ média, na které se provádějí zálohy velkého objemu dat. Zálohovat lze na HDD připojený pomocí USB, přítomný „napevno“ v počítači nebo přítomném někde síti podniku.

Použití externího disku pro zálohy se hodí pro běžného domácího uživatele. Moderní operační systémy obvykle obsahují vestavěné nástroje, které takové zálohování dobře podporují. Windows podporují tento typ zálohování od verze 8 pomocí nástroje Historie souborů a Apple v OS X využívá nástroj Time Machine. Výhodou použití externího disku je možnost fyzického odpojení disku od počítače. Záloha tak může zůstav v bezpečí i pokud počítač jako celek zasáhne nějaká neblahá událost jako je přepětí v síti, selhání zdroje apod.

Zálohování na stejný disk nebo na jiný disk ve stejném počítači může chránit proti chybám oprávněného uživatele, např. nežádoucí smazání nebo změna souboru. V případě, že je bezpečnost počítače kompromitována zvenčí, pak útočník kromě ostrých dat získává taktéž přístup k zálohám. Záloha na jiný disk v rámci jednoho počítače ale může ochránit data proti hardwarovému selhání jednoho z disků. Podobně jako v předchozím případě nejsme zálohou chráněni proti selhání počítače jako celku.

Rychlost zálohování je v tomto případě limitována rychlostí čtení dat na zdrojovém disku, zápisu na cílovém disku a použitého rozhraní pro připojení disku.

V případě, že místo, na které probíhá zálohování je přítomno na síti, např. formou NAS, limitující je především přenosová kapacita sítě., pokud není v síti zaveden 10 Gbitový ethernet. 10 Gbit/s je již rychlost, kdy pro přenosy na síti začíná být limitující rychlost čtení a zápisu na použitých discích.

Do budoucna se dá předpokládat, že svou cenou a kapacitou vyrovnají a následně také předeženou HDD disky Solid State Disc (SSD). Tyto disky netrpí některými neduhy HDD, mají ale životnost omezenou počtem zápisů. O proti běžným HDD hůře snáší vysoké provozní teploty a také se u nich obtížněji detekuje blížící se hardwarové selhání. O selhávání disků a možnosti jejich včasné detekce budeme podrobněji hovořit u diskových polí.

Magnetický zápis používají také páskové mechaniky s kazetami, na které se zálohuje. Záloha probíhá rychlostí přibližně 1 TB/hod. Svými vlastnostmi (kapacitou, cenou a rychlostí) jsou páskové mechaniky určeny pro vysoko objemové zálohování především serverů a diskových polí, tedy centralizovaným zálohám.

Posledním místem, kam lze zálohovat je *cloud*. Zálohování tedy probíhá do vzdálené sítě ve vlastnictví jiné společnosti. Zálohování lze řešit vlastními silami - pronajmutím prostoru v některém z dostupných datových center a nainstalovat tam vlastní systém pro zálohování. Běžní uživatelé zvolí spíše připravené zálohování poskytované některou ze specializovaných firem jako je CrashPlan [16], Backblaze [3] nebo Carbonite [4].

Při použití cloudových služeb je potřeba počítat s tím, že limitujícím je v tomto případě přenosová kapacita připojení k internetu. Při použití připojení typu DSL (např. VDSL) pak rychlost downloadu a uploadu není stejná - rychlost uploadu je řádově nižší (rychlost downloadu je až 10x vyšší). Střední a větší firmy se také proto připojují jinými technologiemi, která podobná omezení nemají.

Při provádění zálohy do cloudu (zejména té první) je proto potřeba počítat s poměrně dlouhou dobou, kterou provedení zálohy může zabrat. Další zálohy jsou již pouze rozdílové a jejich nahrání na cloud je proto podstatně rychlejší. Proces obnovy je limitován pouze rychlostí downloadu.

Zálohování do cloudu má své výhody - záloha je realizována obvykle v nějakém datovém centru, kde provozovatel centra může efektivně řešit ochranu provozovaných IT aktiv centra. Záloha je realizována ve vzdálené lokaci a proto je odolná vůči poškození/změnách např. v důsledku kompromitace vnitřní sítě organizace, popř. následkům mimořádných událostí lokalizovaných do objektů organizace.

Zálohování do cloudu má ale také své nevýhody. Zálohovaná data svěřujeme do rukou další firmy, která může, ale také nemusí být solidní. Je vyžadováno rychlé připojení k Internetu. V podmínkách České republiky bohužel stále v některých místech rychlé připojení k Internetu není dostupné buďto vůbec, nebo je dostupné, ale pouze v nepříznivých cenových relacích.

4.1.2 Náročnost záloh

Podle objemu dat, které je potřeba chránit je možno odhadnout čas nutný pro realizaci zálohy. Při velkých objemech dat se proto často vyplatí uvažovat o způsobu, jak proces zálohy zefektivnit. Z tohoto pohledu rozlišujeme dva typy záloh:

- úplná záloha
- inkrementální záloha

Úplnou zálohou se rozumí záloha obsahující veškeré chráněné údaje. Obnova ze zálohy je v takovém případě přímočará - obnovovaná data pouze „tečou“ opačným směrem. Nevýhodou takové zálohy je doba, kterou její provedení vyžaduje.

Alternativou k úplné záloze je provedení *záloh inkrementálních*. Technicky přesnější by bylo provedení kombinace úplných a inkrementálních záloh. Prakticky to znamená, v rámci volby zálohovací strategie volíme časové intervaly v rámci kterých budou chráněná data zálohována a specifikujeme, které z těchto záloh mají být úplné a které inkrementální.

Inkrementální (rozdílovou) zálohou rozumíme zálohu, která obsahuje pouze taková data, která se od provedení poslední zálohy změnila. Identifikaci změněných souborů je přitom možné udělat efektivně na úrovni operačního systému vyhodnocením metaúdaje *čas modifikace* připojeného k jednotlivým souborů v rámci souborového systému. Takový atribut je podporován všemi moderními operačními systémy.

Počet takto změněných souborů je obvykle velmi malý, proto provedení rozdílové zálohy trvá zlomek času a zabere zlomek místa ve srovnání se zálohou úplnou.

Obnova ze zálohy je však komplikovanější. Obnova se nejprve provede z poslední úplné zálohy a následně se na ni aplikují změny obsažené v jednotlivých inkrementálních zálohách. Proces obnovy je proto složitější.

Podle citlivosti údajů a frekvence jejich změn volíme frekvenci záloh. Pro některá data tak může být vhodné provádět např. v neděli úplnou zálohu (den pracovního klidu, dostupné zdroje pro zálohování) a v pracovní dny a sobotu lze volit rozdílovou zálohu, např. v nočních hodinách. Pro kritické systémy ale může být žádoucí provádět zálohy v hodinových intervalech.

Z otázek, které zohledňujeme v rámci přípravy zálohovací strategie je velmi důležitá otázka ochrany - je potřeba zálohu chránit, proti neoprávněné manipulaci nebo přečtení? Pokud ano, je možno poměrně jednoduše nasadit některé z existujících šifrovacích schémat. Existenci šifrování je nutné zohlednit při úvahách o případné obnově - budu mít v okamžiku obnovy k dispozici klíč, pomocí, kterého šifrované zálohy budu schopen dešifrovat?

Prostě není nad to zjistit v okamžiku, kdy potřebujete data ze zálohy, že je nemůžete použít, protože jediné místo, kde byly uloženy klíče byl počítač, který byl zálohován a který hardwarově odešel, což je důvod, proč jste chtěli provést obnovu ze zálohy.

V případě, že je záloha má sloužit jako „archivní“ záloha. Tedy záloha se zaarchivuje pro případ, že by ji bylo někdy v budoucnu potřeba, ačkoliv se to v blízké budoucnosti neočekává. Nabízí se související otázka - jak provedu v budoucnu obnovu. Dá se předpokládat, že do budoucna se bude použitý hardware i software měnit. Bude možné na něj ze zálohy obnovit, nebo bude vyžadován specifický hardware, operační systém, nebo program?

Zálohování představuje proto poměrně komplexní problém, kterému se vyplatí věnovat zvýšenou pozornost. Toto úsilí se má totiž tendenci vrátit právě v okamžiku, kdy to nejvíce oceníte!

4.2 Klonování disků

Možná jste v předchozí podkapitole zaznamenali, že v souvislosti se zálohami se objevoval opakovaně pojem data. Toto významný moment, protože data jsou údaje fungující v podstatě nezávisle na umístění. Proti tomu programy nebo dokonce celý operační systém není často možné jednoduše přenášet pouhou kopií do nového umístění.

To je důvod, proč pro ochranu instalace operačního systému a nainstalovaných programu volíme odlišný nástroj - volíme vytvoření tzv. *obrazu disku* pomocí nástroje pro klonování disků. Tyto fungují tak, že provedou kopii disku (přesněji řečeno diskového oddílu (disk partition)). V obrazu disku je obsažen nejen obsah samotných souborů, ale také jejich pozice na disku, což je informace potřebná pro některé počítače, např. ty s operačním systémem Microsoft Windows. Operační systémy jako je např. OS X společnosti Apple podobné požadavky nemají.

Vytvoření obrazu disku je výhodné tím, že je zaručena planá funkčnost obnovovaného systému ihned po dokončení rozbalení obrazu na disku. Reinstalace počítače zabere přitom minimálně několik hodin a může se v některých případech protáhnout i na několik dní.

Z hlediska technické realizace je výhodné, aby „datová“ část a „programová“ část byla byla oddělena. Jinými slovy jde o to, aby programy a data byly na odlišných oddílech disku nebo odlišných discích. To odpovídá konfiguraci menší, rychlé SSD pro operační systém a programy a pomalejší, spolehlivější pevný disk s větším dostupným prostorem pro data.

Programová část se příliš nemění - image disku se tak vyplatí provádět v okamžiku provádění velkých změn v konfiguraci systému, jako je přechod na odlišnou verzi operačního systému nebo provedení významných změn v konfiguraci počítače, u které je očekávána možnost vzniku problémů. Data proti tomu je možné (a žádoucí) zálohovat častěji.

Obraz disku je možno připravit buďto pomocí vestavěného nástroje operačního systému nebo s použitím specializovaných programů. Výhodou použití specializovaných programů je obvykle lépe řešený proces obnovy. Specializované nástroje mohou obsahovat i další pokročilou funkčnost, jejíž využití je výhodné v rozsáhlejších sítích.

Z programů vhodných pro domácí užití je možné zmínit:

- Paragon Backup and Recovery 2015 [18] - dostupné pro osobní použití zdarma
- Acronis TrueImage 2016 [1]

Z programů vhodný pro nasazení v rozsáhlejších sítích je možno zmínit:

- Symantec Norton Ghost [46]
- Clonezilla [7] - open source nástroj pro klonování disků

Rozdíl mezi programy pro použití v domácnostech (a menších společnostech) proti těm, které jsou určeny středním a velkým firmám je kromě ceny také funkčnost zaměřená na efektivní správu velkého množství obrazů. Za normálních okolností každý obraz tvoří samostatný soubor. Pokročilejší programy pro zálohování a správu diskových obrazů, ale umožňuje tyto obrazy analyzovat a udržovat informace o opakujících se souborech na jednom místě, čímž se efektivně minimalizuje prostor, který takový obraz zabírá.

Opakujícími se programy může být operační systém, kancelářské produkty apod. Úspora může na jednom obrazu disku tvořit desítky, v některých případech i stovky GB.

Produkty určené do větších sítích často umožňují také hromadné nasazování obrazů na stroje. Hromadné nasazování se výhodné v okamžiku kdy máme velké množství počítačů s totožnou hardwarovou i softwarovou konfigurací. Nasazení probíhá automatizovaně, po síti hromadným broadcastem dat obrazu. Nasazení nové konfigurace je pak otázkou práce jednoho administrátora a několika minut práce.

Aby hromadné nasazení fungovalo s maximální efektivitou, musí organizace:

1. implementovat serverovou i klientskou část řešení
2. zajistit pro ukládané obrazy dostatečně velký prostor
3. získat kontrolu nad pořizováním výpočetní techniky s cílem omezit počet různých podporovaných konfigurací PC a notebooků v dané organizaci

Získání kontroly na pořizováním a nasazováním prostředků výpočetní techniky je přitom přínosné samo o sobě a výrazným způsobem může zjednodušit podporu takových zařízení v průběhu jejich „života“ v organizaci.

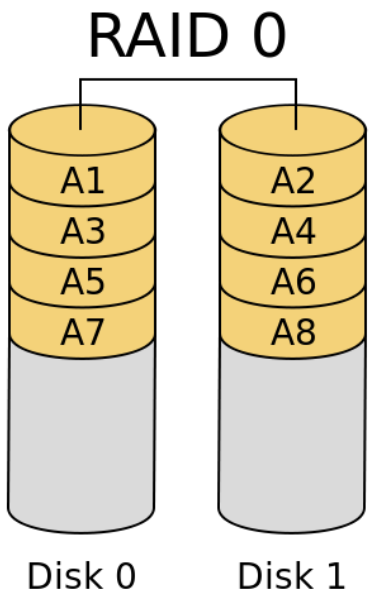
4.3 RAID

Posledním tématem, kterému se budeme v této kapitole věnovat je problematika Redundant Array of Independent Discs (RAID) - tedy problematika redundantních polí nezávislých disků. RAID umožňuje propojovat prostor dostupný na různých discích do jediného celku, způsobem, který činí výsledné pole odolné vůči selhání disku.

Aby bylo možné dosáhnout takové odolnosti není veškerá kapacita použitých disků použita pro samotná data, jak jsme tomu zvyklí při použití běžných disků, část kapacity je alokována pro tzv. *paritní informaci*. Právě paritní představuje redundanci (nadbytečnost) v RAID. Tento druh informací je možno následně použít pro rekonstrukci údajů z disku, který selhal.

Existují různé druhy RAID, které pracují s paritní informací různým způsobem, my se v rámci výkladu zaměříme na ty nejpoužívanější - RAID-0, RAID-1, RAID-5, RAID-6. Používané jsou také některé kombinace, jako např. kombinace RAID-0 a RAID-1 označované jako RAID-10.

RAID-0 je v rámci diskových polí poměrně specifickým druhem pole a to tím, že neobsahuje redundanci. RAID-0 pracuje tak, že spojí jednotlivé disky do jednoho celku. Hlavní výhodou je opticky velká kapacita takto vytvořeného pole a také vyšší rychlost čtení i zápisu. Proč tomu tak je, lze odvodit z grafického pohledu na organizaci dat v poli, viz obr. 4.2.



Obrázek 4.2: RAID-0 se dvěma disky tvořící jeden logický disk (převzato z [19])

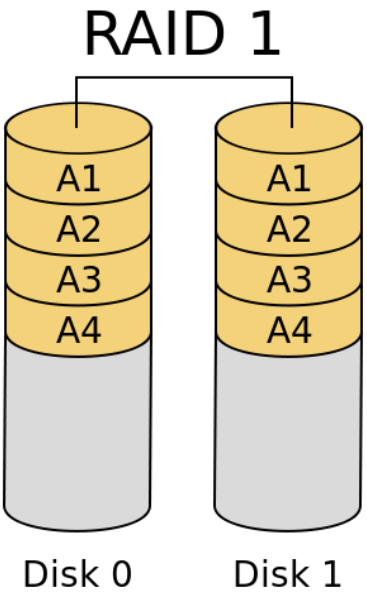
Jednotlivé soubory jsou rozdělovány do bloků a ty zapisovány postupně na jednotlivé disky „na přeskáčku“. Prakticky to znamená, že čtení i zápis mohou najednou pracovat se všemi disky zapojenými do pole. Tímto způsobem se minimalizuje význam některých úzkých hrdel v systému, zejména rychlosti jednotlivých disků.

Absence paritní informace má ale některé nepříjemné dopady. V případě, že některý disk selže, pole jako celek přestane pracovat. Z tohoto stavu se pak pole není schopno samo zotavit. Obnova dat proto musí proběhnout z externích záloh.

RAID-1 je opačným extrémem - pracuje tedy s plným zrcadlením. Tento druh pole se používá často pro systémové disky (disky na kterých je instalován operační systém). Plné zrcadlení znamená, že obsah jednoho disku je přesně zkopírován (přesněji řečeno replikován) na disk druhý, viz obr. 4.3. Více než dva disky se obvykle do tohoto pole nezapojují - přece jenom celá polovina diskové kapacity je „ztracena“ - použita pro paritní informaci.

Pozitivním na použití RAID-1 je to, že v případě selhání jednoho z disků se v podstatě nic neděje - systém pracuje dál, protože má pořád k dispozici úplná data z disku funkčního. Po výměně vadného disku se z disku funkčního replikují replikují data.

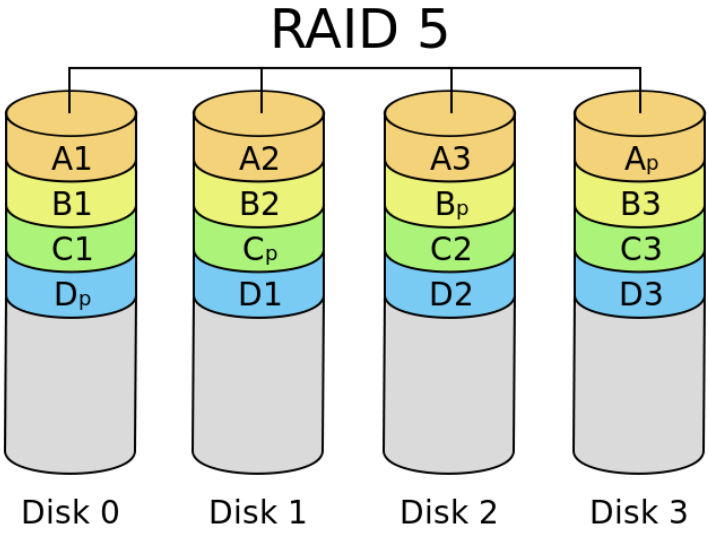
RAID-10 propojuje vlastnosti RAID-1 a RAID-0, prakticky to funguje jako RAID-1 pole složené ze dvou RAID-0 polí. Zrcadlí se tedy RAID-0 pole, které jak víme neobsahují žádnou paritní informaci.



Obrázek 4.3: RAID-1 se dvěma disky tvořící jeden logický disk (převzato z [20])

Tento druh pole se používá všude tam, kde je kritická rychlost výsledného pole a jsou kladeny vysoké nároky na bezpečnost.

Z praktického hlediska se používá spíše pole RAID-5. To je pomalejší než RAID-10, ale zato tak neplýtvá místem. Práci s paritní informací nejlépe demonstrujeme graficky, viz obr. 4.4.

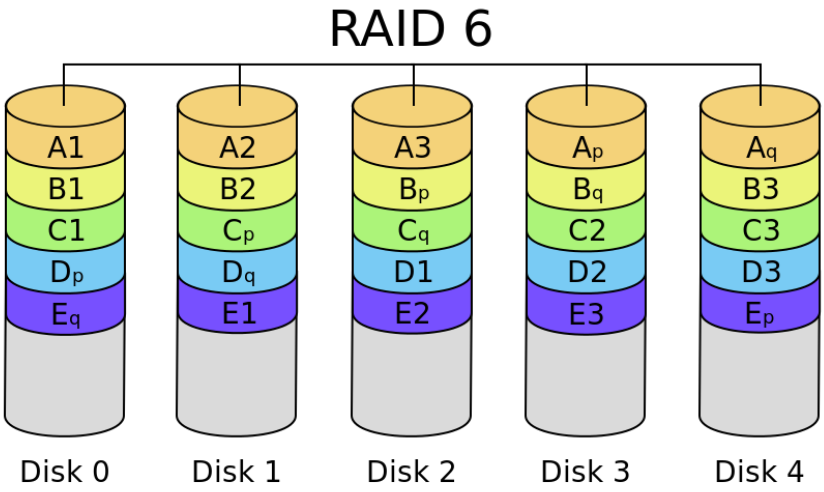


Obrázek 4.4: RAID-5 se čtyřmi disky tvořící jeden logický disk (převzato z [21])

Paritní informace je v tomto případě distribuována, tedy nenachází se na jednom disku. Paritní informace na obr. 4.4 představují bloky dat A_p, B_p, C_p a D_p. Za předpokladu, že disky tvořící pole jsou stejné, pak paritní informace v poli zabere kapacitu jednoho disku v poli.

Z bloků dat se počítá paritní informace a zapisuje se na disky. V případě selhání disku pak pole přestane fungovat, ve smyslu, že není možné jej standardním způsobem využívat jako před selháním disku, dokud se poškozený disk nevymění a pole se automaticky nezotaví. Chybějící paritní informace na vyměněném disku se dopočtou z data na ostatních discích, chybějící datové bloky na vyměněném disku se dopočtou z paritní informace a zbývajících datových bloků na ostatních discích. Délka procesu zotavování je přímo úměrná množství dat uložených v poli a tedy také počtu použitých disků.

Pokud je vyžadována odolnost proti selhání více než jednoho disku, je možné použít RAID-6, který funguje podobně jako RAID-5 ovšem s tím, že počítány jsou dvě distribuované parity (obě různým způsobem).



Obrázek 4.5: RAID-6 se pěti disky tvořící jeden logický disk (převzato z [**?**])

Dvě vypočítané parity znamenají, že celkově kapacita dvou disků je využita pro paritu. Pole je tak odolné proti selhání dvou disků. Při ztrátě jednoho nebo dvou disků pole přestává pracovat běžným způsobem a čeká na výměnu disků a následně se pole automatizovaně zotaví a normálně pokračuje v poskytování služeb.

Výše uvedený popis procesu zotavení zní poměrně jednoduše a po technické stránce také je, je ovšem potřeba si uvědomit, že proces zotavení i na „malém“ několika terabajtovém poli může trvat hodiny, pro pole velká může trvat i dny. Navíc úplné zotavení nemusí být možné. Tato situace nastane v případě, že zbývající paritní informace nebo datové bloky jsou poškozené. Zotavení pole může být tedy možné, ale nemusí být bezztrátové. Tedy nasazení diskového pole nás nezbavuje nutnosti zálohovat.

Celkově vzato je lepší se hardwarovému selhání disku vyhnout. Technologie nám umožňují, aby v některých případech takové vyhnutí se problémům bylo možné. Většina moderních HDD má implementován Self-Monitoring, Analysis, and Reporting Technology (S.M.A.R.T.). S.M.A.R.T. monitoruje chyby v zápisu na disk a různé další operační parametry signalizující zdraví HDD. Operační systém pak může S.M.A.R.T. informace zpracovávat a v případě, že se začnou hromadit na discích chyby, což signalizuje blížící se selhání disku, upozornit administrátora např. e-mailem. Včasná výměna disku má minimalizuje případné problémy se zotavením.

Shrnutí

Základním nástrojem ochrany dat je jejich zálohování. *Zálohováním* rozumíme proces v rámci kterého kopírujeme data z místa jejich běžného použití na bezpečné místo, obvykle na jiném počítači nebo médiu, než se běžně nachází. Pro efektivní ochranu dat specifikujeme zálohovací strategii, která nám říká, která data, jak často, v jaké formě a kam budou zálohována.

Chránit lze také přímo celé instalace operačního systému a programů na něm nainstalovaných. Tuto ochranu lze realizovat pomocí metody zvané *klonování disků*. Klonováním disku se udělá obraz disku obsahující nejen chráněné soubory, ale také informace o jejich poloze na disku. Právě tato dodatečná informace umožňuje přenášet operační systémy jako je např. Windows, které by na novém místě při použití běžného kopírování souborů nefungovaly.

Jako zajímavou metodu pro zodolnění úložného prostoru, je nasazení diskových polí RAID. V diskových polích obětováváme část kapacity disku, aby pole jako celek mělo naději „přežít“ selhání jednoho disku (u určitých typů polí - více). Nejpoužívanějšími typy polí RAID jsou:

- RAID-0 - pole bez parity, celá kapacita disků se propojí a je použita pro data
- RAID-1 - plné zrcadlení, obvykle se používá pro 2 disky, obsah jednoho disku se automaticky replikuje na disk druhý
- RAID-5 - pro 3 a více disků. Kapacita jednoho disku je vyčerpána na paritní informaci (pokud mám 4 1TB disky, pro data mám k dispozici 3TB). Paritní informace samotná je distribuována na všech discích.

Kontrolní otázky

1. Co je to zálohování?
2. Jak se liší inkrementální a úplná záloha?
3. Jak se liší zálohování a klonování disků?
4. Proti selhání kolika disků je odolné pole RAID-5?
5. Co je to redundance v diskových polích?

Odpovědi

1. Zálohování je proces kopie dat z místa jejich použití na bezpečné místo obvykle fyzicky oddělené od místa původního.
2. Inkrementální záloha zálohuje pouze ta data, která se od poslední zálohy změnila, úplná záloha kopíruje úplně všechno.
3. Klonování oproti zálohování uchovává také informaci o umístění souborů na disku.
4. 1
5. Redundance = nadbytečnost, jedná se o paritní informaci vypočtenou na základě uchovávaných dat, umožnující zotavení pole v případě výpadku některého z disků.

Kapitola 5

Lidský činitel

Náhled kapitoly
Systémy jsou tak bezpečné, jak je bezpečný jejich nejslabší článek. Nejslabším článkem bývá často člověk.

Po přečtení kapitoly budete
Vědět

1. s jakými druhy útočníků se lze v praxi setkat
2. jaký je životní cyklus zaměstnance ve firmě a jaké jsou s ním spojeny bezpečnostní aspekty

Čas pro studium
Pro prostudování této kapitoly budete potřebovat přibližně 2 hodiny.

Člověk je často nejslabším článkem technologických systémů. Působení lidského činitele působí různým způsobem. Technologický systém samotný je vytvořen člověkem a my dobře víme, že člověk je tvor omylný. Existují dokonce studie zkoušející kvantifikovat, nakolik je člověk omylný při navrhování takových systémů - měřeno počty řádku programového kódu, na jednu chybu, přítomnou ve finální verzi provozovaného programu.

Studie naznačují, že průměrný programátor nechá takovou chybu v kódu průměrně 1x za 100 řádků kódu. Průměrný programátor vytvoří přibližně 8 000 - 20 000 řádků kódu ročně. Pro zajímavost se uvádí, že Windows 7 má okolo 40 mil. řádků kódu, jádro operačního systému Linux pak okolo 20 mil. řádek kódu.

Přestože existují metody umožňující minimalizovat počet takových a také metody na minimalizaci dopadu chyb na celkovou bezpečnost a stabilitu systému, ani jejich důsledné nasazování nezajisti bezchybovost software. Chyby v software pak mohou být zneužity pro průnik kdo systému.

Člověk také obsluhuje systémy - používá je pro realizaci svých pracovních úkolů, popřípadě pro informování nebo zábavu. Informace a možnostmi, kterými takový člověk disponuje jsou veliké a proto se jejich bezpečností je potřeba zabývat také.

Ochrana proti vnitřním nebo vnějším hrozbám je přitom výrazně odlišná. Externí hrozby se primárně snažíme řešit realizací technických opatření (z nichž některá jsme popisovali v předchozích kapitolách), zatímco hrozby interní jsou technicky obtížněji detekovatelné a proto se zaměřujeme spíše na „soft (měkká)“ řešení spočívající v proškolování a stanovování pravidel a procesů.

5.1 Útoky zvenčí

Pro označení útočníků zvenčí (mimo organizaci) se vžil název *hacker*. Toto slovo začal používat v padesátých letech minulého století známý matematik, nositel Nobelovy ceny za ekonomii (za teorii her) Jonh Nash. Nash názvem hacker označoval trošku posměšně studenty, kteří hledali zkratky ve snaze zjednodušit si cestu k cíli [38]. S postupem času se ale význam posunul, nejprve označoval programátory zaměřené na tvorbu (hackování) jádra operačního systému, později pak získal lehce pejorativní nádech označující člověka pronikajícího do systému, který mu nepatří.

Přesto nelze dát rovnítko mezi hackera a zločince. O tom zda-li je průnik legální nebo ne rozhoduje motivace a způsob provedení útoku. Z hlediska motivace rozlišujeme hackery „podle klobouků“. Toto označování pochází z černobílých kovbojek natáčených v USA. V těchto filmech byl problém v akčních scénách, kde hrálo větší množství lidí, odlišit hrdiny od padouchů. Filmaři přišli s jednoduchý, ale efektivním řešením - hrdinové dostali bílé klobouky a padouši černé. V tomto smyslu rozlišujeme:

- *white hat* - bílý klobouk - bezpečnostní specialista (etický hacker), často najímaný organizacemi pro nalezení slabých míst v zabezpečení, zabývá se penetračním testováním a konzultační činností
- *black hat* - černý klobouk - zabývá se prováděním útokům na systémy za účelem dosažení vlastního prospěchu (krádeže citlivých údajů, ovládnutí dalších počítačů pro rozesílání spam, apod.)
- *gray hat* - většinou etický hacker, ale někdy může jít „přes čáru“ ať už úmyslně nebo neúmyslně

Výše uvedené *penetrační testování* si objednávají organizace od specializovaných firem s cílem zjistit, jak na tom objektivně je zajištění počítačové sítě dané organizace a aktiv na ni připojených. Penetrační testování se děje v čase, délce a intenzitě, na které se obě organizace předem dohodnou. Penetrační testování má za úkol simulovat útok, který by mohl proběhnout z vnějšku organizace, ale v kontrolovaných podmínkách a bez ničivých následků.

Výsledkem testu je zpráva popisují použité postupy a informaci o tom, zda vedly k úspěšnému průniku nebo nikoliv. Organizace realizující penetrační test většinou také formuluje doporučení k lepší ochraně sítě. Výhodou použití externí firmy je zejména to, že má většinou zkušenosti s tímto typem činností (je to konečně také jeden ze základních důvodů její existence), má k dispozici patřičné nástroje pro efektivní realizaci takového útoku a proti interním bezpečnostním odborníkům netrpí „provozní slepotou“.

Jednotlivé skupiny lze pak dále klasifikovat podle podrobnějších kritérií. My se v textu zaměříme ale pouze na představitele skupiny black hat, které lze dále klasifikovat:

- *script kiddie* - používá specializované nástroje umožňují realizovat některé jednoduché útoky. Sám ale nemá potřebné znalosti k tomu, aby přesně věděl, co dělá.
- *běžný hacker* - specialista na průniky do systémů
- *hacktivista* - ideologicky motivovaný hacker - své nelegální průniky nerealizuje za účelem zisku, ale ve jménu určité ideologie, např. ekologické (hackování společností zabývající se těžbou ropy apod.).
- *autor virů* - nevěnuje se realizaci samotných průniků, ale vytváří nástroje, které je umožňují.

Zajímavou a extrémně nebezpečnou skupinou jsou hacktivisté. Etické zdůvodnění průniků umožňuje zástupcům této skupiny způsobovat velké škody aniž by je tížilo svědomí. Organizovanost těchto skupin umožňuje také shromáždění nadkritického množství znalostí pro realizaci velmi sofistikovaných útoků. Některé hacktivistické skupiny jsou všeobecně známé:

- Anonymous
- LulzSec
- AntiSec
- a další

Někde na předělu mezi vnitřními a vnějšími hrozbami stojí služby jako Wikileaks [28]. Wikileaks, jsou neziskovou organizací, která se zabývá zveřejňováním údajů „ve veřejném zájmu“. Etickým problémem je, že ačkoliv veřejný zájem může existovat, zveřejňovaná data jsou často získávána proti vůli jejich vlastníka a často v rozporu se zákonem. Zdrojem dat mohou být hacktivisté nebo útočníci zevnitř organizace.

5.2 Útoky zevnitř

Z hlediska závažnosti jsou útoky realizované zevnitř organizace obzvláště závažné. Aby byl útok zvenčí úspěšný, musí projít několika vrstvami ochrany sítě a aktiva, na které je útočeno, pokud je však útok realizován zevnitř organizace, ochranné vrstvy na vnějším perimetru sítě útok nemohou zachytit.

K realizaci útoku samotného mohou být navíc využity přímo běžné systémy, využívané pro práci. Z tohoto důvodu nejsou schopny takový útok zaznamenat ani systém IDS nebo IPS, které by technicky útok zachytit mohly - není jej možné jednoduše odlišit od běžně prováděných činností na síti.

Útoky zevnitř sítě jsou realizovány obvykle zaměstnanci, někdy hovoříme o hrozbě tzv. *insiderů*. Motivace může být různá. I v případě insidera mohou být motivem peníze - např. některá obchodní tajemství, technická schémata, chemické vzorce složení (např. léků) mohou být dobře zpeněžnitelné např. u konkurence. S tímto druhem kriminality se ale pracuje již velmi dlouho - průmyslová špionáž, nasazování lidí do konkurenčních firem s cílem získat informace se děje již po staletí. IT tento druh kriminality ale velmi zjednodušuje.

Druhým typem motivace může být zjištění nějaké nepřístojnosti v organizaci, kterou daný člověk řeší vynesením informací na veřejnost. V tomto případě nelze říci, že by šlo o kriminální akt. Jedná se ale o činnost, která nutně není v zájmu firmy, je spíše ve veřejném zájmu. Takovéto lidi často označujeme jako tzv. *whistle blowery*.

I činnost whistle blowera může být z pohledu platné legislativy sporná. Dobrým příkladem může být aféra Edwarda Snowdena, zveřejnil řadu tajných materiálů popisující problematické praktiky celosvětového monitoringu prakticky všech forem komunikace americkou NSA. Přestože rozsah monitoringu podle některých odborníků na problematiku překračuje meze stanovené legislativou USA, vynášení a zveřejňování tajných údajů je trestné také.

Posledním motivem, který insider může mít, je pomsta. Pomsta je pokrm, který je nejlépe servírovat za studena (staré Klingonské přísloví). Pomsta, jako motivační faktor, je obzvláště nebezpečná, protože je vetšinou dlouhodobě naplánována s cílem ve finále způsobit maximální škody.

Je potřeba si uvědomit, že běžný člověk stráví v práci 8 nebo více hodin denně - to je podstatná část doby, po které je člověk vzhůru. V práci máme přátele, někteří lidé si v práci nalezli svého životního partnera, jiní ho (ji) kvůli práci ztratili. Proto každá křivda, ať už domnělá nebo skutečná, může být vnímána jednotlivými účastníky konfliktů velmi intenzivně. To pak může i jinak bezproblémové zaměstnance motivovat k odvetným akcím, poškozujícím organizaci.

Pracovní poměr je vždy ukončen nějakou formou odchodu zaměstnance. Celý proces života zaměstnance ve firmě lze znázornit jako koloběh života, viz obr. 5.1.

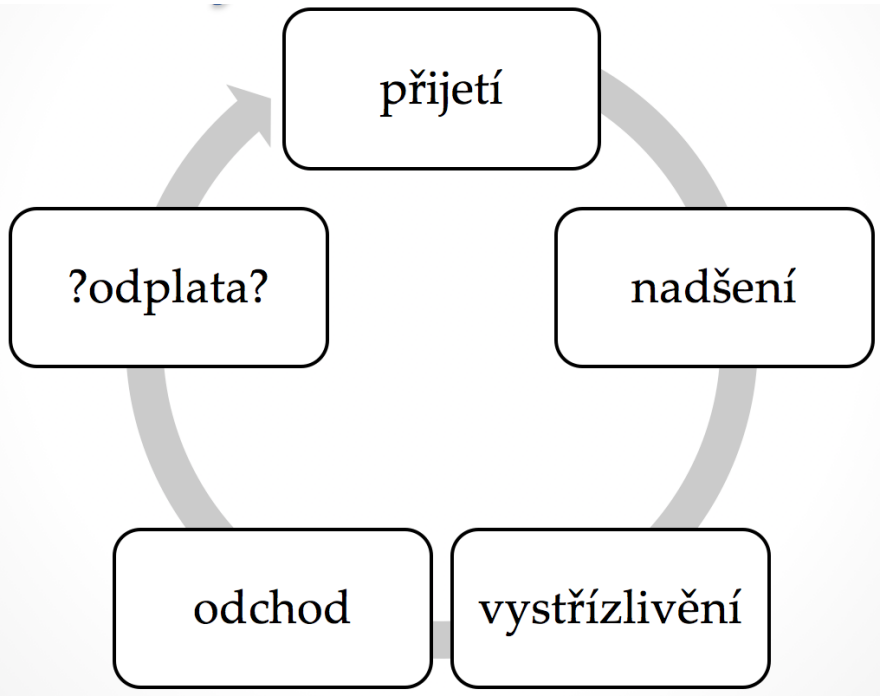
Když zaměstnanec nastupuje do nové práce většinou tak činí s určitou dávkou nadšení. Jednak získat práci není až tak úplně jednoduché, jednak každá nová práce představuje do určité míry nový začátek. Nadšení, ale častá záhy vezme za své a je nahrazeno často šedivou realitou každodenní práce. Přijdou konflikty s kolegy a nadřízenými a ve finále dříve nebo později také odchod.

To jestli tento odchod proběhne bez problémů je otázka přístupu obou stran (zaměstnance i zaměstnavatele). Z pohledu minimalizace případných škod je možné výše uvedený cyklus charakterizovat třemi pracovními situacemi:

1. přijetí - je možno identifikovat osobnostní rysy uchazeče
2. práce - nastavení minimálních možných práv k systémům
3. odchod - korektní jednání, pečlivý monitoring činností odcházejícího

V rámci přijímacího řízení je možno do určité míry poznat uchazeče, identifikovat jeho základní osobnostní rysy a podle toho se zařídit. Bohužel osobnost se do určité míry v průběhu času mění v důsledku vnějších vlivů, zdraví, úspěšnosti v osobním životě apod. Mění se také pracovní prostředí: staří zaměstnanci odcházejí a jsou nahrazováni zaměstnanci novými, mění se technologie a systémy, se kterými pracujeme, stejně jako procesy, kterými tak činíme. To je také důvod proč ve všech případech není možno předem problémové lidi identifikovat.

Nově přijímaný člověk by měl splňovat předem definované etické standardy práce a po přijetí by co nejdříve měl projít školením, kde bude seznámen s tím, co a jak je od něj očekáváno. Pracovní činnosti, které zaměstnanec vykonává by měly být jasně vymezeny a měly by s nimi být spojeny také potřebné vymezení práv k systémům, které jsou nutné pro vykonávání této práce. Správné určení portfolia přístupových práv omezuje do určité míry možnost zneužití pro účely poškození organizace. Přiděleno by **vždy mělo být minimální množství práv** k systému.



Obrázek 5.1: Působení zaměstnance ve firmě

Odchod by měl proběhnout co nejkorektněji - toto ale organizace může ovlivnit pouze ze strany zaměstnavatele, nikoliv toho jak nepříjemnou zprávu vezme samotný zaměstnanec. Platná legislativa v ČR poskytuje přitom poměrně velkou míru ochrany odcházejícího zaměstnance, jako je dvouměsíční lhůta, odstupné apod. Z pohledu bezpečnosti je zejména problematická ochranná dvouměsíční lhůta. To je období, po které zaměstnance již ví, že odchází a může osnovat pomstu.

Ochrannou lhůtu je možno zkrátit, ale odchod zaměstnance musí být formou dohody. Alternativou je možnost přeřadit zaměstnance na jinou práci (s patřičnou úpravou přístupových práv) do doby odchodu z organizace. Z pohledu obzvláště rizikových skupin zaměstnanců je možno zmínit dvě: administrátoři a manageři. Zaměstnání administrátora představuje riziko z pohledu rozsahu práv, které má administrátor pro svou práci k dispozici. Manageři jsou problematičtí informacemi, se kterými pracují.

Manager při odchodu navíc často dostává notebook, který používal během své práce. Přestože se to zdá jako poměrně velký benefit, ve skutečnosti tomu tak není. Cena použitého hardware s časem klesá - firma proto z hlediska nákladů „dává“ managerovi pouze zůstatkovou hodnotu notebooku, která představuje pouze zlomek pořizovací ceny zařízení. Z pohledu bezpečnosti je rizikový obsah takového zařízení. Předávané zařízení by mělo být „čisté“ - neobsahovat žádné firemní informace.

Tento požadavek je možno zajistit jednoduše přeinstalováním zařízení a smazáním nežádoucích dat jako přípravy na odchod managera a poslední službu, kterou mu daná organizace poskytne. Prosaditelnosti tohoto opatření pomáhá, že reinstalace zařízení obvykle vede k znatelnému zvýšení rychlosti zařízení.

Z hlediska ostatních zaměstnanců lze obecně říci následující. Snadněji se identifikuje problém u zaměstnanců, kteří jsou povahově spíše extroverti a své názory a nálady jsou schopni a často více než ochotni ventilovat na veřejnosti. Naopak „osamocení vlci“ jsou velmi obtížně odhalitelní před provedením útoku.

V minulosti byly provedeny některé studie popisující charakteristiky hrozeb plynoucích od insiderů, viz např. zpráva [33] zabývající se hrozbou insiderů pro finanční sektor USA. Studie ukázaly, že pomsta není realizována z náhlého popudu, rozhodnuté zraje v zaměstnance dlouhou dobu. Podobně i doba přípravy útoku samotného může být dlouhá. Výzkum ukázal, že lidé překvapivě vnímají odlišně hodnotu fyzických předmětů a dat. Překvapivost je v tom, že fyzické předměty jsou vnímány jako cennější, ačkoliv v praxi je tomu často naopak.

Z hlediska bezpečnosti, je tato situace velmi problematická, protože znamená, že zaměstnanec byť třeba fyzicky nepoškodí automobil svého vedoucího, může být ochoten odstavit klíčový server

společnosti a ani si neuvědomí, že takový čin je podstatně závažnější.

Odlišně je vnímána také odhalitelnost jednání on-line. Připojení na Internet nám dává jistý, většinou neoprávněny, pocit anonymity. Pokud jsme anonymní, naše případné přečiny nemohou být odhaleny, že? Pokud spojíme pocit anonymity s nízkým vnímáním hodnoty dat, co nám z tohoto vyplyne z hlediska provedení útoku ... vyplyne, že se vlastně jedná o *takový žert*. Z hlediska organizace, se ale nejedná o žert. Způsobené škody jsou reálné a obvykle velké. Realizace útoku může být klasifikována jako trestný čin a organizace se může domáhat náhrady škod.

Nástroje, jak tento problém řešit, specializované v podstatě nejsou. Obecně lze doporučit:

- budovat příznivé pracovní prostředí
- mít stanovená pravidla pro přijímání, odchod zaměstnanců, stejně jako situaci, kdy se mění pracovní pozice/úkoly zaměstnance (nastavování přístupových práv k IT aktivům společnosti)
- pravidelné zálohování, řešení ochrany záloh a způsobu obnovy funkce aktiva ze zálohy

Shrnutí

Při ochraně IT, je zdrojem většiny hrozeb člověk - ať už přímo (např. útok hackera) nebo nepřímo (vytváření a provozem IT systémů). Z pohledu členění takových hrozeb je výhodné rozlišovat mezi hrozbami přicházejícími z vnějšku a těmi, které pocházejí od vlastních zaměstnanců - tzv. insiderů.

Externí hrozby lze do určité míry řídit nasazováním technických prostředků pro zabezpečení především perimetru sítě. V případě insiderů, ale případný útok přichází zevnitř - vnější ochranný perimetr sítě je tedy již překonán. Navíc insider má často velmi podrobné informace o vnitřním fungování systémů v organizaci (útočník z vnějšku se pouze dohaduje jak fungují), může mít do systémů přístupová práva a může systémy samotné zneužít pro provedení útoku.

Takový typ útoků je proto obtížně technicky detekovatelný. Řešení spočívá v práci s personálem a pečlivém nastavování práv uživatelům k jednotlivým systémům.

Kontrolní otázky

1. Jaký je rozdíl mezi White hat a Black hat?
2. Jak je možné se chránit proti útokům z vnějšku?
3. Co je to penetrační testování?
4. Čím je specifická hrozba od insidera?
5. Kdo je to hacktivista?

Odpovědi

1. White hat je bezpečnostní specialista, black hat se zabývá počítačovou kriminalitou.
2. Technická opatření zejména na vnějším perimetru sítě.
3. Organizace si může zaplatit externí konzultační firmu pro provedení penetračního testu. Kontraktor se pak pokusí kontrolovaně proniknout do sítě. Organizace je následně seznámena s výsledky a doporučeními, jak dále postupovat v zabezpečení sítě.
4. Insider bude útočit zevnitř firmy, technicky je útok špatně detekovatelný a následky takového útoku jsou často zničující.
5. Politicky motivovaný hacker.

Kapitola 6

Typy útoků a jejich provedení

Náhled kapitoly
V této kapitole se seznámíme s nejčastěji realizovanými typy útoků a způsobem jejich provedení.

Po přečtení kapitoly budete
Vědět

1. co jsou to útoky typu DoS a DDoS
2. jaké typy útoků se realizují fyzicky - za účelem fyzického průniku do objektů a získání přístupu k prostředkům IT

Čas pro studium
Pro prostudování této kapitoly budete potřebovat přibližně 2 hodiny.

6.1 Útoky DoS a DDoS

Útoky typu Denial of Services (DoS) a Distributed Denial of Services (DDoS) jsou jedněmi z nejčastěji prováděných útoků, které mohou vést k úplnému a dlouhodobému odstavení IT služeb poskytovaných napadeným prostředkem IT. Denial of Services, česky odepření služeb je založeno na způsobu fungování moderní výpočetní techniky. Zranitelné tímto útokem jsou veškeré systémy připojené do počítačové sítě, především pak ty, které jsou přístupné z Internetu (ale nejen výhradně ony).

Prostředek IT poskytuje své služby na základě zaslaného požadavku. Požadavky na poskytnutí služby si dané zařízení zařazuje do fronty požadavků, kterou postupně v rámci svých možností vyřizuje, obvykle systémem First In First Out (FIFO). FIFO znamená, že požadavek, který přijde první bude také první vyřízen. Každé zařízení má určitou kapacitu vyřizování takových požadavků. Tato kapacita může být omezena přenosovými kapacitami sítě, přes kterou je zařízení připojeno a také vnitřní konfigurací zařízení (jak silný procesor, kolik paměti apod.).

Kapacita fronty tedy není bezedná. V okamžiku, kdy je požadavků více než může zařízení vyřídit jsou některé požadavky odmítány. Obvykle se postupuje tak, že se nastaví doba platnosti požadavku, a ty požadavky, které jsou ve frontě déle než je nastavená doba platnosti jsou zahazovány, aniž by byly vyřízeny. Místo požadovaného výsledku proto zařízení vrátí chybové hlášení o vypršení času (timeout).

Útok DoS je založen na tom, že útočník vytváří velké množství požadavků na službu s cílem vyčerpání její kapacity. Prakticky to funguje tak, že ve frontě požadavků pomalu přibývají požadavky podvržené. Pro oprávněného uživatele se tak odezva vzdáleného zařízení zpomaluje s tím jak ve frontě narůstá procentní podíl podvržených požadavků a požadavků oprávněných uživatelů, až přestane zařízení poskytovat služby úplně (je plně zahlceno podvrženými požadavky).

Existuje velké množství typů útoků DoS, které se liší náročností technické realizace, náročností zpracování požadavků na straně serveru a také možnostmi ochrany proti nim. V těchto skriptech se nebudeme zabývat technickými podrobnostmi provedení těchto útoků, podíváme se spíše na jejich základní typologii.

Základní rozdíl mezi útoky typu DoS a DDoS je místo provedení. Útok DoS je realizován obvykle z jednoho nebo několika málo míst. To nám dává možnost tato místa identifikovat a preventivně, např. pomocí firewallu, síťový provoz z těchto míst blokovat. Oproti tomu je útok DDoS silně distribuován - zdrojů útoku je tak příliš mnoho, aby je bylo možné jednoduše blokovat. Jednoduché řešení takového útoku pak není možné.

Organizace se do určité míry může bránit útokům DDoS tak, že použije serverové farmy podporující rozkládání zátěže mezi servery (load balancing), čímž se výrazně navýší kapacita systému reagovat na požadavky. Toto řešení ale není levné, proto se volí pouze pro kritické systémy, které musí být online neustále a zejména pro velké firmy. Ani takové řešení však není 100 % účinné.

Pro určité typy útoků může jít řešení úplně nad rámec běžných možností firmy - teoreticky je možno provádět regionální filtraci síťového provozu. Regionální je zde myšleno síťový provoz plynoucí z určitého státu. Tento typ filtrace je ale primárně určen (alespoň v podmínkách ČR) pro účely ochrany kritické infrastruktury popřípadě významných informačních systémů, dle platné legislativy.

Ochrana KI
V těchto skriptech není prostor jít příliš do podrobností o této problematice. V případě zájmu konzultujte proto skripta z předmětu *Bezpečnostní informatika 1* [48] v sedmém nebo novějším vydání (určeném pro výuku předmětu v roce 2017). Pozornost věnujte zejména organizaci národních a vládních CERT a CSIRT týmů a také kapitole věnované zákonu o kybernetické bezpečnosti.

6.2 DNS spoofing, DNS cache poisoning

Oba dva typy útoků jsou velmi nebezpečné tím, že narušují funkčnost služeb pro jména domén, tedy služby DNS. Nebezpečnost spočívá v tom, že DNS je používáno pro převod doménových jmen na IP adresy - tedy určení adresy místa, kam se zašle požadavek. Narušení funkčnosti DNS znamená, že uživatel zadá adresu do WWW prohlížeče tak, jak je zvyklý, jeho požadavek však bude přesměrován na odlišné místo než očekává.

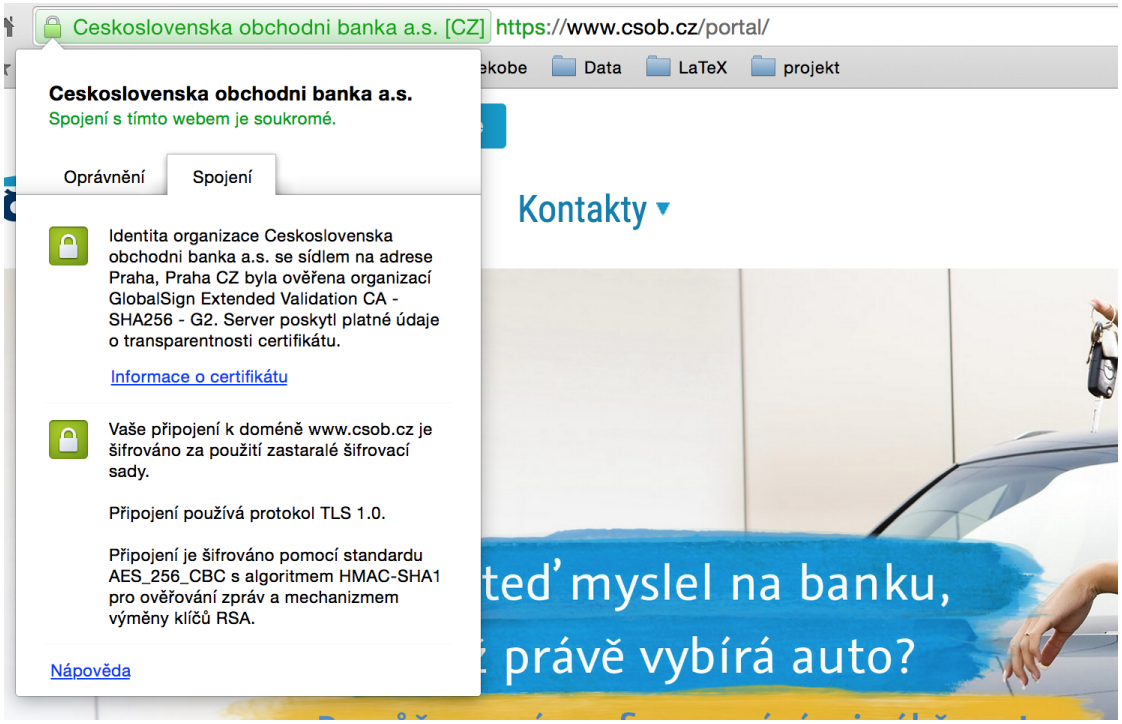
Provoz je často přesměrováván na kompromitované servery nebo servery přímo pod kontrolou útočníka, který se může pokusit získat z uživatele cenné informace jako jsou přihlašovací jména a hesla ke službám a podobně.

Výše uvedené útoky jsou ještě nebezpečnější pokud jsou doprovázeny útokem phishingovým. Oba útoky využívají toho, že DNS je nutné aktualizovat – útok se děje prostřednictvím šíření požadavků na aktualizaci DNS. Útočník se tedy snaží přesvědčit DNS server, aby změnil své záznamy. Útok tedy probíhá nutně na koncové zařízení postiženého ale provozovatele DNS služby. Možnosti jak případné přesměrování odhalit existují, ale jednotlivé servery s nimi musí počítat předem.

Základní ochrana je nasazením DNSSec. DNSSec pro účely ochrany zavádí do běžného DNS prvky asymetrické kryptografie. Vlastník pak požadavky na zavedení a změny v DNS elektronicky podepisuje. Jelikož privátní klíč by měl být ve vlastnictví pouze privátní osoby - jsou požadavky na změny důvěryhodně spojeny s oprávněným uživatelem a je tak prakticky nemožné požadavek na změnu podvrhnout.

To je výhodné i pro koncového uživatele - tedy odběratele služby. V okamžiku, kdy se ke službě připojí moderní WWW prohlížeč vizuálně upozorní, že spojení je bezpečné. Pokud tedy je uživatele „zvyklý“ pracovat v bezpečném režimu a náhle se mu v prohlížeči ukáže, že připojení bezpečné není - může tušit, že něco není v pořádku a začít situaci řešit.

Příklad bezpečného spojení pomocí WWW prohlížeče Chrome 45 na web ČSOB je znázorněn na obr. 6.1.



Obrázek 6.1: Příklad bezpečného spojení pomocí WWW prohlížeče Chrome 45 na web ČSOB

6.3 SQL injection

Útoky typu SQL injection využívají slabin v ošetření příkazů v jazyce SQL, kterým se manipuluje v záznamy v databázích. Jedná se o útok, který je realizován pomocí běžného rozhraní často rozhraní WWW, do kterého ale útočník zavádí některé neočekávané znaky, které nutí systém pracovat jiným způsobem než bylo očekáváno, což může vést k navýšení právy, poskytnutí většího množství informací apod.

Tento vychází z toho, že prakticky všechny informační systémy jako back end využívají relační databáze. Tyto databáze jsou ovládány příkazy SQL. Za normálních okolností koncový uživatel s SQL nepřijde do styku - při své práci používá připravené grafické uživatelské rozhraní (Graphical User Interface (GUI)). Systém sám činnosti uživatele interpretuje a dynamicky si sestaví SQL příkaz, který pošle dál databázi.

Útočník se však snaží toto vnitřní chování poznat a zneužít ve svůj prospěch.

Zkusme si představit jednoduchý příklad. Mějme aplikaci, která vyžaduje zadání uživatelského jména a hesla. Jména a hesla uživatelů jsou ložena v databázi v tabulce *uzivatele*. Abychom situaci nekomplikovali budeme předpokládat, že tabulka obsahuje jen dva sloupce: *jmeno* a *heslo*.

Většina aplikací postupuje při ověřování tak, že načte heslo daného uživatelského účtu - ten je identifikován v přihlašovacím formuláři zadaným uživatelským jménem a toto heslo porovná z heslem zadaným. SQL dotaz na takové heslo může vypadat následovně:

```
SELECT heslo FROM uzivatele WHERE jmeno LIKE 'zadaneJmeno';
```

Zadané jméno se přejímá z formuláře - to co tam bude napsané je tedy pod kontrolou případného útočníka. Ten se může rozhodnout místo zkoušení různých jmen a hesel zadat např. následující řetězec: `a' OR 'b'='b`. Systém pak sestaví následující SQL příkaz:

```
SELECT heslo FROM uzivatele WHERE jmeno LIKE 'a' OR 'b'='b';
```

Útočník tak změní samotnou logiku vyhodnocení přihlašovacích údajů. Útočník může podvrhnout celý SQL příkaz (do formuláře zadaná část tučně):

```
SELECT heslo FROM uzivatele WHERE jmeno LIKE ''a';DROP TABLE uzivatele; -';
```

Ochrana proti SQL injection není možná na straně uživatele - ochranné prvky musí být implementovány na straně systému. Mělo by přitom platit, že údaje zadávané uživatelem jsou nedůvěryhodné. Systém by měl počítat s tím, že se jej pokusí někdo zneužít tímto způsobem.

Systém by proto měl:

- kontrolovat parametry zadaných políček, tedy že položka datum má formát data, e-mailová adresa vypadá jako e-mailová adresa apod.
- aplikovat specializované funkce (v programovacích jazycích) a knihovny na ochranu proti těmto problémům

Z pohledu firemního by měl být kladen důraz na aplikování vhodných postupů vývoje, pokud systémy jsou vyvíjeny vlastními silami. V případě, že je vývoj kontraktován nebo systém byl dodán jako hotové řešení je potřeba dbát na dlouhodobou podporu takového řešení ze strany dodavatele.

Případné opravy pak organizace, která systém používá, musí instalovat co možná nejdříve po vydání, tak aby riziko zneužití odhalených chyb bylo co možná nejnižší.

6.4 Sociální inženýrství

Do této skupiny patří řada postupů, které lze využít pro získání citlivých informací nebo získání přístupu do jinak nepřístupných (bezpečných) lokací:

- Pretexting (blagging, bohoing)
- Diversion theft
- Phishing
  - IVR, phone phishing (vishing)
  - Baiting
- Quid pro quo
- Tailgating
- a další

Pretexting je základní metodou sociálního inženýrství. Útočník shromažďuje informace o organizaci, ale také jednotlivých zaměstnancích s cílem vydávat se za důvěryhodnou osobu v této organizaci. Kontakt mezi útočníkem a skutečným zaměstnancem je buďto po telefonu nebo dokonce osobní.

Základním zdrojem informací jsou veřejně dostupné informace o organizaci, webové stránky, profily organizace a zaměstnanců na sociálních sítích. Útočník tyto informace použije během konverzace aby prokázal znalosti, které jsou očekávány pouze od skutečného zaměstnance. Konverzace pak probíhá jinak, než by zaměstnanec mluvil s cizí osobou a může být náchylnější ke sdělování citlivých informací.

Tímto způsobem může útočník získat např. pro získání údajů osobního charakteru - jako jsou zákaznická čísla, rodné číslo, postupy používané v organizaci, neveřejné dokumenty a další.

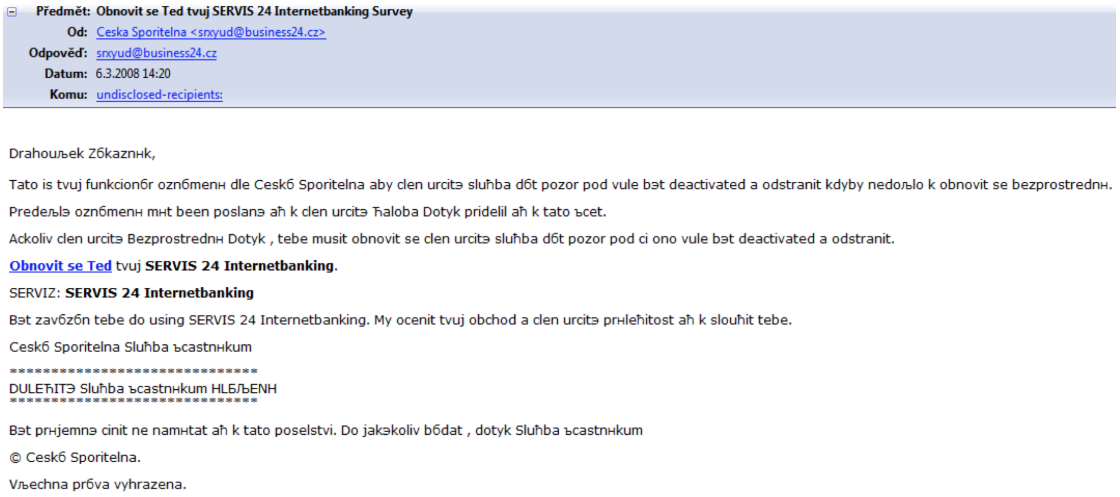
Diversion theft je poměrně známý a dlouho používaný trik, který je prováděn profesionálními podvodníky. Cílem je přesvědčit doručovací společnost, aby cennou zásilku doručila na odlišné místo, které je pod kontrolou podvodníka.

Ověřování místa doručení probíhá obvykle pomocí mobilního telefonu, který by měl být pouze ve vlastnictví oprávněného uživatele. Aby byl útok úspěšný, musí útočník vědět, že taková zásilka je na cestě a alespoň krátkodobě získat kontrolu nad mobilním telefonem, přes který je realizována komunikace s doručovací službou.

Často používanou metodou pro získávání citlivých informací je *phishing*. V češtině se používá také název *rhybaření*. Útočník kontaktuje budoucí oběť obvykle pomocí e-mailu, ve kterém jej přesvědčuje, že je v jeho nejlepším zájmu sdělit mu osobní nebo jiné citlivé údaje. Phishingové útoky jsou realizovány velmi často na zákazníky bank. Jeden z prvních phishingových útoků v ČR byl dnes již legendární „drahoušek zákazník“, viz obr. 6.2, který byl cílen na zákazníky České spořitelny.

V minulosti poskytovala pro ČR poměrně dobrou ochranu čeština - její zvládnutí totiž není jednoduché. Strojově přeložený text je tak jednoduše identifikovatelný a logicky důvěryhodnost takového mailu mizivá. V dnešní době je ale možné zaznamenat v této oblasti velký posun a i v ČR se objevily útoky, které jsou po stránce použitého jazyka naprosto v pořádku.

Ve firemní sféře se používá útok na podobném principu - ovšem s tím, že obvykle nejsou přímo požadovány citlivé údaje - útočník se spíše snaží motivovat svou oběť aby otevřela přílohu obsahující



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 Z6kaznнk,

Tato is tvuj funkcionбr oznбmenн dle Ceskб Sporitelna aby clen urcitэ sluћba dбt pozor pod vule bэt deactivated a odstranit kdyby nedoљlo k obnovit se bezprostrednн.

Predeљlэ oznбmenн mнt been poslanэ aћ k clen urcitэ ћaloba Dotyk pridelil aћ k tato ъcet.

Ackoliv clen urcitэ Bezprostrednн Dotyk , tebe musit obnovit se clen urcitэ sluћba dбt pozor pod ci ono vule bэt deactivated a odstranit.

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

SERVIZ: **SERVIS 24 Internetbanking**

Bэt zavбzбn tebe do using SERVIS 24 Internetbanking. My ocenit tvuj obchod a clen urcitэ prнlehitost aћ k slouћit tebe.

Ceskб Sporitelna Sluћba ъcastnнkum

****
DULEЋITЭ Sluћba ъcastnнkum HLБЉENH
****

Bэt prнjemnэ cinit ne namнtat aћ k tato poselstvi. Do jakэkoliv bбdat , dotyk Sluћba ъcastnнkum

© Ceskб Sporitelna.

Vљechna prбva vyhrazena.

Obrázek 6.2: Drahoušek zákazník - jeden z prvních zaznamenaných phishingových útoků v ČR

škodlivý kód. Zaznamenány byly případy, kdy útočník využil známé zranitelnosti starší verze Adobe Readeru a upravil PDF soubor obsahující nevinně vyhlížející pozvánku na konferenci, aby infikovala počítač, na kterém je soubor otevřen.

V případě úspěchu si postižený ani neuvědomí, co se stalo.

Vhodnou obranou je obezřetnost a zajištění včasných aktualizací software používaného na počítačích v organizaci, tak aby se riziko zneužití známých zranitelností minimalizovalo.

V posledních několika letech se můžeme setkat také s aplikací phishingových postupů s použitím odlišných technologií. Kontakt může být navázán např. po telefonu - v takové případě hovoříme o tzv. *vishingu*. Útok je založen na tom, že při osobním kontaktu, nebo kontaktu po telefonu mnohem snadněji sdělíme citlivé informace, než kdyby ke kontaktu došlo pouze písemnou formou.

Vishingový útok je také v mnoha ohledech pružnější, protože útočník komunikuje se svou obětí v reálném čase a může tak okamžitě reagovat.

Obvzláště záludnou technikou je tzv. *baiting*. Útočník nechá ve veřejných prostorech organizace infikovaný nosič (USB, CD, apod.) v očekávání, že jej někdo najde a podívá se co, je na něm obsaženo, čímž dojde k napadení počítače.

Zvláštním typem útoku je útok typu *quid pro quo*. Útočník se v něm vydává za technickou podporu a začne s obětí řešit imaginární technický problém, o kterém postižený neví, že ho má. Tímto způsobem může útočník přesvědčit svou oběť aby otevřela porty a umožnila tak útočníkovi ovládnout počítač.

I v případě, že nedojde k „odevzdání“ počítače do rukou útočníka, může postižený předat spousty citlivých informací.

Tailgating je další poměrně starou technikou, pomocí které se může útočník dostat do míst s řízeným přístupem, kde by rozhodně přístup mít neměl. Technika funguje velmi jednoduše - útočník jednoduše počká až někdo půjde od dané oblasti a jde za ním. Oprávněná osoba spustí autentizační proces, útočník ale protože projde „společně“ s takovou osobou jej ale obejde.

Řešením je realizace takových opatření, aby každá osoba vstupující do takových oblastí prošla předepsaným autentizačním procesem.

Obecně jako ochranu proti metodám sociálního inženýrství lze doporučit:

- provádět školení na použití důvěrných informací a situací, kdy je mohou sdělit někomu dalšímu (Váš administrátor se Vás nikdy nezeptá na heslo, nepotřebuje ho)
- návrh procesů v organizaci, které s takovými útoky počítají
- provádět testování bezpečnosti
- vhodně provádět skartaci údajů (pozor na odpadkové koše)

Další možnosti studia

Je k dispozici řada zdrojů, které mohou pomoci zorientovat se podrobně v možnostech sociálního inženýrství v oblasti bezpečnosti IT. Průkopníkem v této oblasti je známy hacker Kevin Mitnick, který napsal knihu zaměřenou čistě na oblast sociálního inženýrství: *Umění klamu* [40].

Shrnutí

Existuje celá řada útoků, které ohrožují provoz prostředků IT v organizacích. Útoky typu DoS zahlcují dálkově přístupné služby podvrženými požadavky s cílem znemožnit vykonávání běžných (oprávněných) požadavků. Obrana proti takovým útokům je problematická a dostupná pouze pro velké organizace schopné do prostředků ochrany investovat. Ochrana je realizována použitím serverových farem - zátěž v takových případech je rozdělována na různé servery.

Útoky zaměřené na DNS ovlivňují to, co koncový uživatel uvidí pokud do WWW prohlížeče zadá webovou adresu - bude to očekávaná stránka nebo stránka podvržená. Existují technologická řešení tohoto problému a to je nasazení technologií elektronického podpisu pro manipulaci s doménovými záznamy - DNSSec.

Útokům SQL injection je ale nutné se bránit na úrovni programového kódu. Ochrana spočívá především v kontrole parametrů zadávaných uživateli do GUI programu.

Metody sociálního inženýrství jsou zaměřeny na zneužití chování běžných lidí k získání informací nebo fyzického přístupu do určitého místa nebo k určitému zařízení. Ochrana je poměrně složitá, jelikož úspěch je limitován dodržování bezpečnostních předpisů všemi zaměstnanci dané organizace.

Kontrolní otázky

1. Co je to útok DoS?
2. K čemu je DNS a proč jsou útoku na ni tak nebezpečné?
3. Co je to tailgating?
4. Jak se chránit metodám sociálního inženýrství?

Odpovědi

1. Útok odepření služeb, útok zahltí zařízení podvrženými požadavky aby zabránil vyřizování těch oprávněných.
2. DNS je stará o překlad IP adres na doménová jména a zpět. Nebezpečnost spočívá v tom, že koncový uživatel nemá šanci jednoduše rozhodnout, zda se dostal na „správné“ stránky.
3. Útočník projde do oblasti s řízeným přístupem společně s oprávněným uživatelem aby se vyhnul nutnosti projít autentizačním procesem.
4. Jednoduchá ochrana není možná. Všechna obranná opatření se musí týkat lidí. Základem je proškolování a příprava procesů.

Kapitola 7

Systémy řízení informační bezpečnosti

Náhled kapitoly
Existuje mnoho způsobů jak získat kontrolu nad informační bezpečností. Řada z těchto způsobů je založena na různých normách, metodách a metodologiích. V této kapitole se zaměříme na problematiku kodexu norem ISO 27 000, především pak na tvorbu bezpečnostních politik.

Po přečtení kapitoly budete
Vědět

1. Jak funguje ISO 27 000
2. jaké jsou typy dokumentů používaných pro řízení informační bezpečnosti
3. jak napsat bezpečnostní politiku (nebo alespoň její základy)

Čas pro studium
Pro prostudování této kapitoly budete potřebovat přibližně 2 hodiny.

ISO 27 000 je jedním z nejpoužívanějších kodexů norem. Jeho účelem je pomoci se získáním kontroly nad řízením informační bezpečnosti (Information Security Management System (ISMS)). Získáním kontroly se v tomto případě myslí transformace organizace tak, aby byla schopna plánovat vývoj v informační bezpečnosti, byla ji schopna řídit a nebyla tažena událostmi.

ISMS proto pomáhá ve stanovení kontextu informační bezpečnosti - co má být předmětem ochrany. To pak umožňuje identifikovat hlavní rizika a způsoby ochrany proti nim. Základním nástrojem ochrany je pak obvykle formalizace procesu, jakým má být chráněné aktivum používáno tak, aby to bylo bezpečné. Takový proces často nazýváme *bezpečnostní politika*.

Kodex norem ISO 27 000 obsahuje základní normy, které jsou obvykle implementovány v každém systému ISMS a pak řada doplňkových norem, které jsou implementovány podle toho, jaké jsou bezpečnostní cíle implementace ISMS a v jakém oboru daná organizace pracuje.

Základní normy:

- ISO/IEC 27000 Information technology - Security techniques - Information security management systems - Overview and vocabulary [13]
- ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements
- ISO/IEC 27002 Information technology - Security techniques - Code of practice for information security management.
- ISO/IEC 27005 Information technology - Security techniques - Information security risk management

Doplňkové normy:

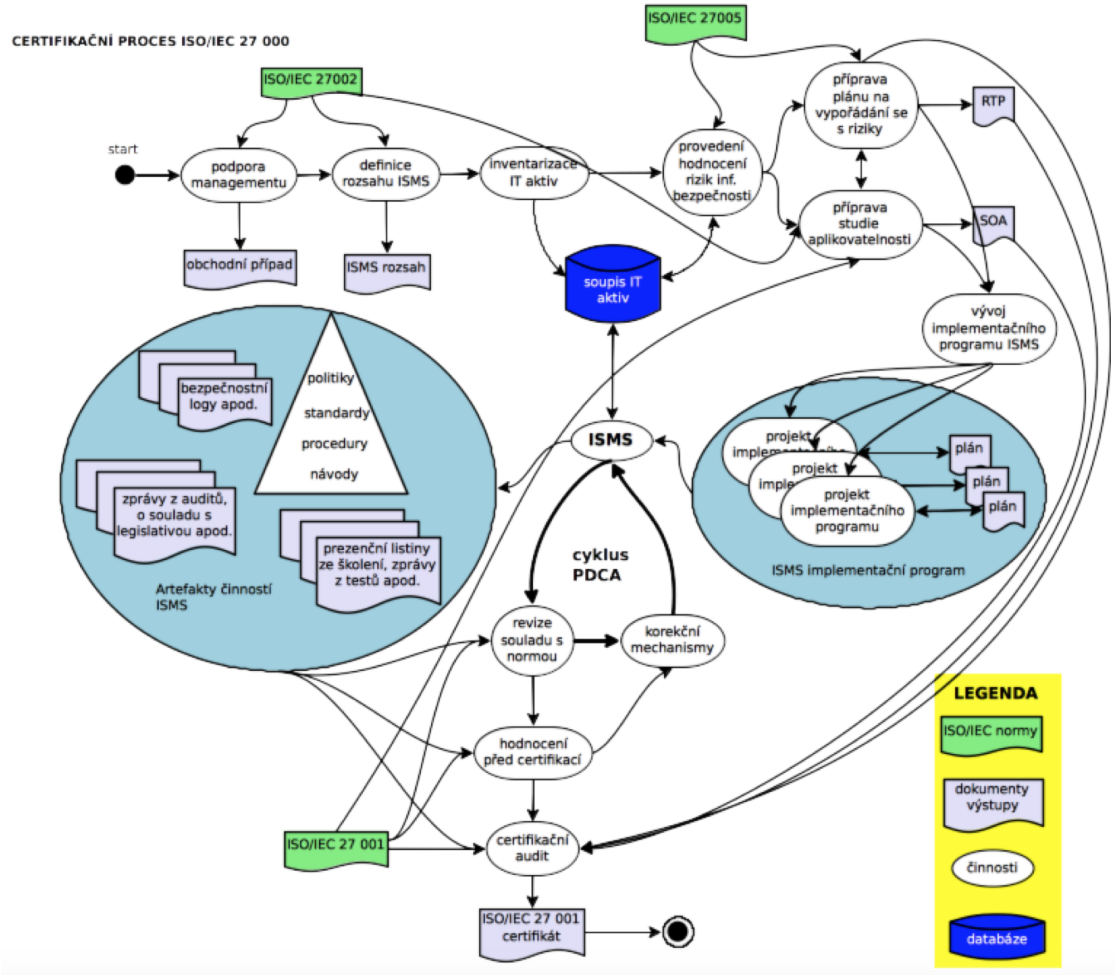
- ISO 27003 - návod pro návrh a zavedení ISMS v souladu s ISO 27001.
- ISO 27004 Information technology - Security techniques - Information security management - Measurement
- ISO 27006 Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems
- ISO 27007 Information technology - Security techniques - Guidelines for information security management systems auditing
- ISO 27008 Information technology - Security techniques - Guidelines for auditors on information security management systems controls
- ISO/IEC 27010:2012 Information technology - Security techniques - Information security management for inter-sector and inter-organisational communications
- ISO/IEC 27011:2008 Information technology - Security techniques - Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
- ISO/IEC 27013:2012 Information technology - Security techniques - Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
- ISO 27014 ITU-T Recommendation X.1054 & ISO/IEC 27014:2013 Information technology - Security techniques - Governance of information security
- ISO/IEC TR 27015:2012 Information technology - Security techniques - Information security management guidelines for financial services
- ISO/IEC TR 27016:2014 - IT Security - Security techniques - Information security management - Organizational economics
- ISO/IEC 27018:2014 Information technology - Security techniques - Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors
- ISO/IEC TR 27019:2013 Information technology - Security techniques - Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy industry
- ISO/IEC 27031:2011 Information technology - Security techniques - Guidelines for information and communications technology readiness for business continuity
- ISO 27032 Guidelines for cybersecurity
- ISO 27033
  - ISO/IEC 27033-1:2009 Network security overview and concepts
  - ISO/IEC 27033-2:2012 Guidelines for the design and implementation of network security
  - ISO/IEC 27033-3:2010 Reference networking scenarios - threats, design techniques and control issues
  - ISO/IEC 27033-4:2014 Securing communications between networks using security gateways
  - ISO/IEC 27033-5:2013 Securing communications across networks using Virtual Private Networks (VPNs)
  - *ISO/IEC 27033-6: Securing wireless IP network access (DRAFT)*
- ISO 27034
  - ISO/IEC 27034-1:2011 Information technology - Security techniques - Application security overview and concepts
  - v řadě norem ISO 27034 jsou plánovány ještě části 2 - 8
- ISO 27035 Information security incident management
- ISO 27036 Information security for supplier relationships
  - ISO/IEC 27036-1: 2014 Information security for supplier relationships - Part 1: Overview and concepts.
  - ISO/IEC 27036-2: 2014 Information security for supplier relationships - Part 2: Requirements
  - ISO/IEC 27036-3:2013 Guidelines for ICT supply chain security
  - *ISO/IEC 27036–4 Guidelines for security of cloud services (DRAFT)*
- ISO/IEC 27037:2012 Information technology - Security techniques - Guidelines for identification, collection, acquisition, and preservation of digital evidence
- ISO/IEC 27038:2014 Information technology - Security techniques - Specification for digital redaction
- ISO/IEC 27799:2008 Health informatics - Information security management in health using ISO/IEC 27002

Přestože je výše uvedený přehled rozsáhlý, není kodex norem ISO 27 000 stále ještě kompletní a bude se dále rozšiřovat o nové postupy a pokrytá odvětví.

Podrobnější studium systémů ISMS
Vzhledem k rozsahu celého kodexu se v tomto předmětu dostaneme pouze na povrch. Podrobnější informace lze získat v předmětu *Bezpečnost informačních systémů* vyučovaném v magisterském studiu.

ISO 27 000 je typem normy, na kterou se organizace často nechávají certifikovat (podobně třeba jako v případě normy ISO 9 000). Požadavek na certifikaci není většinou zakotven přímo v legislativě. Organizace proto mohou zavést např. pouze vybrané aspekty ISMS a necertifikovat se. Motivace k takovému jednání je obvykle snaha zlepšit bezpečnostní situaci ve firmě.

V případě oficiální certifikace, postup je schématicky znázorněn na obr. 7.1.



Obrázek 7.1: Proces zavedení ISO 27 000 v organizaci

Celý proces doprovází celá řada dokumentů, organizačních artefaktů apod. Zkusme projít alespoň stručně celý proces krok po kroku.

Celý proces začíná oficiálním rozhodnutím managementu, že organizace zavede ISO 27 000. Toto rozhodnutí obvykle nepřichází samo od sebe - obvykle je iniciováno ze strany pracovníků odpovědných za bezpečnost IT nebo za IT obecně. Toto rozhodnutí je také většinou podpořeno studií s cílem vyčíslit očekávané ekonomické dopady zavedení a nezavedení systému ISMS.

Následuje stanovení definice rozsahu ISMS. Jedná se o krátký dokument (např. 1 str. A4) stanovující obecně, co má řešit ISMS. Má se zaměřit pouze na elektronickou bezpečnost, nebo bude mít

fyzický rozměr (např. ochrana archívu tištěných dokumentů)? Rozsah ISMS je rozpracováván tzv. *politikou ISMS*, která stanovuje základní pravidla řízení informační bezpečnosti v dané organizaci.

Po stanovení rozsahu se provádí inventarizace všech aktiv IT, která mají být předmětem ochrany a jejich riziková analýza. Kromě samotného textu analýzy rizik, jsou v této fázi vytvářeny dokumenty pro vypořádání se s riziky (Risk Treatment Plan (RTP)) a studie aplikovatelnosti (Study of Applicability (SOA)). Úkolem RTP je rozhodnout, co se bude v organizaci s identifikovanými riziky dít (ve smyslu řešit, přenést, akceptovat). Úkolem SOA je pak mapovat dostupné nástroje pro management rizik na jednotlivá rizika.

Na základě výše uvedených dokumentů se zavádí postupně ISMS jako takové - navrhují se jednotlivé procesy a ty se pak postupně zavádí kontrolovaným, plánovaným způsobem. Organizace tak získává postupně kontrolu nad svými procesy mající vazbu na bezpečnost.

Bezpečnostní opatření týkající se různých aspektů bezpečnosti IT zavádíme do závazných vnitropodnikových předpisů, které nazýváme *bezpečnostní politiky IT aktiv*.

Po zavedení ISMS jako takového je spuštěn cyklus Demingův cyklus označovaný někdy také PDCA (plánuj, proveď, zkontroluj, oprav). Úkolem PDCA je zajistit, že postupem času nebude organizace ztrácet kontrolu nad ISMS v důsledku měnícího se prostředí ať už vnitřního nebo vnějšího.

Takový systém je možno již certifikovat.

7.1 Politika ISMS

7.1.1 Obsah politiky ISMS

Jak jsme zjistili již výše slouží *Politika ISMS* k nastavení základních parametrů řízení informační bezpečnosti v organizaci. Pojetí řízení bezpečnosti je v tomto případě obecné. Předpis se proto neorientuje na konkrétní opatření, konkrétních IT aktiv, ale obecných opatření platná pro všechna aktiva. Politika ISMS pak slouží jako podklad pro formulaci bezpečnostních politik konkrétních IT aktiv.

Z hlediska struktury by politika ISMS mohla vypadat následovně:

1. Úvod
2. Slovník pojmů
3. Organizace bezpečnosti (organizační struktury)
4. Role, práva a povinnosti v ISMS
5. Organizace inventarizace aktiv
6. Organizace analýz rizika aktiv
7. Schvalování bezpečnostní dokumentace
8. Bezpečnostní incidenty a jejich řešení
9. Bezpečnostní audit
10. Přechodná a závěrečná ustanovení

V úvodní části se organizace obvykle formou deklarace přihlásí k řešení informační bezpečnosti. Úvodní část zároveň specifikuje dokumenty, na jejichž základě je politika zpracovávána. Obvykle se jedná o Rozsah ISMS, případně Vizi a Misi organizace a normy ISO 27001 a 27002.

Návaznosti na další dokumenty jsou důležité, jelikož ISMS funguje jako celek. Jednotlivé předpisy v řízené dokumentaci by tak měly na sebe vhodně navazovat.

Organizací bezpečnosti se rozumí fyzická organizace bezpečnosti, tedy kdo, za co zodpovídá. Zajímají nás především, která oddělení v dané organizaci se zabývají IT a budou tak nejspíše zodpovědné za organizaci informační bezpečnosti. Jaká je role managementu - schvaluje/kontroluje bezpečnostní předpisy.

Existují klíčové role, skupiny uživatelů, které je potřeba řídit separátně? Základní role pravděpodobně budou administrátor a uživatel. Organizace, ale může obdobných rolí využívat více. Pro takto identifikované role politika ISMS specifikuje základní práva a povinnosti.

Problematika inventarizace aktiv a analýz rizika není v politice ISMS obvykle řešena podrobně. Proto obvykle stačí, že se k inventarizaci a řízení rizik přihlásíme a odkážeme se na další vnitropodnikové předpisy, které tuto problematiku řeší podrobně.

Nastavení procesu schvalování dokumentace řešící bezpečnosti IT je kritickou částí ISMS. Je totiž potřeba si uvědomit, že ISMS nemůže být zavedeno pouze formálně (na papíře) - bezpečnostní opatření proto budou mít praktický dopad. Očekávaný dopad těchto opatření je z hlediska informační bezpečnosti pozitivní, opatření ale mohou mít také řadu dalších sekundárních dopadů na fungování

organizace a práci jejích zaměstnanců. Vyšší úrovně bezpečnosti je dosahováno na úkor poskytovaných služeb - tedy služby omezujeme a svazujeme, aby u nich byla maximalizována bezpečnost do určité míry na úkor užitnosti.

Tyto sekundární dopady mohou být silně pociťovány zaměstnanci, mohou vést k nevoli nebo dokonce k ignorování takových opatření. Aby byl ISMS funkční musí jej dodržovat všichni - ty kteří předpisy poruší je pak možno sankcionovat. Řeší se tak pouze excesy. Pokud se však z excesu stane norma, pozbývají sankce smysl - chyba je systémová v organizaci ISMS. Tomuto stavu je potřeba se vyhnout.

Jako prevenci tohoto typu problémů řada organizací vytváří v rámci svých organizačních struktur platformu, kde tyto problémy je možno včas identifikovat a odstranit je ještě předtím, než předpis vejde v platnost. Tuto platformu lze nazývat různě, např. Rada IT nebo Výbor bezpečnosti IT (nebo jakkoliv jinak). Aby byla taková platforma účinná musí v ní být nominováni zástupci vedená, odpovědné osoby za bezpečnost a provoz IT aktiv a také zástupci významných skupin uživatelů. Platforma musí mít svůj status ať už jako samostatný dokument nebo jako součást dokumentu jiného.

Bezpečnostní incidenty politika ISMS řeší pouze v obecné rovině. Měla by konstatovat, že bezpečnostní incident je potřeba řešit. Řešení by primárně mělo být na garantovi nebo administrátorovi aktiva. Pokud je centralizovaná evidence bezpečnostních incidentů, je potřeba říct kam je potřeba je hlásit, popřípadě se odkázat na patřičný předpis, kde se tato problematika řeší.

Auditní činnost, ať už vnitřní nebo vnější, je také důležitou součástí řízení informační bezpečnosti. V některých případech je explicitně vyžadován audit nezávislé firmy, např. v rámci certifikace organizace na ISO 27000. Ve většině případů však organizace sama rozhoduje, jak bude audity řešit.

Častěji se realizují *audity interní*, realizované vlastními zaměstnanci organizace. Tyto audity jsou relativně levné a mohou proběhnout také rychle, jelikož zaměstnanci jsou již předem seznámeni se způsobem organizace informační bezpečnosti v organizaci. Tato „znalost“ je však zároveň hlavní slabinou interních auditů - interní auditoři mohou totiž trpět provozní slepotou. Tedy současný stav řešení může být akceptován, jako správný bez úvah, zda tomu tak skutečně má být. Interní audity jsou proto schopny odhalit problémy, které jsou především menšího rázu a nebo které jsou do očí bijící.

Externí audit volíme v okamžiku, kdy možnosti interního auditu jsou vyčerpány nebo organizace řeší problém, se kterým zkušenost - např. došlo k novému typu průniku do sítě organizace a je proto potřeba provést audit postižených systémů a způsobů jejich použití, aby se zjistilo, v čem je problém.

Politika ISMS většinou neřeší standardní audity, které se dělají v pravidelných intervalech. Mimořádné audity vyžádané aktuální bezpečnostní situací jsou ale jinou záležitostí. V politice ISMS lze řešit v jakých případech se bude tato forma auditu organizovat a kdo bude na to mít páva.

Přechodná a závěrečná ustanovení jsou součástí většiny předpisů. Ošetřují se pomocí nich situace, kdy např. neexistuje navazující dokumentace. V této části se také často řeší frekvence aktualizací. Politiku ISMS díky její relativně obecnosti není potřeba provádět aktualizace příliš často, přesto je potřeba politiku revidovat v pravidelných intervalech a to i v případech, kdy žádná změna nebude provedena. Účelem je zajistit, aby bezpečnostní dokumentace nezastarávala.

7.1.2 Formulace bezpečností politiky ISMS

Tolik k obsahu politiky ISMS samotné. Problémem při tvorbě politiky ale často není ani tak vytipování, čeho by se měla týkat a jaká opatření přijmout, ale jak zajistit, že stanovená opatření budou skutečně vymahatelná. Existuje několik základních principů, které každá politika (nejen pouze politika ISMS) musí zohlednit:

- adresné odpovědnosti,
- znalosti,
- integrity,
- aktuálnosti a periodického hodnocení,
- úměrnosti

Pokud má být politika vymahatelná, musí být možné spojit uložená opatření s konkrétní osobou. V politice tedy musí být explicitně formulována *odpovědnost*. Z praktických důvodů není možné tuto odpovědnost přímo v textu politiky napsat ke konkrétní osobě, jelikož při každém příchodu/odchodu zaměstnance v organizaci, nebo změně jeho pracovní náplně by bylo nutné revidovat celou bezpečnostní

dokumentaci. To z pochopitelných důvodů není proveditelné. Proto volíme spíše mapování odpovědností na role v řízených systémech nebo funkční zařazení. Mapování samotné funkce/role může být realizováno v samostatném dokumentu, který je jednodušeji aktualizovatelný.

Politiku lze také vymáhat pouze v případě, že všichni lidé s politikou byli prokazatelně seznámeni. Seznámení s předpisy lze řešit různým způsobem. Z hlediska organizačního lze do nějakého základního předpisu zakotvit povinnost seznamovat se z nově vydanými předpisy. Následně se lze na tuto povinnost odkazovat během případných kárných řízeních v organizaci. Povinnost seznámit se však není z praktického hlediska totéž jako skutečně se seznámit. Alespoň na část bezpečnostních předpisů je proto dobré zaměstnance proškolit.

Oba přístupy mohou být účinné, první za předpokladu, že, že dodržování politiky je navíc podpořeno nějakými neformálními metodami, jako je např. gentlemanská dohoda, nebo široce přijímaný konsenzus o způsobu řešení věcí. Školení je proti tomu časově náročné a zaměstnanci jsou často nuceni jej absolvovat v době svého pracovního volna. Na druhou stranu zaměstnanci se v tomto případě skutečně seznámí s probíranou problematikou v požadovaném rozsahu. Volit lze také něco mezi tím, proškolení lze provést formou e-learningu s připojeným testem znalostí apod.

Princip integrity říká, že jednotlivé dokumenty v ISMS nesmí narušovat integritu dalších předpisů - jinak řečeno jeden platný předpis nesmí rušit ustanovení jiného platného předpisu. Nejasnosti ve výkladu a rozpory ve formulacích způsobují obtížnou vymahatelnost sporných ustanovení. Je totiž obtížně zdůvodnitelné, které z nich platí a proč tomu tak je.

Konečně dodržení *principu úměrnosti* by mělo zajistit, že naše úsilí vynaložené na řízení bezpečnosti jednotlivých aktiv bude přímo úměrné významu těchto aktiv pro fungování organizace. Jelikož dostupné množství finančních prostředků určených pro realizaci ochranných opatření je obvykle omezené, je nutné soustředit se na ta opatření, která řeší bezpečnost významných aktiv na úkor aktiv nevýznamných.

Akceptace výše uvedených základních principů tvorby vymahatelných předpisů poskytuje dobrý rámec, o který se lze opřít při návrhu předpisů obecně. Principy samotné by však měly být doprovázeny vhodnými jazykovými formulacemi. Při návrhu předpisů je dobré se vyhnout vágním formulacím s nejasným dopadem.

Při formulaci politik proto používáme formulace typu *musí* pro stanovení povinnosti a formulace typu *měl by*, pro stanovení doporučeného, zároveň ale nevymahatelného postupu. Srovnejme následující formulace a jejich dopady:

1. Identita návštěvníka je kontrolována při vstupu do areálu organizace
2. Návštěvník musí prokázat svou identitu na vrátnici, kde pracovník vrátnice vystaví průkazku návštěvníka ...

Obě formulace řeší stejný problém - vstup do objektu. První konstatuje, že identita je kontrolována při vstupu do areálu - ale co když tam zrovna nikdo nebude? Může návštěvník prostě pokračovat dále? Druhá formulace je mnohem ostřejší. Říká, že návštěvním musí prokázat identitu na vrátnici kde dostane průkaz nutný ke vstupu. To říká, že pokud v areálu podniku bude zjištěn návštěvník bez průkazky, bude se v objektu pohybovat neoprávněně a můžeme s ním podle toho jednat.

Právě popisné věty jsou velmi problematické, protože se jedná o způsob který používáme běžně při konverzaci. Vzdát se tohoto způsobu uvažování je přitom velmi těžké.

Jazykově by pokud možno měly být používány krátké věty, s jasnými formulacemi, jejichž výklad je jednoznačný. Toto se zdá být jasným požadavkem, pravdou však je, že většina jazyků je formulačně natolik bohatá, že jednu větu lze v různých kontextech vykládat různě. Čeština je v tomto ohledu obzvláště bohatá, takže bychom se při psaní dokumentů tohoto typu měli krotit.

7.2 Bezpečnostní politika IT aktiva

Strukturálně je politika IT aktiva podobná politice ISMS, ovšem s tím, že stať předpisu je většinou podstatně konkrétnější a lze jej proto pouze velmi obtížně specifikovat obecně. Základní struktura by mohla vypadat následovně:

- Úvod
- Slovník pojmů
- Stať předpisu
  - Role, práva a povinnosti v aktivu

  - Specifická ustanovení týkající se provozu aktiva
  - Řešení bezpečnostního incidentu aktiva
- Přechodná a závěrečná ustanovení

V úvodní části politiky je potřeba se přihlásit k řešení bezpečnosti IT daného aktiva. Z úvodních vět by mělo jasně vyplynout, co hodláme řešit a proč. Úvod by měl jasně určit, komu je předpis určen, kdo tedy podle něj má postupovat.

Součástí úvodní části je taktéž specifika předpisů a norem, podle kterých se postupuje. Z předpisů se obvykle odkazuje politika ISMS, z norem pak ISO 27 001 a 27 002.

Jednoznačnosti výkladu vždy pomáhá existence slovníku pojmů, kde jsou ustanoveny definice výrazů použitých v politice. Jak jsme již probírali během výkladu politiky ISMS je jednoznačný výklad základním kamenem vymahatelnosti předpisu. Existence slovníku pojmů v tomto úkolu může výrazně pomoci.

Stať samotná se liší podle toho, co přesně se řeší. Může obsahovat podmínky konfigurace, postupy nakládání s aktivem, může ale řešit také věci jako je vytváření/rušení uživatelských účtů v systému nebo cokoliv dalšího.

Formulace v této části by měly následovat doporučení principů a doporučení z předchozí kapitoly.

Přechodná a závěrečná ustanovení by měla obsahovat kromě možnosti běžné aktualizace také možnost aktualizace mimořádné, např. jako reakci na závažný bezpečnostní incident.

7.3 Případová studie Politiky ISMS

Následující případová studie je vytvořena pro smyšlený podnik XYZ. Jedná se o stručnou verzi politiky, kterou by bylo možné výrazně rozvinout - to ale není účelem této studie. Účelem v tomto případě je demonstrovat vzájemnou provázanost jednotlivých pasáží a také jazykové zpracování, které pro vymahatelnost politiky hraje významnou roli.

Jednotlivé pasáže politiky jsou doplněny komentáři. Pro odlišení textu studie a komentáře k ní jsou komentáře v textu sázeny kurzívou.

7.3.1 Úvod

Touto politikou vyjadřuje společnost XYZ konzistentně zajišťovat bezpečnost svých aktiv manipulující s informacemi v jakékoliv podobě (elektronické, papírové podobě, nebo na jakémkoliv jiném nosiči informací).

Politika řeší organizaci bezpečnosti, základní bezpečnostní postupy ve společnosti XYZ a je určena všem zaměstnancům organizace. Politika vstupuje v platnost dnem jejích zveřejnění v registru vnitřních předpisů XYZ[1]

Systém ISMS ve formě XYZ vychází z ustanovení norem ISO 27001 a ISO 27002.

Komentář

Z hlediska typografického obvykle úvod není číslován - v tomto případě, je číslo přiděleno k úvodu pouze z důvodu, že je součástí skript. Alternativně lze k úvodu dát číslo 0 - to je způsob, který je někdy používán v USA. V případě formulace politiky ISMS jako součásti semestrálního projektu nebo jiného širšího dokumentu je potřeba rozlišovat mezi úvodem tohoto dokumentu (semestrálního projektu) a úvodem politiky ISMS jako takové. Uvedení např. do organizace, kterou ISMS politika řeší, může být v rámci semestrálního projektu přínosná. Tento úvod ale nemůže nahradit úvod politiky ISMS.

Z hlediska obsahu samotného se prostě hlásíme k řešení problematiky IT bezpečnosti, říkáme co se řeší a koho se to týká a také na základě čeho je politika sestavena.

7.3.2 Slovník pojmů

- **administrátor** - správce IT
- **aktivum** - informační systémy, hardware, software, komunikační prostředky a další zařízení, která manipulují s informacemi a mají pro společnost nějakou hodnotu.
- **bezpečnostní incident** - jakékoliv porušení integrity dat nebo postupů stanovených v systému ISMS

[1] http://portal.xyz.cz/predpisy/ - portál vnitropodnikových předpisů.

- **garant** - osoba zodpovědná za IT aktivum
- **IS** - informační systém
- **IT** - informační technologie

Komentář

Výše uvedený výčet pojmů by ve skutečnosti mohl být podstatně větší. Do slovníku volíme takové pojmy, které používáme v politice, a jejichž definice nemusí být jasná. Slovník pojmů tedy není samostatně použitelný, pouze nám definuje kontext, ve kterém má politika fungovat. Dále na začátku práce nemusí být úplně očividné, které pojmy mají být zavedeny do slovníku pojmů. Proto může být potřeba se k formulaci slovníku pojmů průběžně vracet, tak jak se budou pojmy objevovat v textu.

Slovník pojmům také umožňuje „neodborníkům" vyznat se v používaných pojmech a zkratkách a přispívá tak k lepší pochopitelnosti (a také vymahatelnosti dokumentu).

7.3.3 Bezpečnostní politika

Bezpečnostní dokumentace IT

Dokument vytváří závazný podklad pro řízení informační bezpečnosti systémem ISMS. Systémem ISMS se přitom rozumí systém formalizovaných procesů, pravidel a postupů, které mají vazbu na řízení bezpečnosti informací ve firmě. Tyto jsou zachyceny ve vnitropodnikových předpisech, které jsou souhrnně označovány jako bezpečnostní dokumentace IT.

Bezpečnostní dokumentace IT musí zahrnovat celý životní cyklus řízeného aktiva od jeho vytvoření nebo pořízení až do doby jeho vyřazení z používání v rámci organizace. Garantem informační bezpečnosti v organizaci je **bezpečnostní ředitel.**

Bezpečnostního ředitele jmenuje a odvolává generální ředitel společnosti.

V rámci životního cyklu aktiva jsou požadavky na informační bezpečnost různé, z tohoto důvodu se rozlišuje:

1. projektová bezpečnostní dokumentace - řídící významné změny v systémech společnosti s potenciálem významných dopadů do bezpečnosti informací
2. provozní bezpečnostní dokumentace - nastavuje procesy použití IT aktiv ve společnosti během běžného provozu

Projektová bezpečnostní dokumentace řeší zabezpečení IT aktiv v souvislosti se zásadní změnou, kterou podstupují. Takovou změnou může být pořízení významného informačního systému, migrace klíčových dat do nového úložiště apod. Předmětem zájmu systému ISMS jsou veškeré změny, které mohou mít dopad na bezpečnost informací v organizaci.

Každý projekt musí mít stanoveného garanta, který je zodpovědný za bezpečnostní aspekty realizace projektu včetně zpracování bezpečnostní dokumentaci projektu a také dozorem nad jejím dodržováním.

Garanta projektu jmenuje vedoucí útvaru, v jehož vlastnictví je nebo bude výsledek projektu.

Provozní bezpečnostní dokumentace je zaměřena na ošetření bezpečnostních aspektů rutinního provozu aktiva IT. Provozní bezpečnostní dokumentace má charakter předpisu orientovaného na specifikaci schválených, bezpečných postupů nakládání s aktivem, orientované primárně na koncového uživatele a administrátora aktiva.

Garantem provozní bezpečnosti je administrátor aktiva. Administrátora aktiva jmenuje vedoucí útvaru, který má dané aktivum ve správě. Administrátor je zodpovědný za kontrolu dodržování ustanovení bezpečnostní dokumentace a její případné revize.

Při jmenování administrátora aktiva nebo garanta projektu musí osoba jmenující poskytnout informaci o jmenování managerovi bezpečnosti, který ji zaznamená do seznamu administrátorů a garantů.

Bezpečnostní politika obsahuje povinné („musí") a nepovinné („měl by") části. Povinné části musí být dodržovány všemi dotčenými osobami. Části volitelné mohou být dále upravovány dle potřeb administrátorem aktiva.

Bezpečnostní dokumentace podléhá revizím, jejichž frekvenci stanovuje administrátor aktiva. Revize obvykle probíhá 1x ročně, pokud bezpečnostní dokumentace nestanovuje jinou frekvenci.

Bezpečnostní dokumentace musí být revidována také v případě, že:

- došlo k velkým změnám v technologiích, které platná bezpečnostní dokumentace nezohledňuje nebo

- byl zaznamená nový typ bezpečnostní hrozby/útoku, který bezpečnostní dokumentace neřeší.

Komentář

Pro bezpečnostní politiku se nemusí používat pouze název - bezpečnostní politika. Pojmenovávání odpovídá vnitroorganizačním zvyklostem - lze proto použít označení jako předpis pro nakládání ..., provozní řád, proces obsluhy ..., bezpečnostní dokumentace... Pojmenování by však mělo být konzistentní napříč celou předpisovou bází ISMS.

ISO 27000 je založeno na procesu PDCA. Prakticky to znamená, že celá dokumentace musí být v pravidelných intervalech revidována, aby se zajistil soulad mezi ustanoveními politiky a skutečným stavem řešení bezpečnosti informací v organizaci. Periodicita revize v politice ISMS je stanovena ve dvou místech - konkrétně v ustanovení týkající se zpracování bezpečnostní dokumentace a také v závěrečných ustanoveních.

Nastavené lhůty se ale týkají různých problémů - v závěrečných ustanoveních je nastavována frekvence revize politiky ISMS samotné, v části věnované bezpečnostní dokumentaci je pak nastavena základní revizní perioda dokumentace z politiky ISMS odvozené - např. bezpečnostní politiky jednotlivých aktiv.

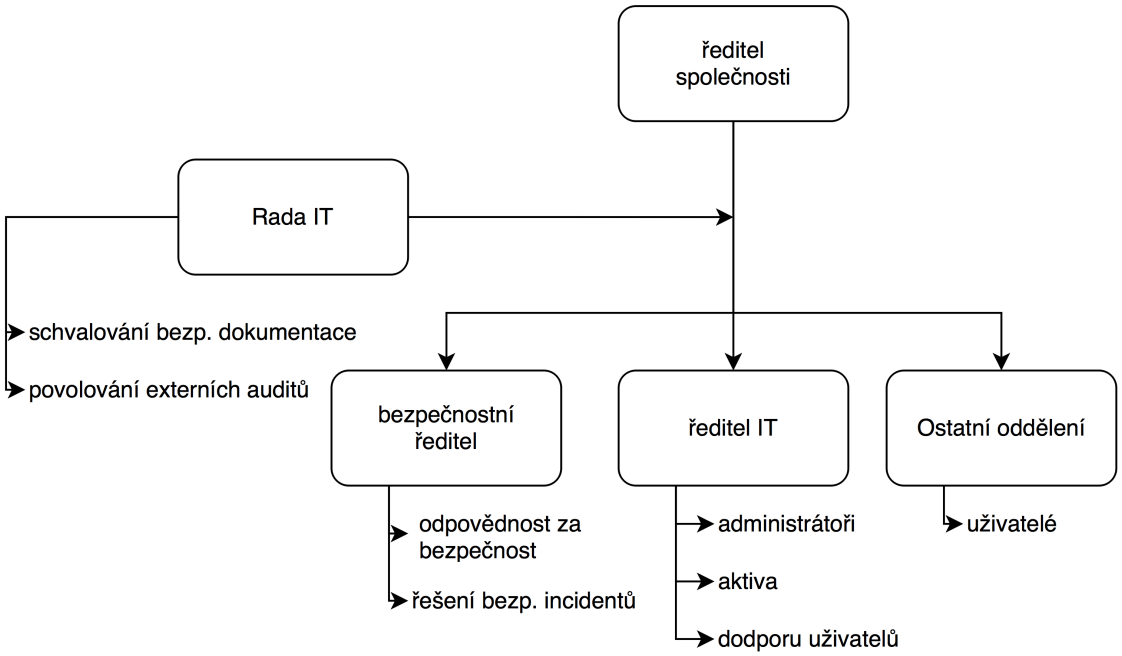
7.3.4 Organizace informační bezpečnosti

Bezpečnostní ředitel

Manager bezpečnosti zodpovídá za celkové řešení bezpečnosti informací ve smyslu *Rozsahu ISMS*[2]. Bezpečnostního ředitele jmenuje a odvolává generální ředitel společnosti.

Bezpečnostní ředitel vede oddělení Informační bezpečnosti (viz obr. 7.2). Je zodpovědný především za:

- přípravu a schvalování bezpečnostní dokumentace a posuzuje návrhy na její změny
- koordinaci zavádění bezpečnostních opatření
- koordinaci za šetření bezpečnostních incidentů
- udržování seznamu aktiv a administrátorů, kteří je spravují



Obrázek 7.2: Organizace informační bezpečnosti ve společnosti XYZ

Bezpečnostní ředitel předkládá Bezpečnostní radě IT zprávu o bezpečnosti IT za uplynulý rok. Bezpečnostní ředitel je také povinen informovat neprodleně Bezpečnostní radě IT, pokud dojde k

[2]předpis ABCD:2015 - Rozsah ISMS

závažnému bezpečnostnímu incidentu, především v případech, kdy došlo k úniku obchodního tajemství společnosti nebo úniku osobních údajů.

Bezpečnostní rada IT

Bezpečnostní rada IT slouží jako poradní orgán ředitele společnosti v otázkách bezpečnosti IT. Bezpečnostní rada rozhoduje ve sboru. Bezpečnostní radu tvoří:

- zástupci všech útvarů (nominuje vedoucí útvaru),
- ředitel bezpečnosti
- zástupce nejvyššího managementu (nominuje ředitel společnosti).

Bezpečnostní rada IT úzce spolupracuje s bezpečnostním ředitelem v otázkách bezpečnosti, schvaluje zprávu o bezpečnosti IT. Bezpečnostní rada má právo požadovat doplnění zprávy.

Bezpečnostní výbor také projednává a schvaluje bezpečnostní politiky aktiv IT společnosti. Jednotliví členové rady mohou dle vlastního uvážení seznamovat s navrhovanými politikami i ostatními záležitostmi projednávanými v radě další zaměstnance společnosti. Při předávání informací však nesmí být ohrožena důvěrnost informací nebo vyzrazeny osobní údaje osobám neoprávněným s takovými údaji manipulovat.

Administrátor aktiva

Každé aktivum musí mít stanoveného svého administrátora. Administrátora aktiva jmenuje a odvolává vedoucí útvaru, který má aktivum ve svém vlastnictví. Administrátor v rámci jmenovacího procesu musí být nahlášen bezpečnostnímu řediteli včetně informace o aktivu (aktivech), která administruje. Bezpečnostní ředitel je povinen tuto informaci zaevidovat do seznamu aktiv a jejich administrátorů.

Administrátor odpovídá:

- za bezpečný provoz aktiva
- jeho údržbu
- řešení bezpečnostních incidentů aktiva

Administrátor shromažďuje požadavky uživatelů na změny v jím spravovaném systému a navrhuje změny bezpečnostní politiky aktiva, které reagují na aktuální požadavky uživatelů a bezpečnostní hrozby.

Uživatelé

Uživatelé jsou povinni dodržovat ustanovení bezpečnostních politik. Nedodržení ustanovení bezpečnostních politik bude posuzováno dle závažnosti jako porušení pracovní kázně. O formě a velikosti trestu rozhoduje vedoucí v souladu s ustanoveními zákoníku práce na základě dokumentaci o bezpečnostním incidentu, za který je daný uživatel odpovědný.

Komentář

Pro formulaci politik obvykle doporučuji vzít jako základ platnou legislativu a v politice pak řešit pouze odchylky, které nelze automaticky předpokládat, nebo způsoby jakými má být dosaženo souladu s legislativním předpisem. Někde mezi těmito dvěma případy je odkaz na zákoník práce v předchozím odstavci. Za normálních okolností bychom se obešli bez odkazu, protože logicky trest nesmí být v rozporu s zákoníkem práce. Odkaz jsem tam přidal pouze kvůli „vyznění“ věty - aby po přečtení nevznikaly nevhodné asociace apod.

Jinak celá tato část politiky je věnována řešení organizaci bezpečnosti. Organizační struktury jsou vysoce závislé na vnitropodnikové kultuře, ve smyslu pojmenování, rozdělení odpovědností, způsobu schvalování předpisů apod. Politika může být doplněna organizačním schématem (ať už přímo v textu nebo v příloze dokumentu), toto schéma by však nemělo být obecným organizačním schématem - mělo by se zaměřit na složku IT - kterou hodláme z hlediska bezpečnosti řídit.

7.3.5 Aktiva a jejich bezpečnost

Inventarizace aktiv

Úspěšné řízení informační bezpečnosti vyžaduje získání kontroly nad všemi aktivy, která manipulují s informacemi řízenými v rámci ISMS. Všechna tato aktiva musí být správně evidována a přiřazena k vhodnému typu aktiva. Za provedení evidence a zajištění její aktuálnosti odpovídá vedoucí útvaru, který aktivum vlastní.

Proces inventarizace aktiv probíhá v rozsahu a frekvenci stanoveným specializovaným předpisem [3].

Riziková analýza aktiv

Pro všechna aktiva, která mají vliv na bezpečnost informací řízených v rámci ISMS je nutné zpracovat analýzu rizik. Pro každé riziko je pak nutné přijmout rozhodnutí o vypořádání se s ním a tyto informace pak použít pro formulaci bezpečnostní politiky aktiva.

Rizikovou analýzu aktiva provádí v součinnosti s administrátorem aktiva a bezpečnostním ředitelem majitel aktiva, v souladu s ustanoveními specializovaného předpisu [4].

Komentář

Politika ISMS řeší problematiku řízení informační bezpečnosti v organizaci v obecné rovině. Může proto zmiňovat další procesy, které na tuto problematiku mají návaznost, neměla by je ale řešit podrobně. V případě, že v dokumentaci taková vazba existuje, je vhodné do politiky přidat odkaz na předpis, který se danou problematikou zabývá podrobně. V našem příkladu politiky je tomu tak jak v případě inventarizace aktiv, tak v případě rizikových analýz.

7.3.6 Závěrečná ustanovení

Tato politika vstupuje v platnost dnem jejího podepsání managerem bezpečnosti a jejím zveřejněním na portálu vnitropodnikové dokumentace.

Tato politika musí být revidována minimálně 1x ročně. O provedení revize a případných změnách se provede záznam v systému řízené dokumentace společnosti.

7.4 Případová studie Bezpečnostní politiky IT aktiva

Komentář

Bezpečnostní politika v tomto případě byla navržena pro systém řízení dokumentů ve firmě.

7.4.1 Úvod

Dokumenty a jejich oběh ve společnosti jsou základním stavebním kamenem fungování organizace. Společnost XYZ se proto rozhodla řídit bezpečnost těchto dokumentů a systémů používaných k řízení jejich oběhu.

Tato politika vychází z Politiky ISMS podniku a ISO 27 002.

Politika formuje základní závazná pravidla pro nakládání s dokumenty v automatizovaných systémech s těmito dokumenty nakládajícími.

7.4.2 Definice a pojmy

- **administrátor** - správce IT
- **autorizace** - důkaz potvrzení totožnosti uživatele
- **DMS** - dokument management system (Systém řízení dokumentů)
- **LDAP** - Lightweight directory access protocol - protokol používaný k ověření identity uživatele

Komentář

Úvodní část a slovník pojmů je velmi podobná jako v případě politiky ISMS. Ostatní části politiky se ale budou výrazně lišit, jelikož zbývající části musí být úžeji zaměřeny na problematiku ochrany vybraného aktiva.

[3] viz předpis 666890:2015 - Inventarizace aktiv společnosti v systému ISMS

[4] viz předpis 44441234:2015 - Řízení rizika IT aktiv v systému ISMS

7.4.3 DMS

Základním úkolem DMS je spravovat dokumenty tak, aby byla zajištěna integrita (dokumenty jsou dostupné pouze v autoritativní - formě), aktuálnost (dokumenty v poslední platné verzi) a neodvolatelnost dokumentů (není možné zpochybnit existenci a autorství dokumenty) evidovaných v DMS.

Z tohoto důvodu DMS musí být nastaven tak, aby zabránil anonymnímu použití - tedy buď bez autentizace nebo s využitím účzu host. Práva všech uživatelů musí být nastavena tak, aby jednotliví uživatelé měli pouze práva k dokumentům, se kterými jsou oprávněni pracovat z titulu své funkce.

Za správu uživatelských účtů je odpovědný administrátor systému DMS. Administrátor vytváří, přenastavuje a ruší uživatelské účty na základě písemné žádost v papírové, nebo elektronicky podepsané elektronické verzi zpracované vedoucím zaměstnancem oddělení, kde uživatel, jehož práva se řeší, pracuje. Nově navedenému zaměstnanci administrátor musí přidělit přístup do složky útvaru žadatele.

Přístup k složkám dalších útvarů se přiděluje na základě žádosti podepsané vedoucím útvaru jehož prostor má být zpřístupněn. Žádost zároveň v obou výše uvedených případech musí obsahovat požadovanou úroveň práv uživatele, které mají být přiděleny.

Přidělování práv k prostoru přiděleným projektům provádí administrátor na základě žádosti uživatele potvrzené projektovým manažerem.

Formuláře žádostí o přidělení práv a jejich změnu jsou dostupné v přílohách 1 - 3.

7.4.4 Organizace systému DMS

Administrátor

- provádí správu uživatelů a jejich práv k dokumentům
- provádí údržbu DMS
- zajišťuje řešení bezpečnostních incidentů ve spolupráci s podnikovým ředitelem bezpečnosti

Jednotlivé úkoly spojené se správou administrátor obvykle provádí neprodleně (do 1 pracovního dne) po vzniku potřeby zásahu. V odůvodněných případech, kdy není možno tento termín dodržet, je administrátor o této skutečnosti povinen vyrozumět osoby, kterých se požadovaný zásah týká.

Vedoucí útvaru

Vedoucí útvaru má povinnost posoudit a v odůvodněných případech schválit žádost o navýšení práv k dokumentům nebo prostoru, který přináleží útvaru vedoucího. Schválenou žádost je povinen vedoucí útvaru elektronicky podepsat a zaslat na oficiální e-mailovou adresu administrátora systému DMS získané ze seznamu administrátorů aktiv ze své pracovní e-mailové adresy.

Vedoucí útvaru má právo na to, aby jím schválená žádost byla neprodleně vyřízena nebo aby mu bylo neprodleně sděleno, že žádosti není možné vyhovět a také důvod zamítnutí žádosti. V případě, že žádosti není možno vyhovět, má vedoucí právo se dozvědět přibližný termín vyřízení žádosti.

Komentář

Příkazy a požadavky je v politice dobré vyvažovat. Příkazy nutíme uživatele dělat něco, co by možná nedělal. Pokud tuto skutečnost vyvážíme právy na služby - tedy pokud se bude určitým způsobem chovat, přinese mu to ty a ty výhody - mohou být ochotnější se těmito pravidly řídit.

Vedoucí projektu

Vedoucí projektu má povinnost zajistit ve spolupráci s administrátorem systému DMS, aby všichni účastníci projektu měli přístup ke všem projektovým dokumentům, které jsou potřebné pro výkon jejich práce na projektu.

Přidělování práv zajišťuje vedoucí projektu zprostředkovaně přes administrátora systému DMS pomocí elektronicky podepsaných žádostí o přidělení práv k dokumentům.

Vedoucí projektu má právo na to, aby jím schválená žádost byla neprodleně vyřízena nebo aby mu bylo neprodleně sděleno, že žádosti není možné vyhovět a také důvod zamítnutí žádosti. V případě, že žádosti není možno vyhovět, má vedoucí právo se dozvědět přibližný termín vyřízení žádosti.

Uživatel

Uživatel má právo získat přístup ke všem dokumentům, které které jsou vyžadovány pro odpovědné plnění pracovních povinností jako zaměstnance společnosti. O přidělení přístupových práv k

dokumentům musí uživatel žádat prostřednictvím vedoucího útvaru, o jehož přístup k dokumentům žádá.

Uživatel má povinnost hlásit se do systému DMS pomocí vlastního uživatelského jména a heslo. Své heslo musí uživatel udržovat v tajnosti a minimálně 2x ročně provést jeho změnu.

Při nakládání s dokumenty uživatel dbá, aby všechny změny, které v dokumentech prováděl byly pravdivé a odpovídaly stavu řešené problematiky v čase jejího řešení.

7.4.5 Závěrečná ustanovení

Tato politika musí být revidována minimálně 1x ročně nebo při realizaci velkých změn v systému DMS nebo zjištění významného bezpečnostního incidentu, který systém DMS postihl.

Revizi politiky provádí administrátor DMS systému.

7.4.6 Přílohy

Komentář

Do příloh je možné vložit podpůrné materiály nebo formuláře. Vzhled formulářů autor ponechává na fantazii čtenáře.

Literatura

[1] *Acronis TrueImage 2016* [online]. [cit. 2015-09-17]. Dostupné z: http://www.acronis.cz/domacnosti-a-kancelare/produkty/

[2] *Asus unveils a monster of a Wi-Fi router, the RT-AC5300* [online]. [cit. 2015-09-4]. Dostupné z: http://www.cnet.com/products/asus-rt-ac5300u-router/

[3] *Backblaze Online Backup* [online]. [cit. 2015-09-18]. Dostupné z: https://www.backblaze.com

[4] *Carbonite* [online]. [cit. 2015-09-18]. Dostupné z: http://www.carbonite.com/

[5] *CESNET Komunikační infrastruktura* [online]. [cit. 2015-06-17]. Dostupné z: http://www.cesnet.cz/e-infrastruktura/komunikacni/

[6] *CipherShed | Secure Encryption Software* [online]. [cit. 2015-09-7]. Dostupné z: https://ciphershed.org/

[7] *Clonezilla* [online]. [cit. 2015-09-17]. Dostupné z: http://clonezilla.org/

[8] *Data Trescor Disc* [online]. [cit. 2015-09-17]. Dostupné z: http://www.datatresordisc.cz/

[9] *DVD-R Information* [online]. [cit. 2015-09-17]. Dostupné z: http://www.cd-info.com/dvd/dvd-r/index.html

[10] *Fujitsu Lifebook S935: Notebook, který vám čte z ruky /test/* [online]. [cit. 2015-09-11]. Dostupné z: http://www.zive.cz/clanky/fujitsu-lifebook-s935-notebook-ktery-vam-cte-z-ruky-test/sc-3-a-177545/default.aspx

[11] *FVC-onGoing: on-line evaluation of fingerprint recognition algorithms* [online]. [cit. 2015-09-11]. Dostupné z: https://biolab.csr.unibo.it/FVCOnGoing/UI/Form/Home.aspx

[12] *Galaxy S5 fingerprint scanner can easily be fooled, hacked* [online]. [cit. 2015-09-10]. Dostupné z: http://www.techspot.com/news/56406-galaxy-s5-fingerprint-scanner-can-easily-be-fooled-hacked.html

[13] *ISO/IEC 27 000 Information technology - Security techniques - Information security management systems - Overview and vocabulary* [online]. [cit. 2015-09-28]. Dostupné z: http://standards.iso.org/ittf/PubliclyAvailableStandards/c063411_ISO_IEC_27000_2014.zip.

[14] *John the Ripper benchmarks* [online]. [cit. 2015-09-9]. Dostupné z: http://openwall.info/wiki/john/benchmarks

[15] *Lenovo ThinkPad T430* [online]. [cit. 2015-09-10]. Dostupné z: http://shop.lenovo.com/us/en/laptops/thinkpad/t-series/t430s/

[16] *Online Data Backup - Offsite, Onsite, & Cloud - CrashPlan Backup Software* [online]. [cit. 2015-09-18]. Dostupné z: http://www.code42.com/crashplan/

[17] *Ova.net* [online]. [cit. 2015-06-17]. Dostupné z: http://www.ovanet.cz/

[18] *Paragon Backup & Recovery 2014* [online]. [cit. 2015-09-17]. Dostupné z: https://www.paragon-software.com/home/br-free/

[19] *RAID 0 with two disks (disk 0 and disk 1) over one logical volume A with odd blocks on disk 0 and even blocks on disk 1* [online]. [cit. 2015-09-18]. Dostupné z: https://cs.wikipedia.org/wiki/RAID#/media/File:RAID_0.svg

[20] *RAID 1 with two disks (disk 0 and disk 1) over one logical volume A with all blocks replicated/mirrored from drive 0 to drive 1* [online]. [cit. 2015-09-18]. Dostupné z: https://cs.wikipedia.org/wiki/RAID#/media/File:RAID_1.svg

[21] *RAID 5 with these four disks (disk 0, 1, 2, and 3) and each group of blocks (orange, yellow, green, and blue) have a distributed parity block that is distributed across the four disks.* [online]. [cit. 2015-09-18]. Dostupné z: https://cs.wikipedia.org/wiki/RAID#/media/File:RAID_5.svg

[22] *RFC 1918 - Address Allocation for Private Internets* [online]. [cit. 2015-06-19]. Dostupné z: https://tools.ietf.org/html/rfc1918

[23] *Touch ID* [online]. [cit. 2015-09-10]. Dostupné z: http://iphonovky.blog.cz/1408/touch-id

[24] *True Crypt* [online]. [cit. 2015-09-7]. Dostupné z: http://truecrypt.sourceforge.net/

[25] V*eraCrypt* [online]. [cit. 2015-09-7]. Dostupné z: https://veracrypt.codeplex.com/Wikipage?ProjectName=veracrypt

[26] *Veracrypt or Ciphershed?* [online]. [cit. 2015-09-7]. Dostupné z: http://forum.truecrypt.ch/t/veracrypt-or-ciphershed/449

[27] *Wifi Analyzer* [online]. [cit. 2015-09-3]. Dostupné z: https://play.google.com/store/apps/details?id=com.farproc.wifi.analyzer

[28] *Wikileaks* [online]. [cit. 2015-09-21]. Dostupné z: https://wikileaks.org/index.en.html

[29] *CD and DVD writing speed* [online]. [cit. 2015-09-17]. Dostupné z: https://en.wikipedia.org/w/index.php?title=CD_and_DVD_writing_speed&oldid=653495926

[30] *RSA SecurID* [online]. [cit. 2015-09-10]. Dostupné z: https://en.wikipedia.org/w/index.php?title=RSA_SecurID&oldid=674333656
[31] *ZTE Grand S3 Release Date, News, Price and Specs* [online]. [cit. 2015-09-11]. Dostupné z: http://www.cnet.com/products/zte-grand-s3/
[32] BOUŠKA, Petr. *Víte, jak pracuje switch?* [online]. [cit. 2015-06-18]. Dostupné z: http://www.samuraj-cz.com/clanek/vite-jak-pracuje-switch/
[33] CUMMINGS, Adam et al. *Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector* [online]. Pittsburgh: Software Engineering Institute, 2012. 76 s. [cit. 2015-09-24]. Dostupné z: https://resources.sei.cmu.edu/asset_files/SpecialReport/2012_003_001_28137.pdf.
[34] ELCOMSOFT. *Ecomsoft News 2015-06-24* [online]. [cit. 2015-09-9]. Dostupné z: https://www.elcomsoft.com/news/606.html
[35] FUJITSU. *PalmSecure® Mouse* [online]. [cit. 2015-09-10]. Dostupné z: http://www.fujitsu.com/us/solutions/business-technology/security/palmsecure/psmouse/
[36] FUJITSU. *Fujitsu Releases ARROWS NX F-04G* [online]. [cit. 2015-09-11]. Dostupné z: http://www.fujitsu.com/global/about/resources/news/press-releases/2015/0525-01.html
[37] GARYLPARAS. *Linksys WAP54G Wireless-G Access Point_Basic Configuration*.
[38] KOVANDA, Lukáš. *Génius John Nash nemohl ani zemřít normálně* [online]. [cit. 2015-09-20]. Dostupné z: http://finmag.penize.cz/kaleidoskop/300588-genius-john-nash-nemohl-ani-zemrit-normalne
[39] MEITIV, Alexander Lobkovsky. *Are Android unlock patterns as secure as numeric PINs?* [online]. [cit. 2015-09-8]. Dostupné z: https://playingwithmodels.wordpress.com/2010/04/14/andorid_unlock_patterns/
[40] MITNICK, Kevin, SIMON, Wiliam L. *Umění klamu*. Praha: HELION, 2003. 348 s. ISBN 83-7361-210-6.
[41] PATRICK, Andrew S. *Fingerprint Concerns: Performance, Usability, and Acceptance of Fingerprint Biometric Systems* [online]. [cit. 2015-09-11]. Dostupné z: http://www.andrewpatrick.ca/essays/fingerprint-concerns-performance-usability-and-acceptance-of-fingerprint-biometric-systems/
[42] PETERKA, Jiří. *Nové e-občanky, co nejsou „e“* [online]. [cit. 2015-09-10]. Dostupné z: http://www.lupa.cz/clanky/nove-e-obcanky-co-nejsou-e/
[43] QNAP. *TVS-671* [online]. [cit. 2015-09-2]. Dostupné z: https://www.qnap.com/i/en/product/model.php?II=159
[44] RETANA, Michael Q. *Iris recognition* [online]. [cit. 2015-09-11]. Dostupné z: https://en.wikipedia.org/wiki/Iris_recognition#/media/File:USMC_Sergeant_identifies_Baghdaddi_city_council_member_with_iris_scanner.jpg
[45] SVĚT SÍTÍ. *Základy počítačových sítí* [online]. [cit. 2006-02-23]. Dostupné z: http://svetsiti.cz
[46] SYMANTEC. *Introducing Symantec Northon Ghost Solution Suite 3.0* [online]. [cit. 2015-09-17]. Dostupné z: http://www.symantec.com/page.jsp?id=ghost
[47] VŠB-TECHNICKÁ UNIVERZITA OSTRAVA. *Studentský průkaz* [online]. [cit. 2015-09-10]. Dostupné z: http://www.vsb.cz/9870/cs/kartove-centrum/prukaz-studenta/
[48] ŠENOVSKÝ, Pavel. *Bezpečnostní informatika 1* [online]. 7 vyd. Ostrava: VŠB-TU Ostrava, Fakulta bezpečnostního inženýrství, 2015. 120 s. [cit. 2015-09-25]. Dostupné z: http://homel.vsb.cz/~sen76/CMS/data/uploads/skripta/bi1_7ed_fin.pdf.

Slovník

AD Active Directory.

AP Access Point.

BD Blu-ray Disc.

CD Compact Disc.

CTU Český telekomunikační úřad.

DDoS Distributed Denial of Services.

DHCP DynamicHost Cache Protocol.

DMZ Demilitarizovaná zóna.

DNS Domain Name Server.

DoS Denial of Services.

DTP Desktop publishing.

DVD Digital Versatile Disc.

EAP Extensible Authentication Protocol.

FAR False Acceptance Rate.

FIFO First In First Out.

FMR False Match Rate.

FNMR False Non-Match Rate.

FRR False Rejection Rate.

FVC Fingerprint Verification Competition.

GUI Graphical User Interface.

HDD Hard Disc Drive.

HPKR Havarijní plánování a krizové řízení.

IDM Identity Management System.

IDS Intruder Detection System.

IPS Intruder Prevention System.

ISMS Information Security Management System.

LAN Local Area Nework.

LDAP Lightweight Directory Access Protocol.

MAC Media Access Control.

MAN Metropolitan Area Network.

NAS Network Attached Storage.

NAT Network Address Translation.

NFS Network File System.

PDF Portable Document Format.

PEAP Protected EAP.

RAID Redundant Array of Independent Discs.

RPC Remote Procedure Call.

RTP Risk Treatment Plan.

S.M.A.R.T. Self-Monitoring, Analysis, and Reporting Technology.

SOA Study of Applicability.

SQL Structured Query Language.

SSD Solid State Disc.

SSID Service Set Identifier.

SSO Single-Sign On.

STP Shielded Twisted Pair.

TAR True Acceptance Rate.

TBOM Technická bezpečnost osob a majetku.

TMR True Match Rate.

TNMR True Non-Match Rate.

TRR True Rejection Rate.

UTP Unshielded Twisted Pair.

VPN Virtual Private Network.

WAN Wide Area Network.

WEP Wired Equivalent Privacy.

WPA Wi-Fi Protected Access.

[title=Seznam zkratek]

Rejstřík

čipová karta, 39
šifrování, 32
    Bitlocker, 32
    CipherShed, 32
    True Crypt, 32
    VeraCrypt, 32
žilkování na dlani, 42
802.11ac, 28
802.11n, 28

AD, 44
aplikační server, 22
audit
    externí, 73
    interní, 73
autentizace, 35
    pass fráze, 36
    vlastnictvím, 39
    vlastností, 40
    znalostí, 36
autorizace, 35

baiting, 67
BD, 48
BD-XL, 48

CD, 48
cloud, 49
computer fingerprinting, 17

důvěryhodná zóna sítě, 31
daktyloskopie, 41
DDoS, 63
demilitarizovaná zóna, 30
Demingův cyklus, 72
DHCP, 23
disk image, 51
Diversion theft, 66
DMZ, 30
DNS, 23
DNS cache poisoning, 64
DNS spoofing, 64
DNSSec, 64
DoS, 63
duhová tabulka, 38
DVD, 48

hacker, 58
hacktivista, 58

HDD, 49

identity management, 44
IDM, 44
insider, 59
IP protokol, 19
IPv4, 19
    loopback adresa, 19
IPv6, 19
ISMS, 69
ISO 27 000, 69

kabel
    koaxiální, 15
    kroucená dvojlinka, 16
    optický, 17
    STP, 16
    twisted pair, 16
    UTP, 16
klient, 20
klonování disku, 51

LDAP, 44

MAC adresa, 18

NAS, 22
NAT, 24
nedůvěryhodná zóna sítě, 31
nespojová služba, 20

oční duhovka, 42
oční sítnice, 42
obraz disku, 51
otisk prstu, 41

páskové mechaniky, 49
papilární linie, 41
paritní informace, 52
PDCA, 72
penetrační testování, 58
Phishing, 66
politik ISMS, 72
politika ISMS, 71
pretexting, 66
princip
    úměrnosti, 74
    adresné odpovědnosti, 73
    integrity, 74

znalosti, 74
principy politiky, 73

quid pro quo, 67

RAID, 52
RAID-0, 52
RAID-1, 52
RAID-10, 52
RAID-5, 53
RAID-6, 53
rainbow table, 38
referenční model ISO/OSI, 17
rozsah ISMS, 71

S.M.A.R.T., 54
síťě
token ring, 14
síťová zařízení
bridge, 19
hub, 18
můstek, 19
opakovač, 18
přepínač, 18
repeater, 18
router, 20
směřovač, 20
switch, 18
sítě
hvězdicová topologie, 14
hybridní topologie, 14
LAN, 15
MAN, 15
topologie, 13
WAN, 15
server, 20
databázový, 22
souborový, 22
WWW, 22
slabé heslo, 37
slovníkový útok, 38
sociální inženýrství, 66
solení hesla, 38
spojová služba, 20
SQL injection, 65
SSD, 49
SSID, 30
SSO, 45
strojově čitelné údaje, 39

tailgating, 67
TCP, 20
tiskový server, 22
token, 39
topologie
sběrnicová, 13

UDP, 20

vishing, 67
vnější perimetr sítě, 27
vnitřní perimetr sítě, 30
VPN, 28
vrstvy sítě
aplikační, 20
fyzická, 18
linková, 18
přenosová, 20
prezentační, 20
siťová, 19
spojová, 20

WEP, 30
whistle blower, 59
Wi-Fi, 28
WPA, 30
WPA2, 30

záloha
úplná, 50
inkrementální, 50
zálohování, 47
zálohovací strategie, 47