doc. Ing. Pavel Šenovský, Ph.D.

Počítačové sítě a ochrana dat

skripta, 2. vydání

Ostrava, 2023

Počítačové sítě a ochrana dat, 2. vydání
tento text neprošel jazykovou úpravou
©Pavel Šenovský, Ostrava, 2023
Vysoká škola báňská - Technická univerzita Ostrava, Fakulta bezpečnostního inženýrství

Obsah

Seznam obrázků

Seznam tabulek

Úvod

Vážený studente, dostává se Vám do rukou učební text předmětu *Počítačové sítě a ochrana dat*. Tento text je především určen studentům třetího, popř. čtvrtého ročníku Fakulty bezpečnostního inženýrství, předmětu *Počítačové sítě a ochrana dat*. 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:

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

V tomto textu se ponoříme hlouběji do výše uvedené problematiky. Podíváme se na ni jednak z pohledu stavby menších počítačových sítí např. v domácnostech nebo malých firmách a podíváme se také na některé postupy, které se používají ve velkých sítích pro zajištěné vysoké úrovně (a stability) funkcí sítě.

Výše uvedenou problematiku doplníme vhodně o oblast Information Security Management System (ISMS) tedy o pohled na procesní řízení kybernetické bezpečnosti.

Kybernetická bezpečnost bohužel není pouze záležitostí pracovníků IT, ale je kombinací hardware, softwarového vybavení a procesů, které jej využívají. I tyto procesy a osoby, které do nich jsou zapojeny musí být předmětem zájmu dobrého (funkčního) řešení informační bezpečnosti.

Absolvováním předmětu, popř. přečtením skript se z Vás nestane odborník na počítačovou bezpečnost. Získáte ale lepší představu o problémech a především technických aspektech jejich řešení.

Na tento předmět pak v navazujícím magisterském studiu navazuje předmět *Bezpečnosti informačních systémů*, který pak k probírané problematice doplňuje čistě managerský pohled. Předmět se tak zaměřuje na problematiku managementu informační bezpečnosti a také na tzv. IT governance, tedy a ucelené způsoby pro efektivní řízení IT v podnikových podmínkách tak, aby provoz IT maximalizoval užitek, který IT organizaci přináší.

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.

Pro zjednodušení orientace v textu jsem zavedl systém ikon:

Poznámka autora:

Právě držíte v rukou Druhé vydání vydání skript předmětu *Počítačové sítě a ochrana dat*. První

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

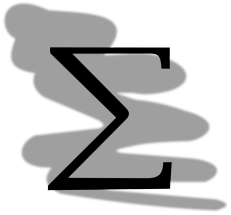
Čas nutný ke studiu
Představuje odhad doby, který budete potřebovat k prostudování celé kapitoly. Jedná se pouze o orientační odhad, neznepokojujte se proto, pokud Vám studium bude trvat o něco déle nebo budete hotovi rychleji.

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.



Shrnutí
Na konci kapitoly obsahuje shrnutí toho, co jste se měli v rámci studia dozvědět. Tuto sekci tak můžete použít pro ověření toho, že jste základní myšlenku kapitoly pochopili správně... pokud jsou zde pro Vás ale informace nové je to znamení toho, že Vaše studium kapitoly nebylo úspěšné a měli byste kapitolu ještě jednou prostudovat.

Jelikož ve skriptech poměrně výrazně navazujeme na některé další předměty (nejvíce na Bezpečnostní informatiku) je tato sekce někdy využívána také pro shrnutí toho, co už byste měli znát.

vydání navázalo na skripta předmětu *Počítače a ochrana dat* (jeho dvě vydání). Toto vydání vyšlo v roce 2015. Od té doby ale uběhla poměrně dlouhá doba, která přinesla kromě reengineeringu dalších předmětů v jednotlivých studijních plánech také pandemii onemocnění covid a s ní spojené poměrně silné rozšíření různých síťových služeb.

Přestože v roce 2023 již nejsme pandemií natolik omezováni, ukazuje se, že změny ve využití síťových služeb a s ní spojené zvýšené nároky na počítačové sítě všeho druhu a jejich bezpečnost představují spíše nový „normál“, se kterým se budeme muset dlouhodobě sžít a zvyknout si na něj.

Z hlediska těchto skript to prakticky znamená, že podstatná část pasáží musela být zcela přepsána, což si vyžádalo poměrně větší úsilí než jsem původně při inovaci skript zamýšlel. Také proto doufám, že informace obsažené v těchto skriptech Vám budou sloužit dobře a budete je využívat také prakticky.

Pokud jste se k těmto skriptům dostali náhodou po nějaké době (z jiného vydání), přikládám také přehled novinek v tomto vydání

Novinky ve 2. vydání

- kapitola věnovaná počítačovým sítí byla přepsána, aby lépe navazovala na základy počítačových sítí z předmětu Bezpečnostní informatika. Kapitola obsahuje také některé informace ke stavbě počítačových sítí.
- v kapitole perimetru sítě byly doplněny
  - moderní generace standardu WiFi, především WiFi 6, 6a a 7,
  - některé podrobnosti o mesh sítích a protokolu WPA3.
  - v sekci vnitřního perimetru byly doplněny některé poznámky ke způsobu realizace demilitarizovaných zón.
  - doplněny některé úvahy k nasazení šifrovacích nástrojů a obnovy šifrovaných dat
  - v sekci autentizace doplněny některé masivně používané technologie, aktualizovány benchmarky pro útoky hrubou silou na šifrovací systémy
- v kapitole o zálohování byly doplněny pásky (LTO), předělána část věnovaná RAID a doplněna sekce věnovaná softwarově definovaným polím (souborovému systému ZFS)

,

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

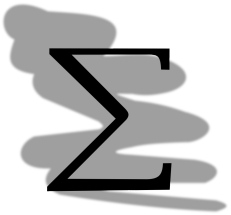
Počítačové sítě

Náhled kapitoly
Na některá specifika stavby počítačových sítí. Zaměříme se na jejich architekturu a to z pohledu stavby domácích sítí, tak trošičku nahlédneme pod pokličku architektury větších sítí.

Po přečtení kapitoly budete
Vědět

1. jak si postavit malou počítačovou síť
2. jaké problémy při jejím provozu můžete očekávat
3. jak přistupují k této problematice větší firmy

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



Předpokládané znalosti
Do této kapitoly vstupujeme s některými předpoklady o Vašich znalostech. Předpokládáme, že jste absolvovali předmět Bezpečnostní informatika, nebo jste se minimálně seznámili s jeho obsahem v oblasti počítačových sítí. Ná základě svého studia byste měli vědět:

- ISO/OSI model síťového stohu
- funkci zařízení typu switch a router
- adresování v síti (MAC adresa, IPv4, IPv6)
- kabeláž typu kroucená dvojlinka CAT 5e, 6, 6a

Výše uvedené informace nebudou v tomto textu opakovány! Pokud si nejste jisti některým z výše uvedených pojmů doporučujeme před započetím dalšího studia Prostudovat znovu skripta z Bezpečnostní informatiky [72], nebo výše uvedené pojmy dohledat na Internetu.

1.1 Základní klasifikace zařízení na síti

Pro účely lepšího pochopení fungování počítačových sítí si nejprve provedeme základní klasifikaci zařízení, která se na ní vyskytují nebo mohou vyskytovat:

- aktivní síťové prvky - infrastruktura zajišťující síťové přenosy

- servery - poskytující různé služby dostupné na síti
- koncová zařízení - počítače, mobilní telefony a další zařízení, která se připojují do sítě a využívají její služby

Každá počítačová síť využívá v určité formě všechny výše uvedené typy zařízení. U menších sítí ale z důvod úspor často volíme zařízení, která kombinují funkcionalitu několika zařízení. Typickým představitelem jsou např. modemy určené pro domácnosti a malé firmy poskytující připojení k internu. Ty velmi často kombinují funkcionalitu routeru, switche, Wi-Fi přípojného bodu apod.

U velkých počítačových sítí takový přístup není úplně typický. Vyplatí se použití dedikovaných zařízení, která je pak možno lépe konfigurovat a škálovat z hlediska požadovaného výkonu.

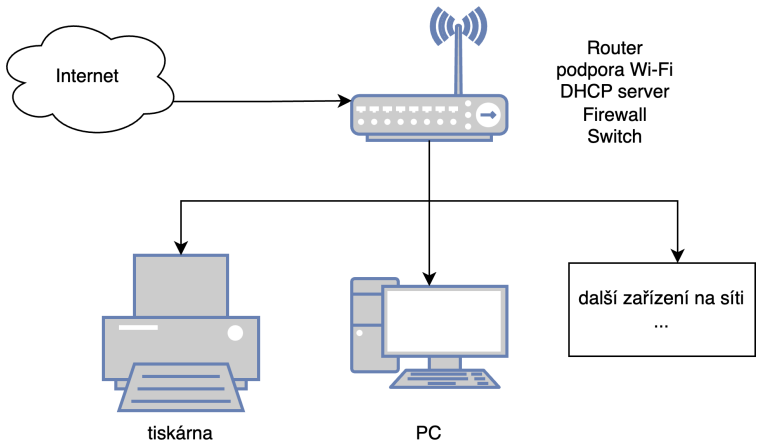
Zkusme se nejprve podívat na menší počítačové sítě, které bychom mohli používat v malých firmách nebo třeba v domácnostech.

1.1.1 Počítačové sítě v domácnostech a velmi malých firmách

Pro tento typ sítí je typické, že k připojení k síti Internet se používá jediná „veřejná“ IP adresa, která je obvykle přiřazena routeru. Ostatní zařízení na síti pak používají tzv. *neveřejné* IP adresy a k plnohodnotnému připojení k Internetu potřebují služby Network Address Translation (NAT).

NAT obvykle běží také na routeru. Tato služba funguje tak že eviduje zařízení, která komunikují s veřejnou sítí a zprostředkovává jejich komunikaci s vnějškem. Zařízení uvnitř sítě tak ve skutečnosti nemají přímý přístup na Internet, ale zprostředkovaný právě pomocí NAT.

Níže přikládáme na obr. 1.1 příklad minimalistické síťové architektury především domácí sítě, na obr. 1.3 je pak typičtější pro malé firmy nebo větší sítě v domácnostech.



Obrázek 1.1: Velmi malá počítačová síť

Jak je patrné z obr. 1.1 jádro počítačové sítě představuje router, který připojuje sít k Internetu, zároveň poskytuje funkcionalitu bezdrátového routeru pro připojení zařízení pomocí Wi-Fi. Takový router by mohl vypadat podobně jako na obr. 1.2.

Podoba routerů se samozřejmě může vizuálně lišit. O2 např. poskytuje několik variant vzhledu bočního panelu a také přední strana s LCD display není příliš častou součástí vybavení routerů. Pokud se ale podíváte na router zezadu, pak naopak zde rozdílů napříč routery nenaleznete. Obvykle je zde připojení Wide Area Network (WAN), Digital Subscriber Line (DSL)[1] Dále jsou zde další síťové porty RJ-45, které zpřístupňují funkcionalitu switche v routeru.

Orientačně routery tohoto typu stojí okolo 2 - 4 tisíc Kč.

Na routerech obvykle není dostupno více než 4 takové porty. Pro rozsáhlejší sítě (viz obr. 1.3) se doporučuje použít spíše samostatný switch. Podle rozsahu služeb poskytovaných Internet Service Provider (ISP) mohou být některé porty předkonfigurované k určitému použití. Na obr. 1.2b je to např. port LAN2, který je předkonfigurován pro O2 TV.

[1] port je sice označen DSL, ale ve skutečnosti modem pracuje s modernější variantou připojení pomocí VDSL, popř. VDSL2.

(a) pohled zepředu (b) pohled zezadu

Obrázek 1.2: Router O2 Smart Box 2 (převzato z [58])

Všimněte si také USB typ A portu, který umožňuje připojit některá další zařízení. Typicky se může jednat o tiskárny nebo úložná média.

Striktně řešeno, není funkcionalita DynamicHost Cache Protocol (DHCP), kterou se přidělují na síti IP adresy vyžadována. Bez ní, je nutné manuálně IP adresy nastavovat na jednotlivých koncových zařízeních. To představuje zvýšené nároky na ruční evidenci a je to celkově nepohodlné. Z tohoto důvodu v dnešní době manuálně přidělujeme IP adresy pouze velmi zřídka a to konkrétně pro servery, kde naopak obvykle požadujeme stabilitu přidělené IP adresy.

Pro úplnost dodáváme, že DHCP přiděluje IP adresu na žádost koncového zařízení a to na dobu určitou. Po uplynutí této doby může zařízení být buďto prodlouženo přidělení stávající adresy nebo přidělena adresa nová. Také je potřeba poznamenat, že v prostředí domácností servery nebývají příliš rozšířené.

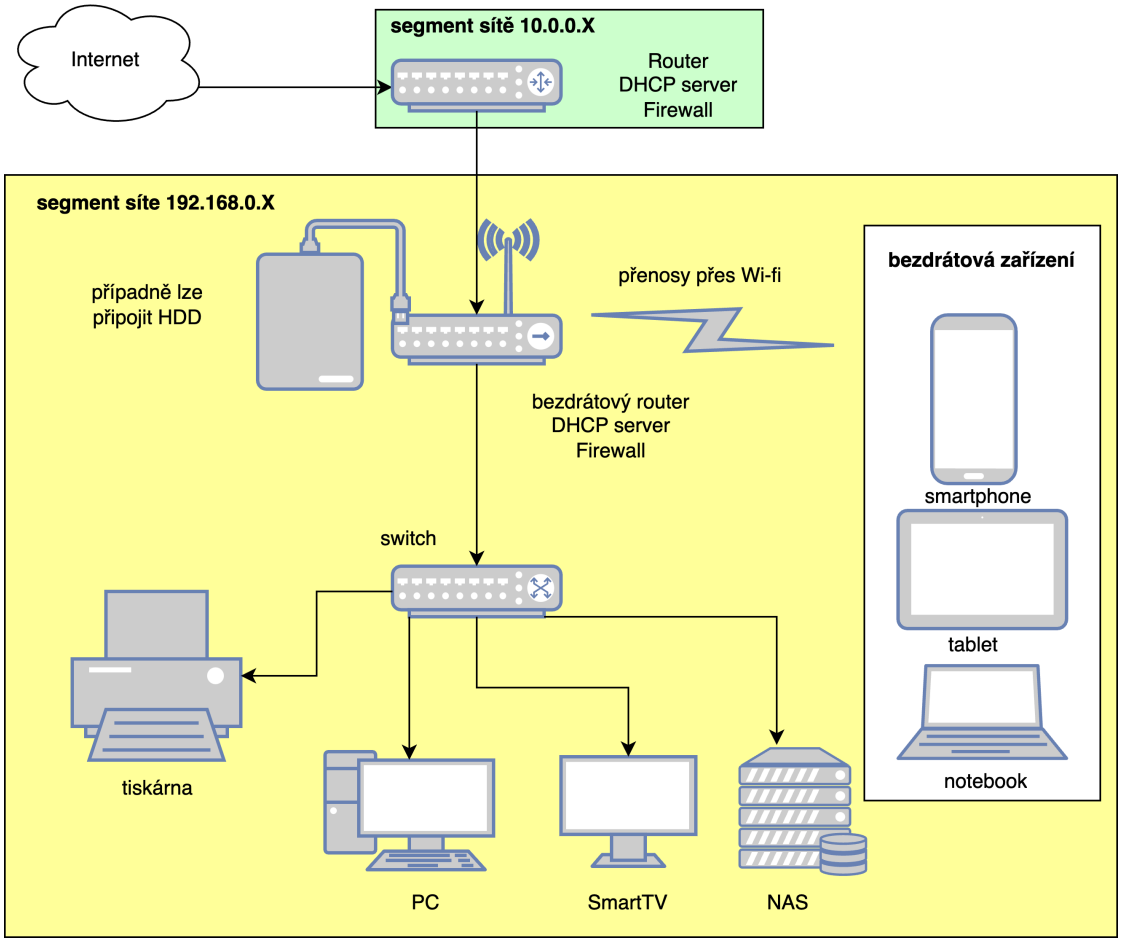
Přidělované IP adresy jsou čistě lokální, což má jisté dopady z hlediska našich možností pro volbu architektury sítě. Sice i v takovém případě můžeme rozdělit síť do jednotlivých segmentů, ale pozor jelikož jsou IP adresy neveřejné nebudou moci jednotlivá zařízení po síti komunikovat (na přímo) mezi těmito segmenty.

Uvažujme příklad: běžná koncová zařízení PC, notebooky apod. dáváme do jednoho segmentu sítě s adresami IPv4 10.0.0.0 - 10.0.0.255, zatímco zařízení IoT dáváme do segmentu sítě 10.0.1.0 - 10.0.1.255. IoT zařízení tak nebudou moci přímo komunikovat s běžnými počítači na síti. V tomto případě bychom ale tuto vlastnost sítě vlastně mohli považovat také za výhodu, tedy alespoň z pohledu bezpečnosti.

Pozor výše uvedené chování vyplývá pouze z použití privátních IP adres. V prostředí větších sítí řešíme tento problém jinak, obvykle pomocí VLAN a filtrováním síťového provozu.

Celkově vzato je tedy tato architektura velmi jednoduchá. Infrastrukturní část stojí na routeru, ke

kterému připojíme všechna zařízení buďto fyzicky pomocí kabelu nebo bezdrátově. Z tohoto důvodu je také router do určité míry úzkým hrdlem systému, pokud ale připojujeme pouze několik málo zařízení, jedná se o velmi efektivní konfiguraci sítě. Pro o něco rozsáhlejší sítě a to i v domácnostech je ale dobré uvažovat o možnosti rozložení zátěže použitím dedikovaných zařízení, viz obr. 1.3.



Obrázek 1.3: Vetší domácí síť, popř. síť velmi malé firmy

V této pokročilejší konfiguraci nám zůstal router jako základní prvek sítě, jeho funkcionalita je ale využívána jinak, v podstatě pouze pro připojení k Internetu. Všechny ostatní funkce jsou zajištěny pomocí samostatných zařízení. Router tedy se bude muset vypořádat s pokusy o komunikaci (a taky útoky) z Internetu a bude zprostředkovávat funkcionalitu NAT pro připojení jednotlivých zařízení k Internetu.

Na obr. 1.3 je funkcionalita DHCP jak na routeru - přiděluje adresu bezdrátovému routeru a také na bezdrátovém routeru, který přiděluje IP adresy všem ostatním zařízením připojených pevně kabelem nebo bezdrátově. Z hlediska zátěže, DHCP obvykle nepředstavuje problém, z tohoto důvodu bychom třeba mohli architekturu „konfiguračně“ zjednodušit ponecháním jenom jednoho DHCP na základním routeru, který by poskytoval adresy všem zařízením na síti.

Bezdrátový router by ale měl zůstat jako samostatné zařízení. Moderní Wi-Fi navazuje dedikované šifrované spojení s každým koncovým zařízením, což představuje už nějakou signifikantní zátěž z pohledu síťového provozu. Samostatný přípojný bod se také lépe škáluje, pokud máme vyšší nároky (nebo specifické podmínky) z hlediska pokrytí signálem Wi-Fi sítě. V takovém případě řešíme problém použitím více přípojných bodů a vytvořením tzv. *mesh sítě*.

K vybudování takové sítě ale obvykle potřebujeme přípojné body, které takovou funkcionalitu podporují. Další podrobnosti o wi-fi naleznete v následující kapitole věnované tzv. *perimetru sítě*.

V případě, že by funkcionalita DHCP zůstala konsolidována na jediném místě - hlavním routeru, bezdrátový router by z hlediska architektury sítě fungoval jako další zařízení připojené do switche, bez přímého připojení na hlavní router. Ten by byl připojen také do switche.

Switch (jeden nebo více) zprostředkovává komunikaci v síti. Ve větších domácích sítích a sítích menších firem je často využívám jeden „větší“ nemanagovaný switch, s velkým množstvím portů (24+). Cena takových zařízení se pohybuje okolo 2 - 3 tisíc Kč. Nemanagované switche se chovají zcela transparentně a obvykle se obejdou bez jakékoliv konfigurace, což u malých sítí považujeme za výhodu.

Nulovou konfigurací přitom rozumíme to, že switch po koupi vybalíme, zapojíme do něj síťové konektory a síť se rozběhne. Switch si zapůjčí IP adresu z DHCP a začne plnit svou funkci. Switch tohoto typu můžete vidět třeba na obr. 1.4.

Obrázek 1.4: Příklad nemanagovaného 24-portového switche TP Link TL-SG1024 (převzato z [20])

Výše uvedený switch podporuje pouze maximální přenosovou rychlost 1 gigabit za sekundu (Gbit/s), což je v současnosti pro většinu nasazení považováno za dostatečnou přenosovou rychlost. Z tohoto pravidla, ale samozřejmě existují také výjimky. Např. pokud uživatelé sítě extenzivně editují video v 8K rozlišení, pravděpodobně budou potřebovat ukládat ohromné objemy dat. K tomu mohou využít různá Network Attached Storage (NAS) řešení. Video data tedy nebudou ukládat lokálně. Tato data proto budou muset přenášet po síti. Pro zajištění plynulosti procesu editace je pak vyžadována podstatně vyšší přenosová rychlost - 10 Gbit/s.

Při volbě switche záleží na předpokládaném (projektovaném) způsobu využití sítě. Při návrhu sítě se snažíme, ideálně předem, identifikovat úzká hrdla architektury sítě, u kterých se vždy rozhodujeme zda z hlediska poskytovaných funkcí budou odpovídat našim potřebám a budeme je tedy akceptovat, nebo budeme hledat alternativní řešení. V případě switche by se jednalo o výkonnější switch.

Z praktického hlediska bývá v podmínkách domácností a malých firem tento hlavní switch doplňován ještě menšími switchi s 4 - 8 porty. Cena takových zařízení se pohybuje okolo 500 Kč. Jejich účelem je zajištění připojení menšího počtu koncových zařízení v místnosti. Tyto menší switche musí být připojeny do hlavního switche. Vzniká tím vlastně do jisté míry stromová struktura.

Jistou představu o architektuře si můžete udělat z obr. 1.5.

Nevýhodou této architektury sítě je to, že je zranitelná výpadky switchů. Např. v okamžiku, kdy vypadne hlavní switch, síť na obr. 1.5 jako taková přestává existovat, což je samozřejmě problém. Přitom platí, že v domácnostech ani malých firmách nejsou připraveny záložní switche, kterými by bylo možné nefunkční nahradit.

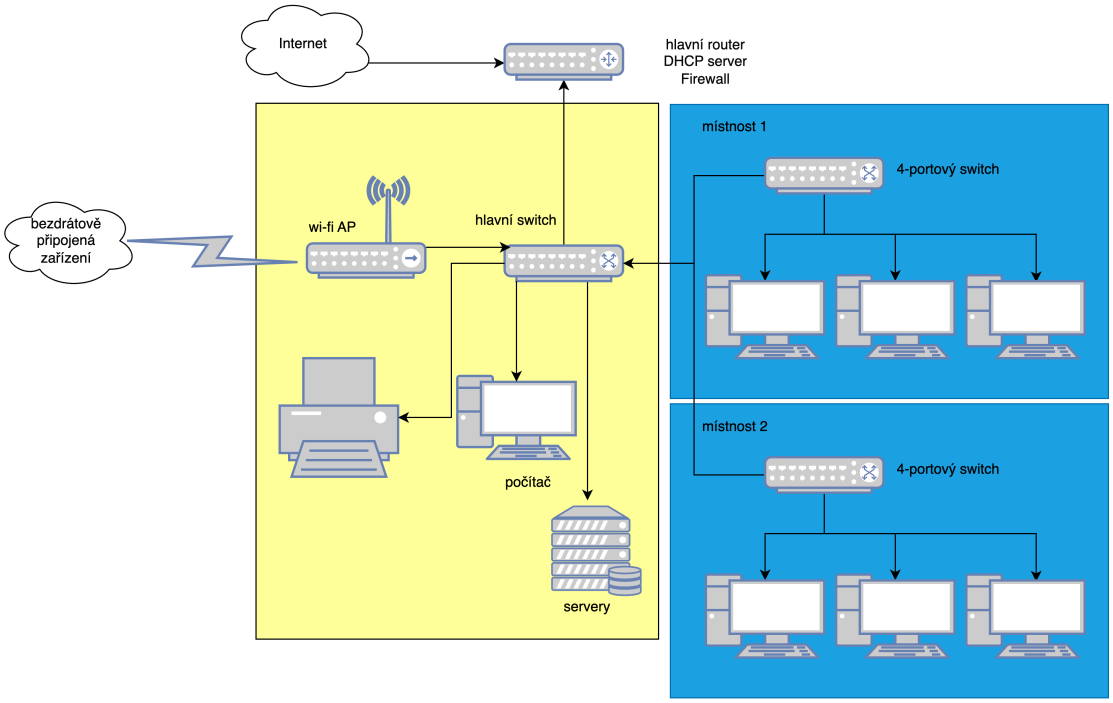
V tomto případě se ale obvykle jedná o akceptované riziko. Hardwarové selhání switchů nenastává příliš často a navíc se jedná o běžnou komoditu, kterou je možno obvykle získat nejpozději do druhého dne. Výpadek služeb v tomto případě tak obvykle bývá považován za akceptovatelný.

V malých sítích neběží obvykle příliš mnoho serverů. Na obr. 1.3 je představitelem takových zařízení NAS. Jedná se o poměrně často nasazované zařízení, které zpřístupňuje velké úložné kapacity, zjednodušuje zálohování, má integrovanou určitou redundanci ve formě diskového pole pro zodolnění systému proti fyzickému selhání jednoho nebo více disků, samozřejmě v závislosti na zvolené konfiguraci. Podrobnosti o typech diskových polí můžete nalézt v kapitole věnované zálohování.

Moderní NAS řešení podporují také technologii docker, která umožňuje s minimální konfigurací rozběhnout vybrané služby v „kontejneru“.

1.1.2 Podnikové sítě

Na tento typ sítí klademe mnohem vyšší nároky. Začněme opět switchi. V případě větších sítí lze předpokládat že do sítě mohou být připojeny stovky, popř. tisíce zařízení a řada z nich bude pracovat souběžně. Zároveň vzhledem k tomu, že uživatelé budou využívat síť pro pracovní účely, dokonce ji k tomuto účelu budou potřebovat, potřebujeme aby síť byla výkonná (měla vysokou rychlost odezvy služeb) a aby byla také spolehlivá.



Obrázek 1.5: Architektura malé sítě s menšími switchi v jednotlivých místnostech

Vaše domácí síť

Zamyslete se nad tím, jak je navržena Vaše domácí síť. Udělejte si jednoduchý náčrtek třeba na kus papíru.

- odpovídá Vašim potřebám?
- co jsou její silné a slabé stránky?
- máte specifické potřeby, které považujete za důležité, ale které nejsou pokryté těmito skripty? ... V tomhle případě byste mi mohli dát vědět tak, aby chybějící problematika třeba mohla být doplněna do dalšího vydání skript.

Velké množství uzlů na síti vede k nutnosti použití stromové topologie, ale případně se zvýšeným důrazem na odolnost infrastruktury. Srovnejte změny v struktuře na obr. 1.6 a 1.5.

Na přístupové vrstvě fungují klasické switche, někdy také označované jako Layer-2 switch. Tedy switch pracující na druhé úrovni ISO/OSI síťové architektury, který jsme probírali v Bezpečnostní informatice. Účelem přístupové vrstvy sítě je poskytnout připojení do síťě jednotlivým koncovým zařízením.

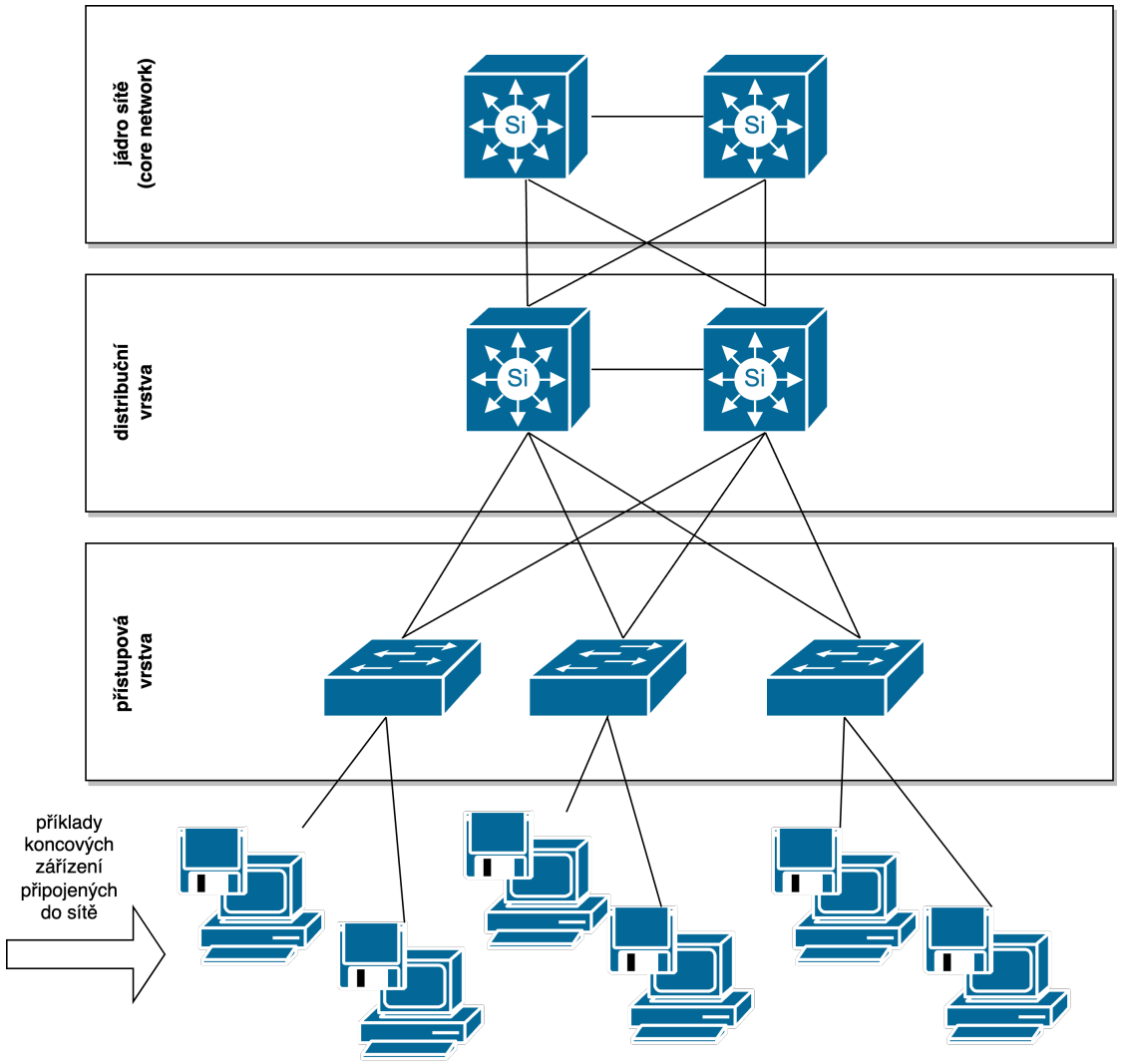
Všimněte si ale, že na dalších vrstvách sítě používáme ale switche jiné. Tyto označujeme jako layer 3 switche, protože pracují na třetí vrstvě počítačové sítě. Zatímco běžný (layer-2) switch pracuje pouze s MAC adresami, layer-3 switch používá IP adresy pro směřování síťové komunikace. Z tohoto pohledu je pokročilejší.

Layer-3 switch je klíčovým zařízením pro konstrukci tzv. Virtuální LAN (VLAN). To nám umožňuje rozdělit jednu fyzickou síť na několik sítí virtuálních, což nám umožňuje zjednodušení správy a zlepšení také bezpečnosti, jelikož síťový provoz mezi VLAN navzájem lze filtrovat (řídit).

Layer 3 switche jsou obvykle zároveň také tzv. managovatelné. Tím rozumíme zejména to, že funkci takových switchů lze lépe konfigurovat. Z hlediska bezpečnosti je např. zajímavá funkce zrcadlení, která umožňuje na vybraný port posílat veškerý síťový provoz, který prochází switchem. To můžeme využít tak, že na port připojíme Intruder Detection System (IDS) senzor a získáme tak přehled o případných problémech, které se v dané části sítě vyskytují.

Z toho důvodu je tento typ switchů obvykle také dražší. Z dnešního pohledu již zastaralý switch Brocade ICX 6430 Řízený L3, s 48 RJ-45 porty na 1Gbit a 4 SFP porty stojí okolo 55000,- Kč. Obdobná varianta Brocade ICX 7750 Řízený L3 10G Ethernet, ale v provedení s podporou 10 Gbit již stojí 470 000,- Kč (obě ceny jsou bez DPH). To už je poměrně významná finanční investice.

Obecně lze říci, že čím výše se ve stromové struktuře sítě dostáváme, tím jsou naše nároky na



Obrázek 1.6: Třívrstvá architektura sítě s použitím switchů

poskytované služby switche vyšší.

Na distribuční vrstvě již switche agregují síťový provoz. To znamená, že do nich (přes ně) půjde veškerá síťová komunikace v síti, kromě té, kterou na koncová zařízení doručí switche přímo na přístupové vrstvě - tedy vše kromě síťové komunikace mezi koncovými zařízeními, která jsou připojena ke stejnému switchi. Z tohoto důvodu tuto vrstvu sítě někdy označujeme jako agregační.

Všimněte si také, že switche na přístupové vrstvě jsou připojeny ke dvěma switchům v distribuční vrstvě. Toto je úmyslné. Umožňuje nám to zodolnit síť proti výpadku jednoho z těchto switchů.

Core network vrstvu je potřeba dělat pouze v případě, že distribuční vrstvě máme natolik velké množství switchů, že pro nás není účelné realizovat síťovou komunikaci mezi nimi „na přímo“, ale potřebujeme je také agregovat. Vodítkem pro potřebu vzniku této vrstvy sítě, může být třeba také geografická distribuce uzlů v síti. Můžeme uvažovat např. situaci, kdy potřebujeme zasíťovat několik rozsáhlých budov. Pro každou z nich můžeme chtít vybudovat distribiční vrstvu. Jednu z těchto budov prohlásíme za jádro sítě (core). Nainstalujeme core switche a fyzicky do nich připojíme distribuční switche.

Všimněte si opět připojení ke dvěma switchům. Také mějte na paměti, že na obr. 1.6 je stromová struktura sítě zjednodušena a tak na přístupové vrstvě mohou být stovky switchů ...

Zkusme se podívat jaká další zařízení mohou na síti fungovat. Jelikož technicky můžeme chtít provozovat taková zařízení nejen v podnikových sítích, ale třeba také v domácnostech. Věnujeme této problematice samostatnou podkapitolu - *Servery a virtualizace*.

1.2 Servery a virtualizace

Problematiku dalších zařízení začneme některými úvahami o architektuře *klient - server*. Z pohledu služeb předpokládáme, že existuje jedno centralizované místo - *server*, kde je nainstalována a nakonfigurována určitá služba. K této službě se pak připojuje řada zařízení - *klient*ů, obvykle dálkově, za účelem konzumace (využití) poskytované služby.

Služby jsou jsou tedy klíčové. Server z tohoto pohledu může být implementován jako:

- fyzický server
- virtualizovaný server
- kontejner

Tradičně bychom server mohli chápat jako samostatné (dedikované) zařízení, zajišťující danou službu. Jednalo by se tedy o počítač, na kterém běží zvolený operační systém a jsou nainstalovány a nakonfigurovány všechny služby, které po daném serveru požadujeme. Tento způsob můžeme označit jako tradiční. Server obvykle umisťujeme do místnosti s řízeným vstupem - *serverovny*. Pokud takových serverů potřebujeme hodně, budujeme tzv. *datová centra*.

Tento přístup má své výhody a nevýhody. Výhodou v tomto případě je to, že s danou službou máme spojen konkretní server, na který fyzicky můžeme ukázat a řešit takové věci jako jestli má dostatečně velkou paměť, jestli počet jader a jejich výkon odpovídá potřebám služby, apod.

Tento přístup má ale také nevýhody. Zkusme si některé z nich odvodit. Uvažujme webový server, který bude provozovat webovou prezentaci organizace a také e-shop. Kapacita serveru se projektuje podle toho, jak velkou špičkovou zátěž má server zvládnout. Pro zjednodušení uvažujeme o nějaké střední firmě, která nehodlá serverový klastr - tedy bude mít jeden webový server a ten musí zvládnout všechny požadavky, které na něj půjdou. Tyto požadavky ale nepůjdou na server s konstantní intenzitou, naopak lze očekávat, že server bude běžně zatížen velmi málo, ale to bude vyváženo extrémními nároky v průběhu špiček.

Výsledkem bude, že hardwarově server musí být připraven na zvládnutí špiček, ale tyto své schopnosti (tento výkon) většinu doby, po kterou bude spuštěn nebude využívat. Z tohoto pohledu nevýhodou je, že investujeme nemalé prostředky pořízení výkonného serveru, ale zároveň tento výkon plně nevyužíváme.

To je velký problém. Jedním z řešení je zprovoznit na jednom serveru více služeb, což technicky můžeme udělat, ale jsou s tím spojeny některé bezpečnostní otázky a také problémy které mohou vznikat při špičkách. Elegantnějším řešením je tzv. *virtualizace* serverů.

Virtualizací rozumíme to, že na jednom fyzickém serveru provozujeme najednou několik serverů virtualizovaných. Na fyzickém serveru běží tzv. hostitelský operační systém. V případě serverů má tento systém jedinou funkci sloužit jako *hypervizor* ke spouštění a ovládání hostovaných operačních systémů.

Hostovaný operační systém pak nepřistupuje k hardware serveru přímo, ale prostřednictvím hypervizoru. To umožňuje hostitelskému OS, aby afektivně rozdělil výpočetní kapacity pro hostované servery.

Virtualizace desktop

Obdobný přístup, jako je popsán pro virtualizaci serverů je možné použít také na desktopu. Tento přístup se používá extenzivně pro testování např. nových verzí operačních systémů. Nebo pokud je potřeba mít počítač nakonfigurován velmi specifickým způsobem a zároveň jej nechceme nebo nemůžeme (např. z bezpečnostních důvodů) používat pro běžnou práci.

V takovém případě je hostitelským systémem běžný operační systém. Jako představitele virtuálních prostředí bychom mohli doporučit třeba open source VirtualBox [59], pro Mac Parallels [31]. V podnikovém prostředí se pak používají řešení na bázi VMWare, popř. CITRIX.

S použitím virtualizace je vždy spojena určitá režie. To znamená že virtualizovaný stroj bude vždy o něco pomalejší, než by byl, pokud by běžel na serveru přímo. Moderní technika, je ale pro tento typ provozu velmi dobře hardwarově připravená a tak je udávaná režie (co padne za oběť použití virtualizace) velmi malá. Udává se, že se jedná o přibližně 10 %.

Tyto ztráty jsou pak vyváženy naší schopností Využít efektivněji stávající hardware a řadou dalších pozitivních vlastností:

- lepší granularita nastavení funkce operačního systému a na něm provozovaných službách
- specifikace požadovaných zdrojů
- možnost dynamické realokace zdrojů, např. ve smyslu přidělení většího nebo menšího podílu zdrojů podle aktuálních potřeb/zatížení
- výrazně jednodušší migrace virtualizovaných strojů, jelikož je klidně mohu spouštěn na jiném fyzickém serveru, pokud to budu potřebovat, což otevírá některé zajímavé možnosti z hlediska údržby a celkové odolnosti infrastruktury proti výpadkům
- možnost provozovat virtuální server pomocí infrastruktury pronajaté v cloudu

Pro úplnost doplňujeme, že tento přístup je agnostický vůči použitému operačnímu systému. Virtualizovat tak můžeme servery s MS Windows, Linux, BSD nebo řadou jiných operačních systémů.

Z technických řešení, která jsou v současnosti masivně nasazována v praxi je možno zmínit VMWare [66], nebo Proxmox [62]. Tato řešení jsou určena pro profesionální nasazení a jsou obvykle poměrně drahá (z pohledu jednotlivce). Organizace, které je prakticky nasazují ale díky nim šetří ohromné množství finančních prostředků a tak se jim vyplatí.

Třetím a svým způsobem nejzajímavějším způsobem je použití tzv. *kontejnerů*. Nejedná se o přístup který by byl zcela nový. I tento přístup je založen na virtualizaci v tomto případě ale spíše na něčem, co bychom mohli označit jako mikro-virtualizace. První implementace byla realizována v OS FreeBSD 4.0, v roce 2000. Jail funguje tak, že se virtualizuje minimalistické jádro operačního systému (konkrétně FreeBSD) a minimální sada komponent, které umožňují provozovat danou službu. To na jedné straně umožňuje, aby režie provozu byla minimální a zároveň, aby zůstala zachována schopnost izolace běhového prostředí a jeho nastavení pro bezpečný provoz.

Jails se používají dosud, ale jelikož je možné je používat pouze v BSD systémech, které nejsou natolik rozšířené. Mnohem rozšířenější je řešení pomocí *Docker* [29]. To funguje na velmi podobných principech. Používá ale jinou terminologii, tedy základní operační jednotkou je kontejner, není založený na BSD systému ale Linuxu a je výrazně rozšířenější.

Toto řešení proti jails umožňuje také používat předpřipravené knihovny kontejnerů, což umožňuje jednotlivé služby bleskově nasazovat podle potřeba a také je v případě potřeby, migrovat, spravovat apod.

Změny v možnostech nasazování serverů vedly také k výrazným změnám v hardware, na kterém jsou založeny. Pokud daná organizace využívá extenzivně virtualizaci, popř. provozuje datová centra, vyplatí se ji investovat do pořizování velmi výkonného hardware, jelikož má jistotu, že tento výkon plně využije. To vede ke konsolidaci hardware v datových center. K této konsolidaci jsou často využívány tzv. *blade servery*, viz obr. 1.7. Česky jsou někdy označovány jako žiletky, byť i v češtině se používá anglický název častěji.

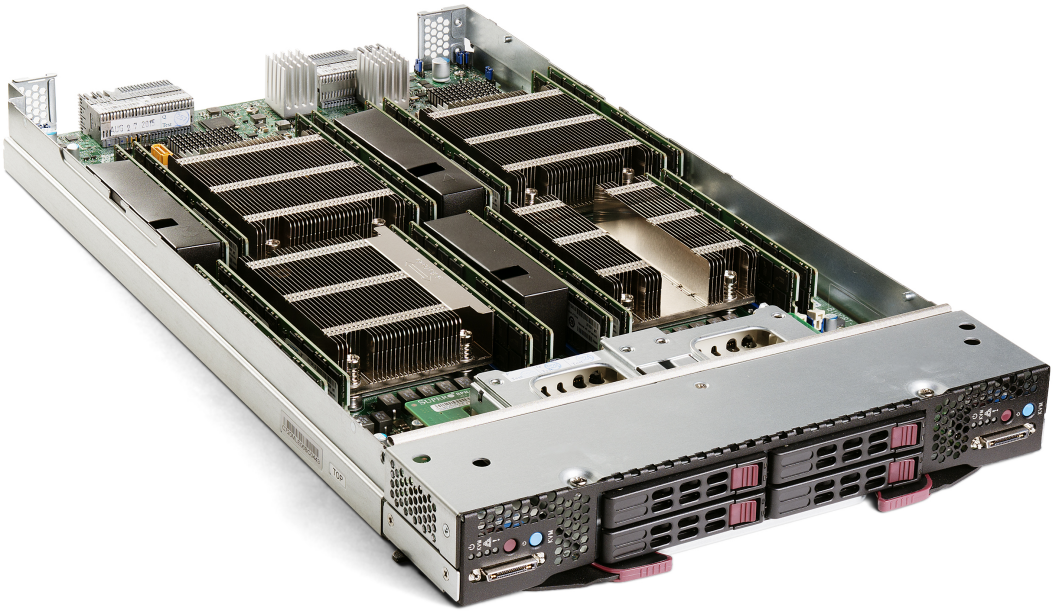
Do blade serveru mohou být instalovány až 2 uzly, každý se dvěma procesory. Pokud uvážíme, že dnešní procesory mohou mít až 64 jader (s podporou 128 vláken) dostáváme k dispozici ohromný výpočetní výkon konsolidovaný do velmi malého prostoru. Blade servery není možné používat samostatně, například v rack, instaluje se do blade enclosure (v češtině označováno jako blade skříň). Příklad jedné takové skříně od společnosti Dell je na obr. 1.8.

Jedna taková skříň může obsahovat až 16 blade serverů. Pokud vezmeme v úvahu výkon jednotlivých serverů popsaný výše, je jasné že tímto způsobem lze na velmi malém prostoru koncentrovat velký výpočetní výkon.

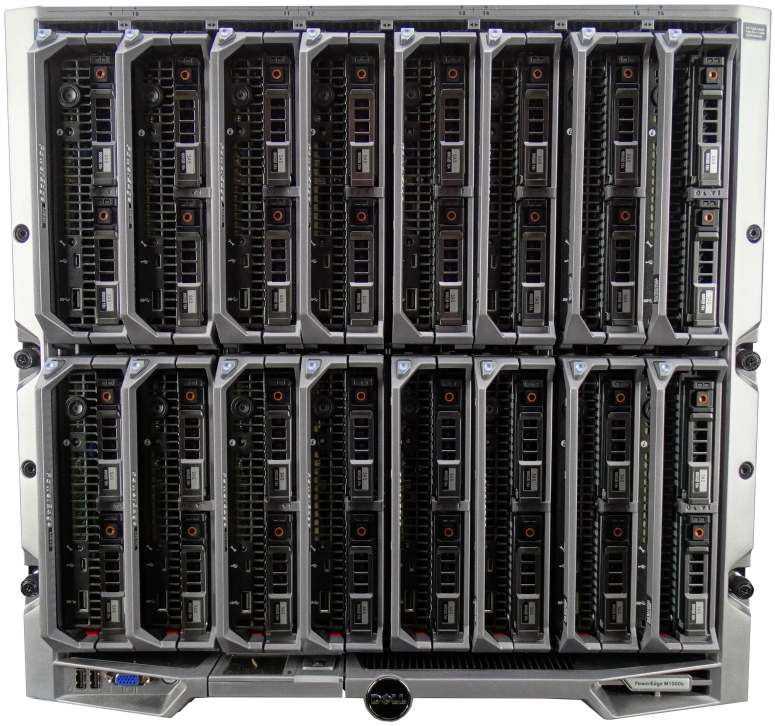
1.3 Role a služby serverů

V předchozí podkapitole jsme brali v úvahu spíše stránku hardware a operační systém serveru. V této podkapitole se zaměříme na služby, která nám server poskytuje. Tyto služby někdy označujeme jako role. Tento rozdíl, není čistě terminologický, je také praktický. *Službou* totiž rozumíme nějaký software, který poskytuje (obvykle po síti) ... něco. Může to být třeba úložný prostor, přístup k síťovým tiskárnám, webové stránky apod.

Role serveru se sada software, která je instalována a konfigurována tak, aby server byl schopen poskytovat určitou funkcionalitu. Jinými slovy, aby server byl schopen zastávat určitou roli, musí mít správně nainstalovány a nakonfigurovány služby. Tedy 1 role = 1 častěji ale více služeb, 1 služba = 1 program.



Obrázek 1.7: Příklad blade serveru - Supermicro SBI-7228R-T2X (převzato z [57])



Obrázek 1.8: Dell PowerEdge M1000e skříň s 16x M640 blade servery (převzato z [33])

Ještě technická poznámka. Termín služba (service) je používán především v ekosystému Windows, v Unixových operačních systémech jsou služby označováni jako démoni (daemon).

Vybrané role serverů pro provoz počítačové sítě:

- DHCP
- Domain Name Server (DNS)
- IDM, viz podkapitola věnovaná identity managementu

DHCP jsme se již dotkli v Bezpečnostní informatice. Jedná se o klíčovou síťovou službu, kterou používáme pro přidělování IP adres zařízení připojených v síti. Bez tohoto kroku, by nebylo možné síť využívat. Znovu připomínám, že statické přidělování IP adres již v současnosti v praxi nepoužíváme.

Zejména ve větších podnikových sítích ale můžeme mít větší požadavky na regulaci způsobu, kterým jsou IP adresy přidělovány. Základním požadavkem bývá omezení přidělování IP adres pouze takovým zařízením, která jsou registrovaná. V tomto případě se ale bavíme pouze o statickém umístění, tedy primárně desktop, popř. dokovací stanice se síťovým portem. Problematiku připojování bezdrátových zařízení budeme probírat podrobněji v následující kapitole.

Pro splnění tohoto úkolu můžeme využít toho, že každá síťová karta má přidělenou unikátní adresu - MAC adresu. Prvním krokem tak bývá nastavení DHCP tak, aby přidělovala IP adresy pouze zařízením s registrovanou MAC adresou.

Některé větší firmy pak přidávají další opatření. Mohou mít jednoduchý informační systém umožnující evidovat také vlastníka a fyzické umístění zařízení. Informaci pak lze použít k tomu, abychom omezili schopnost zařízení připojovat se odkudkoliv. Jinými slovy připojení je možno nastavit tak, aby se zařízení připojilo pouze pokud je připojené ke konkrétní síťové zdířce.

DNS umožňuje přidělovat doménová jména jednotlivým zařízením na síti. To je velmi důležitý moment, protože IP adresa je přidělovaná a obvykle není statická. Jméno zařízení naopak statické je. To nám pak umožňuje zlepšenou správu identit a otevírám nám možnosti pro aplikaci politik konfigurace např. pomocí služeb Active Directory (AD).

Tato problematika úzce souvisí s problematikou identity managementu, které se budeme věnovat podrobněji v dalších kapitolách.

DNS v malých sítích

V malých sítích obvykle neprovozujeme vlastní DNS server. Důvodem je, že v takových sítích nejsou provozovány další služby, které by ke své funkci DNS vyžadovaly. Z tohoto důvodu je DNS v takových případech přebíráno od ISP nebo je poskytovatel DNS služeb manuálně nastaven na jednotlivých koncových uzlech sítě nebo globálně na routeru.

Často používané jsou v takovém případě otevřené DNS od společnosti Google [47] s adresami 8.8.8.8 a 8.8.4.4, nebo společnosti Cloudflare [39]. Pro využití Cloudflare DNS se potřeba provést registraci, služba jako taková je ale poskytována zdarma.

Podle funkce můžeme servery dělit také následovně. Berte přitom prosím v úvahu, že se jedná spíše o příklady typů serverů/rolí, než ucelený výčet:

- databázové servery
- WWW servery
- souborové
- tiskové
- aplikační
- atd.

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.

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

Všechny výše uvedené servery patří do rodiny tzv. *relačních databází*, tedy do stejné rodiny, jako např. MS Access, se kterým jsme se seznámili na cvičeních z bezpečnostní informatiky.

Databázové servery nám umožňují zpřístupnit databázi, což je funkcionalita vyžadovaná drtivou většinou informačních systémů, jelikož každý informační systém musí někde ukládat svá data. Tím vhodným místem je obvykle právě databáze.

Relační databáze, ale nejsou jediným typem databází. Pokud daná organizace manipuluje s gigantickými objemy dat a zároveň tato data chce používat pro analytické účely, využívají se často také tzv. NoSQL databáze. Ty fungují na jiným principech než relační databáze.

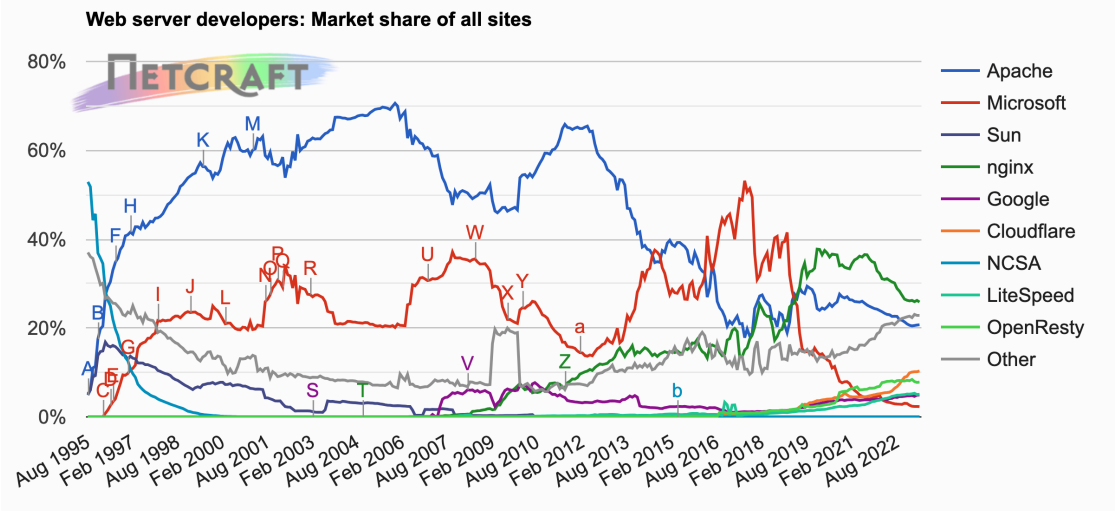
Data v nich jsou ukládána „na jedné hromadě“ a jsou opatřována různými metadaty, podle kterých je lze třídit, filtrovat a dále zpracovávat. Nevýhodou tohoto typu databází je to, že strukturálně nejsou schopné vynucovat automaticky kontroly integrity záznamů apod. Což sice lze obejít implementací takových kontrol třeba ná úrovni informačního systému, ale není to úplně jednoduché. To je také důvod proč se tento typ databází obvykle nepoužívá jako back end běžných informačních systémů.

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

Pokud se ale podíváme na tržní podíly webových serverů, viz obr. 1.9, uvidíme zajímavou věc - tržní podíly prakticky všech populárních webových serverů postupně klesají.



Obrázek 1.9: Tržní podíly populárních webových serverů (převzato z [56])

Tento pokles je způsoben několika souběžně probíhajícími trendy. Jednak provozovatelé velkých infrastruktur poskytující služby pro provoz webových sídel upravují některá open source řešení tak, aby lépe fungovala na její infrastruktuře. To je případ OpenResty, které je založené na Ngix s doplněnou podporou pro jazyk Lua. Google, Cloudflare postupují obdobným způsobem. Jejich řešení jsou ale proprietální.

Druhým trendem je vytváření webových aplikací, které nejsou založeny na použití klasického webového serveru. Představitelem takových systémů je třeba poměrně populární Node.js. Node.js umožňuje

vývojářům poměrně elegantně psát webové aplikace v programovacím jazyce JavaScript. Node.js proto není ale obecně použitelný. Aplikace musí být napsané přímo pro něj a nejsou přenositelné. Oproti tomu, klasické webové aplikace běžící např. na Apache web server mohou obvykle stejně snadno běžet na Ngix i řadě dalších webových serverů.

Důvodem pro vzestup popularity Node.js je tak proto něco jiného. Jednak je to přímá podpora JavaScriptu, jako jednoho z nejpoužívanějších programovacích jazyků současnosti, jednak je to snadnější škálovatelnost aplikací, vestavěná podpora asynchronního zpracování požadavků, což je nesmírně užiteční funkcionalita systémů, které podléhají vysoké zátěži.

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 NAS. Taková zařízení umožňují domácnostem, malým a středním firmám efektivně spravovat relativně velké diskové kapacity. Představu o vzhledu NAS si lze udělat z obr. 1.10.

Obrázek 1.10: Příklad NAS TVS-671 od společnosti QNAP (převzato z [63])

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.

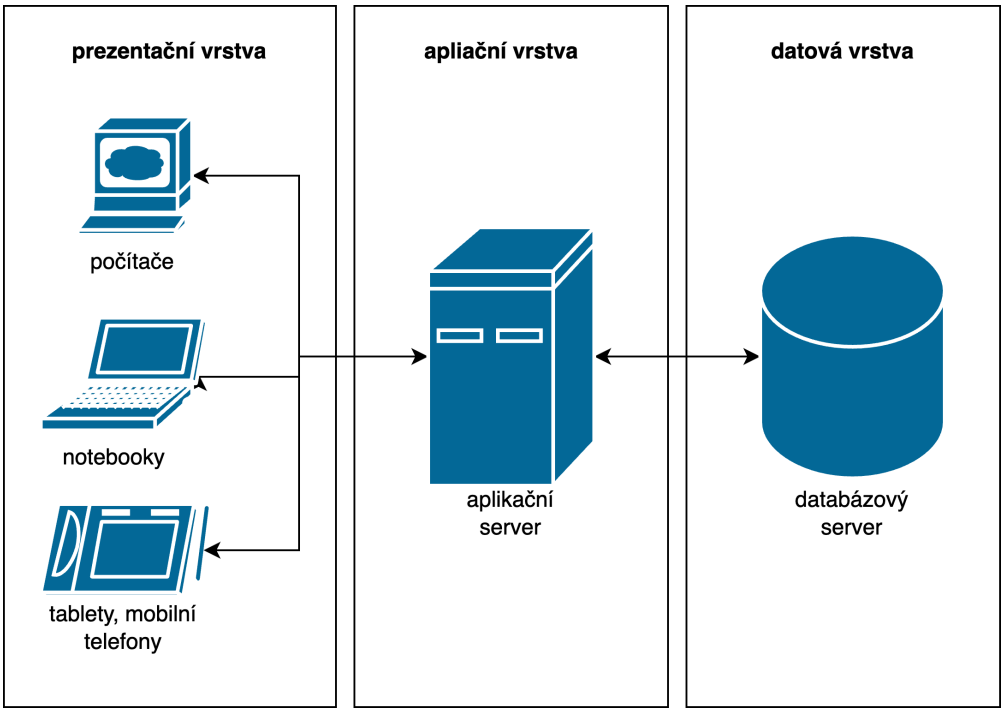
Úkolem **tiskového serveru** je spravovat tiskárny a jejich tiskové úlohy. Použití tiskového serveru má tu výhodu, že správa tiskáren je centralizovaná, to umožňuje:

- 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 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.

Nasazení aplikačního serveru si klade za cíl tyto výše uvedené problémy řešit konsolidací celé aplikační logiky na jediném místně - *aplikačním serveru*. Jednou z nejznámějších architektur, nikoliv však jedinou, je 3-vrstvá architektura klient-server. Graficky bychom ji mohli znázornit podobně jako na obr. 1.11.

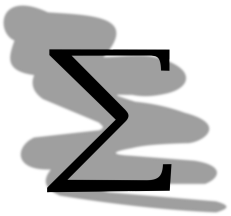


Obrázek 1.11: Třívrstvá architektura klient server

Jak je patrno z obrázku, jednotliví klienti přistupují na prezentační vrstvě konzumují služby nabízené aplikačními serverem na aplikační vrstvě. Děje se tak obvykle pomocí *tenkých* klientů. Tenkým klientem obvykle rozumíme webový prohlížeč. Na straně aplikačního serveru tak logicky musí naslouchat webový server. Mimochodem to je také důvod proč jsme šli celkem do podrobností ohledně webových a databázových serverů o několik odstavců výše.

Aplikační server zpracuje požadavky pomocí programové logiky. K tomuto účelu obvykle aplikační server potřebuje data. S těmito daty ale aplikační server nenakládá přímo, ale zprostředkovaně pomocí databázového serveru fungujícího na datové vrstvě. Aplikační server s nim komunikuje pomocí požadavků v jazyce SQL, v případě relačních databází.

Všimněte si, že klienti na prezentační vrstvě nemají přímý přístup k datům. Data mohou získat pouze prostřednictvím aplikačního serveru a pouze v rozsahu, který klientovi umožní zvolený bezpečnostní model. Toto omezení lze vynutit tak, že na úrovni databázového serveru zpřístupníme data z databáze pouze účtu, který používá pro komunikaci s databází aplikační server a nastavíme možnosti připojení na IP adresu aplikačního serveru.



Shrnutí

Tato kapitola byla poněkud hutnější. Ověřte si proto, že chápete základní funkce všech zmiňovaných prvků sítě. Např. co je účelem routeru. Jaký je rozdíl mezi vrstvy 2 a 3 switchi, jaká jsou specifika stavby podnikových sítí. Jaká je funkce DHCP, DNS, NAT apod.

Kontrolní otázky

1. Co je účelem NAT?
2. K čemu slouží aplikační server?
3. Jaký je rozdíl mezi switch na 2. a 3. vrstvě?
4. Jaká je funkce routeru?
5. Co je to VLAN?

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, nebo jejich rozsahy) mohou komunikovat a pomocí jakých služeb (nastavením portů). Filtrování je založeno na tom, že každá služba, která má být přístupná po síti musí „naslouchat“ na určitém portu, přes který pak bude komunikovat s okolím.

Řekněme, že na serveru s IP adresou 153.10.50.15 provozujeme webový server a z historických důvodů udržujeme na něm podporu jak šifrovaných, tak nešifrovaných verzí protokolu Hyper Text Transfer Protocol (HTTP). V takovém případě, bude nešifrovaná verze HTTP používat port 80 a šifrovaná HTTPS port 443.

Existuje řada protokolů, pro které jsou používané protokoly dobře popsány. Základní přehled naleznete např. na Wikipedii [36]. Používané porty jsou ale součástí každého manuálu pro síťové služby.

Rozlišujte firewally a osobní firewally
Osobní firewally jsou určeny pro posílení schopností operačního systému na desktopu bránit se útokům realizovaným po síti. Osobní firewall má schopnosti filtrace síťového provozu popisované výše, zároveň ale často obsahuje pokročilou funkcionalitu pro:

- blacklisting/whitelisting aplikací
- funkcionalita Host Intruder Prevention System (HIPS)/Network Intruder Prevention System (NIPS)
- sandboxing aplikací
- a řada dalších.

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

Z tohoto důvodu firewall na vnějším perimetru sítě je doplňován řadou dalších nástrojů, které teprve společně tvoří celkový obraz bezpečnosti v dané organizaci. Z praktického pohledu to vede k nutnosti kromě vnějšího perimetru sítě budovat také perimetr vnitřní a zamýšlet se také nad architekturou sítě jako takovou.

Existuje také 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.).

Toto je dlouhodobý požadavek. V minulosti mu ale řada organizací úspěšně odolávala a pak v roce 2020 přišel covid-19. Přišly různé lockdowny, práce z domova (homeoffice) a organizace se tak dostaly do situace, že funkce sítě musely v nějaké podobě zpřístupnit i z vnějšku.

Píše se rok 2023. Situace s covid-19 se uklidnila, ale změny v našem přístupu k práci zůstaly do značné míry zachovány. A tak se z možnosti pracovat v podstatě odkudkoliv stal vlastně „nový normál“. Uživatelé i organizace se prostě přizpůsobili a tak není úplně možno tyto změny zvrátit.

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

Pro vyřešení tohoto rozporu se v praxi využívají zařízení **Virtual Private Network (VPN)**. Jejich úkolem 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 provozovaného organizací 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 a 802.11ac (pro starší sítě) a 802.11ax (pro novější sítě). Společným prvkem standardů je využití nelicencovaných pásem. Podle verze standardu se jedná o pásma 2,4, 5 a 6 GHz.

Kromě označení standardu se pro zjednodušení používá označení WiFi s číslem, což je jednodušeji zapamatovatelné a lze takový název lépe využít marketingově pro snadnější komunikaci schopností přípojných bodů a zařízení, které se k nim připojují. Podrobnější seznam v současnosti platných standardů je dostupný v tab. 2.1.

Tabulka 2.1: Současné standardy Wi-Fi (stav k 2023)

označení	**standard IEEE**	**rok**	**max. rychlost [Mbit/s]**	**frekvence [GHz]**
Wi-Fi 7	802.11be	2024[1]	46 Gbit/s	2,4/5/6
Wi-Fi 6E	802.11ax	2020	9,6 Gbit/s	2,4/5/6
Wi-Fi 6	802.11ax	2019	9,6 Gbit/s	2,4/5
Wi-Fi 5	802.11ac	2014	3,5 Gbit/s	5
Wi-Fi 4	802.11n	2008	600	2,4/5
	802.11g	2003	54	2,4
	802.11a	1999	54	5
	802.11b	1999	11	2,4
	802.11	1997	2	2,4

Prosím všimněte si, že oficiální „přečíslování“ Wi-Fi začíná na Wi-Fi 4. Wi-Fi 1 - 3 nebylo přiděleno, neoficiálně se ale Wi-Fi 3 používá pro verze standardu a/g, 2 pro verzi b a 1 pro původní bezpísmenkovou verzi standardu.

Dále výše uvedené rychlosti je potřeba vnímat jako maximální teoretickou rychlost, realisticky tak lze očekávat poloviční rychlost, ve ztížených podmínkách pak rychlosti ještě výrazně nižší.

Situace je z hlediska rychlosti také komplikovaná tím, že ne všechny zařízení využívající určitý standard jsou schopna použít všechny vlastnosti tohoto standardu. Jde o to, že standard má obvykle povinné části, které logicky mají všechna zařízení, která se k němu hlásí, má ale také nepovinné části, které mohou ale nemusí být podporovány.

To je problém zejména z časového pohledu. První AP podporující daný standard obvykle jsou objektivně horší, než pozdější revize hardware. Dobrým příkladem jsou standardy 802.11ac a 802.11ax. Všimněte si, že pro ax standard existují varianty Wi-Fi 6 a 6E. Varianta 6E přitom přidává podporu 6 GHz frekvenčního pásma.

Oproti tomu ac je jenom jeden standard, jenomže existují dvě zásadní revize označované jako wave 1 a 2. Wave 2 zařízení pracují s dvojnásobnou šířkou kanálu a podporují Multi-User Multiple-Input and Multiple-Output (MU-MIMO). Tato technologie umožňuje navázat až 4 přímá směrovaná spojení mezi AP a koncovými zařízeními, což výrazně zefektivňuje komunikaci v bezdrátové síti a to i v nepříznivých podmínkách (např. vysoké koncentraci různých sítí v bytových domech). Vzhledem k tomu, že jak obchodní označení tak číslo standardu jsou v tomto případě stejné, jsou rozdíly poměrně obtížně komunikovatelné koncovým zákazníkům.

To byl pravděpodobně důvod, proč pro ax verzi standardu je rozlišení Wi-Fi 6 a 6E, které je na první pohled patrné.

[1] rok 2024 je předpokládaným rokem finalizace standardu

Z hlediska investic do AP bychom měli pro domácí použití volit co možná nejnovější verzi, s tím, že poskytuje nejlepší funkcionalitu pro uživatele sítě. To však bývá vyváženo vyšší cenou za taková zařízení. Je také logické, že s novými verzemi Wi-Fi je trochu problém ve smyslu podpory ze strany koncových zařízení. AP je obvykle zpětně kompatibilní. Klienti, kteří podporují pouze starší verze standardu se tak budou moci připojit, akorát pro ně nebude dostupná pokročilá funkcionalita, kterou AP nabízí.

Lze ale předpokládat, že v průběhu času v důsledku obměny zařízení se tento problém vyřeší sám. V závislosti na našich potřebách ale můžeme ze určitých okolností investovat do obměny wi-fi karet např. v noteboocích. Toto bývá totiž jedna z mála komponent, kterou je možno v notebooku vyměnit. Bohužel však ne u úplně všech typů. Pro představu taková karta (viz obr. 2.1) stojí necelých 600,- Kč.

Obrázek 2.1: Intel Wi-Fi 6E AX210 (převzato z [54])

Nové vlastnosti Wi-Fi 7

Wi-Fi 7 má celou řadu nových vlastnosti, které výrazným způsobem dále zefektivní fungování bezdrátových sítí:

- až 4-násobná přenosová rychlost ve srovnání s Wi-Fi 6E (
  - širší přenosové kanály
  - Quadrature Amplitude Modulation (QAM) - Wi-Fi 7 podporuje 4K-QAM, 6 podporuje pouze 1024-QAM, platí čím vyšší hodnota, tím víc informací se do předášených signálů dá vložit
  - Multi-Link Operation (MLO) - umožňuje zkombinovat několik několik frekvencí napříč pásmy do jediného spojení
- Wi-Fi 7 dále vylepšuje stávající technologie jako např. MU-MIMO
- podporuje autentizaci pouze pomocí protokolu WPA 3 (nejsou podporovány starší)

Podstatnou vlastností AP je dosah. Ten 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. Obecně platí že čím vyšší je frekvence tím vyšší je na jedné straně přenosová rychlost, ale na druhou stranu tím je také nižší dosah signálu. Frekvence 5 a 6 GHz jsou na to obzvláště citlivé.

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 jehož okolí nejsou ideálně provozovány žádné bezdrátové sítě. V opačném případě budou interference v signálu způsobovat zmenšení dosahu signálu vysílaného z našeho AP.

Obecně také v současnosti (léto 2023) platí, že sítě na 6 GHz budou stále ještě méně nasazované, než sítě na tradičních 2,4 a 5 GHz. To se ale v příštích několika letech změní.

Existuje celá řada aplikací pro mobilní telefony nebo tablety, které umožní pohodlné zmapování využití Wi-Fi spektra v dané lokalitě. Pro správnou funkci je ale samozřejmě důležité, aby zařízení, ve kterém budeme frekvence monitorovat mělo podporu všech pásem, která bude AP využívat. To je problém zejména právě pro 6 GHz, pro které se zařízení tyto frekvence využívající dostaly do prodeje v roce 2023.

Pro ilustraci přikládáme výstup z populární aplikace Wi-Fi Analyzer pro zařízení s operačním systémem Android je znázorněn na obr. 2.2.

Obrázek 2.2: WiFi Analyzer (převzato z [22])

Na obr. 2.2 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.

Výše uvedenou analýzu je potřeba realizovat na všech frekvencích samostatně, tedy 2,4 Ghz, 5 GHz a případně také 6GHz. Bezdrátová síť by měla v každém případě fungovat na všech podporovaných frekvencích.

AP volíme obvykle podle toho, v jakém prostředí má být AP nasazeno a také našich finančních možností. Pro určitou představu jsou na obr. 2.3 přiloženy některé z v současnosti prodávaných AP určených pro domácnosti a malé firmy. Ceny se běžných bezdrátových routerů se pohybují v rozmezí 6 - 7 000,- Kč za kus. Jsou ale routery s pokročilou funkcionalitou za násobně vyšší ceny.

Vzhledem k výše uvedenému je očividné, že pokrýt kvalitním Wi-Fi signálem větší prostor může být celkem výrazný problém. Řešení může spočívat v instalaci více AP, které předmětný prostor pokryjí. Aby takové řešení fungovalo efektivně, bylo by dobré, aby každé z těchto AP nepracovalo samostatně, ale aby se vytvořila síť těchto zařízení. Uživatelé by se v ideálním případě mohli pohybovat volně v pokrytém prostoru a volně přecházeli podle potřeby mezi AP.

Bezdrátové sítě tohoty typu mají jméno - *mesh*. K tomuto účelu obvykle používáme zařízení stejného typu, která mesh funkcionalitu podporují. Obě zařízení na obr. 2.3 mají podporu spojování AP do mesh, ale zařízení Deco se navíc prodávají po baleních po více kusech. Pořízení takových sad AP může z ekonomického pohledu dávat větší smysl než pořizování jednotlivých zařízení.

Určitou představu o způsobu zapojení AP pro malou, např. domácí síť je možné si udělat z obr. 2.4.

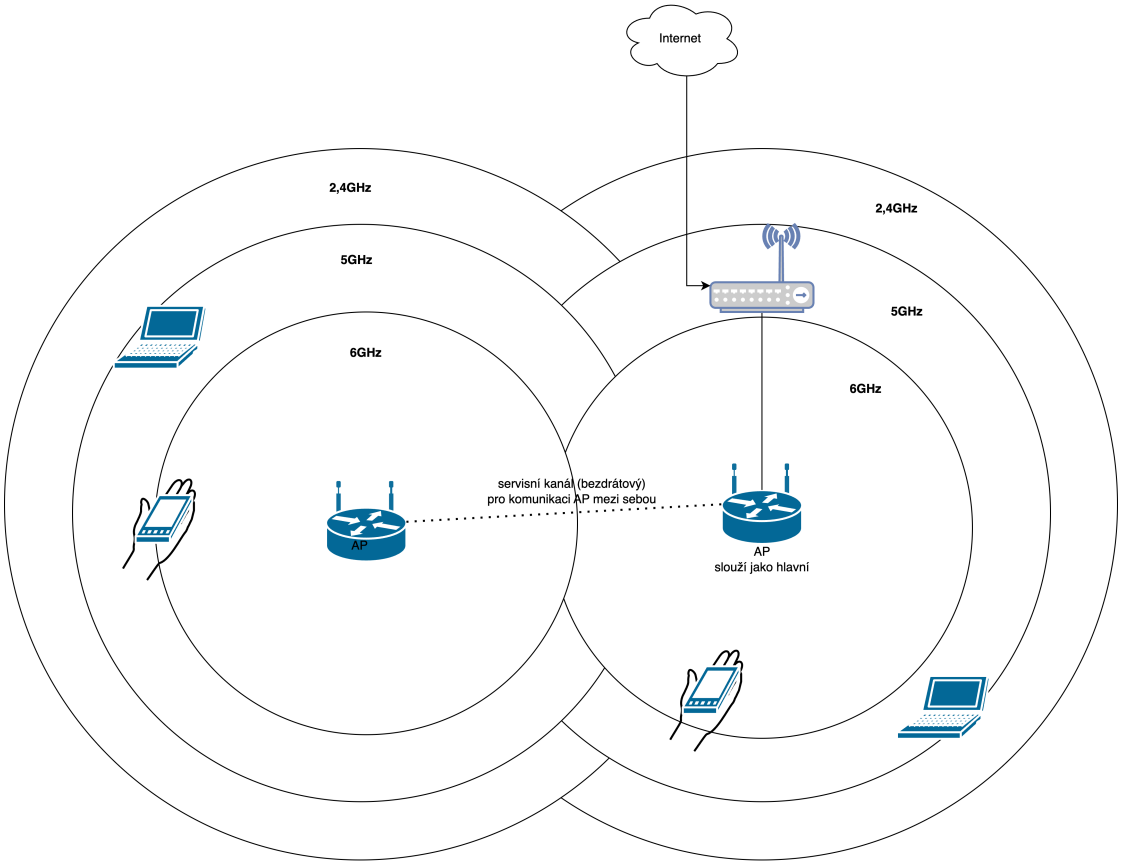
V rámci malé sítě lze předpokládat, že plnohodnotně, kabelovým připojením bude připojen pouze jediný (hlavní) AP, na obr. 2.4 vpravo. Ostatní AP k němu budou připojeny bezdrátově. Toto připojení se realizuje na samostatném kanálu. Jednotlivá AP si na něm předávají servisní informace o stavu sítě a zařízení, která se na ní nacházejí.

Vzhledem k nutnost jednotlivých AP komunikovat mezi sebou bezdrátově, musí být umístěna relativně blízkou u sebe a mohla navázat spojení. Ve větších organizacích se proto volí jiný způsob. Jednotlivá AP se připojena pevným (kabelovým) připojením k nejbližšími switchi a jsou rozmístěna tak, aby pokrytí signálem bylo co nejlepší. Pro takové řešení se vyžaduje obvykle také serverová

(a) TP-Link Deco XE75, AXE5400 WiFi6E

(b) Router Asus RT-AXE7800

Obrázek 2.3: AP přípojné body TP-Link Deco XE75, AXE5400 WiFi6E (převzato z [42]) a Asus RT-AXE7800 (převzato z [43])



Obrázek 2.4: Wi-Fi mesh síť složená ze 2 AP (příklad velmi malá síť)

komponenta, která bude celou bezdrátovou síť řídit.

AP určená pro podnikové nasazení jsou obvykle výrazně dražší, jsou schopna obsluhovat spolehlivě velké množství klientů a mají některé specifické vlastnosti oblasti např. v oblasti autentizace. Vzhledem k odlišným požadovaným vlastnostem působí v tomto segmentu odlišní dodavatelé - namátkou je možno zmínit společnosti Ubiquiti nebo třeba Cisco.

Frekvence, umístění AP, útlum signálu při prostupu různými překážkami, vše vede k tomu, že

hranice (perimetr) bezdrátové sítě je značně neostrá. Můžeme ale předpokládat, že bude přesahovat hranice budov, ve kterých jsou AP nainstalovány.

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
- WPA3

Z výše uvedených protokolů je v současnosti možno považovat za **bezpečný pouze WPA2 a WPA3**.

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 128-ti bitovým klíčem a využívá Temporal Key Integrity Protocol (TKIP). Ten generuje a aplikuje šifrovací klíč samostatně pro každý packet. Využívána je šifra RC4. WPA také obsahuje Message Integrity Check (MIC), který by měl zabránit útoku pomocí opětovného přehrání (pozměněných) starších packetů. Ačkoliv je WPA výrazně kryptograficky silnější než WEP, nepovažujeme poskytovanou úroveň bezpečnosti z dnešního pohledu za dostatečnou.

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 minimálně WPA2 mělo být standardem.

WPA3 oproti starším iteracím protokolu již nepoužívá před-sdílený klíč, místo toho využívá Synchronous Authentication of Peers (SAE). Pro případného útočníka je pak mnohem obtížnější nalézt heslo potřebné k připojení do sítě. WPA3 také zvyšuje podporovanou délku šifrovacího klíče na 256 bitu (stále je používán šifrovací algoritmus AES). Ačkoliv je pokrok v oblasti bezpečnosti u tohoto algoritmu výrazný jsou v současnosti již známy některé zranitelnosti (slabiny) tohoto protokolu. Zdá se proto, že v dohledné budoucnosti bude potřeba vyvinout a nasadit protokol nový (nebo upravit stávající).

Jak je patrno z předchozího textu, pro použití Wi-Fi v domácnostech, nebo malých firmách je typické, že klienti se autentizují pomocí jednoho, pro všechny stejného autentizačního klíče. To je právě to, čím rozumíme „předsdílený klíč“, který Vás možná zarazil v předchozím odstavci. Takový přístup je efektivní, ale z hlediska bezpečnosti udržitelný pouze pro velmi malé počty uživatelů.

V okamžiku, kdy by tento způsob měl být použit pro střední nebo velkou firmu, pak tento klíč bude fungovat jako veřejné tajemství a nebude tak poskytovat žádnou ochranu. WPA protokoly proto rozlišují *osobní* a *podnikové* nasazení. Použití jednoho hesla odpovídá právě osobnímu použití.

Extensible Authentication Protocol (EAP) Protected EAP (PEAP) Pro podnikové nasazení se používá většinou některá z rozšíření WPA2 nebo WPA3, 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.

Uživatelé se do bezdrátové sítě v takovém případě neautentizují pomocí jediného společného hesla, ale pomocí svého uživatelského účtu a hesla, obvykle jiného než do běžné počítačové sítě. Důvodem je že šance na kompromitaci takového hesla jsou přece jenom vyšší. V případě, že toto heslo bude jiné než do běžné sítě, útočník nezíská přístup k citlivým systémů.

Použití samostatných účtů pak také umožňuje, aby tyto účty byly případně blokovány, pokud bude detekována nějaká nežádoucí aktivita.

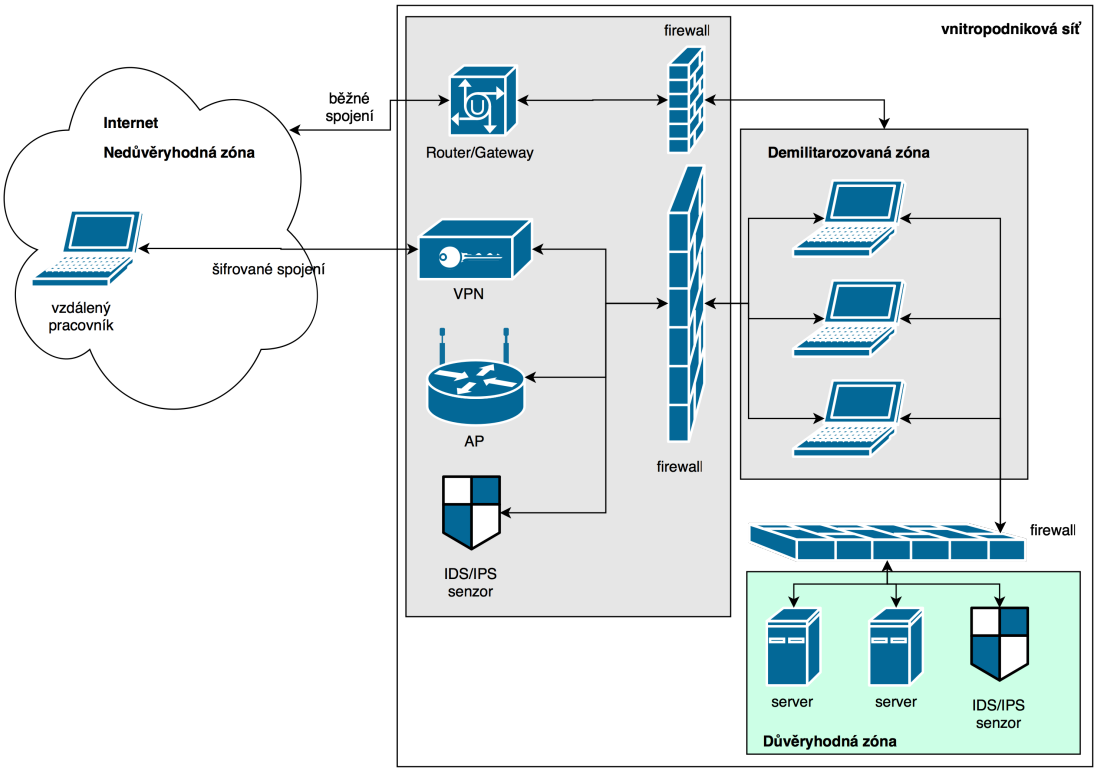
Autentizačním mechanismům je věnována samostatná kapitola.

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. 2.5.



Obrázek 2.5: Vnitřní perimetr sítě

Schéma na obr. 2.5 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.

Výše uvedené je poměrně dosti obecné, z praktického pohledu bychom výše uvedené principy mohli aplikovat a získat tak některá doporučení pro vhodné nastavení architektury sítě.

Začněme firewally. Obr. 2.5 předpokládá použití klasického firewallu pro filtraci síťového provozu. To je v pořádku, v současnosti ale máme již k dispozici novou generaci firewallů (Next-Generation Firewall (NGFW)). Ta má navíc schopnosti hloubkové analýzy packetů, což umožňuje tomuto zařízení aplikovat výrazně širší pravidla pro filtrování. NGFW proto v sobě obvykle kombinují také funkcionalitu IDS/Intruder Prevention System (IPS).

To je ohromný posun v oblasti bezpečnosti. Do uvedení těchto firewallů jsme byli odkázáni na dedikovaná zařízení IDS/IPS, pomocí kterých jsme analyzovali určitou část síťového provozu obvykle formou zrcadlení síťových portů na managovatelném switchi. Tím, že přes firewall by měl směřovat veškerý síťový provoz bude z pohledu bezpečnosti pokryta síť podstatně lépe.

Toto řešení také do jisté míry zjednodušuje úvahy o bezpečnostní architektuře sítě.

Z hlediska segmentace sítě, kromě základní segmentace uvedené na obr. 2.5 (a popsané v předchozím textu) často oddělujeme také:

- wi-fi přípojné body a k nim připojená zařízení
- oddělení geograficky vzdálenějších lokací v síti organizace (např. síť FBI od zbytku sítě VŠB-TU Ostrava)
- oddělení částí sítě se specifickými požadavky na bezpečnost (např. z důvodu manipulace s citlivými údaji)
- oddělení automatizační sítě (ve výrobních firmách se stará o provoz výrobních linek apod.)
- oddělení senzorů zařízení IoT od běžného síťového provozu
- a další

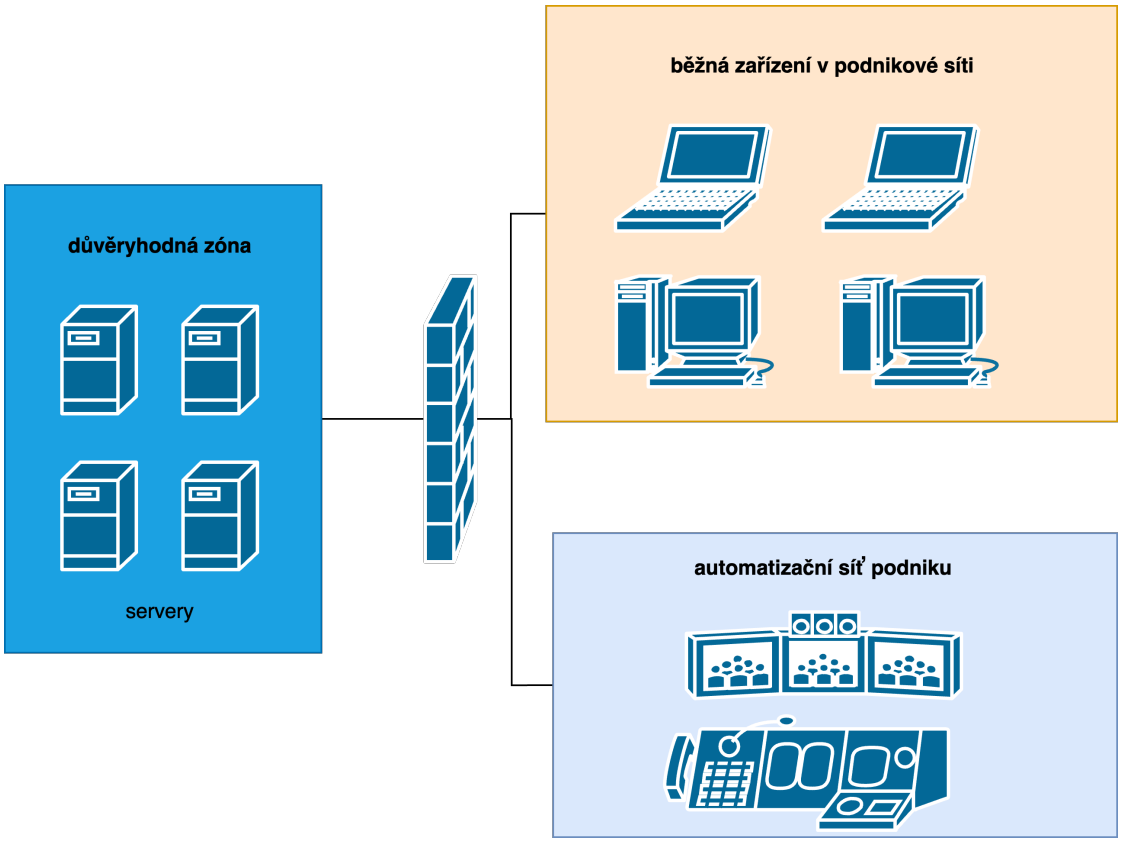
Vemte prosím v úvahu, že výše uvedený seznam není konečný. Jedná se spíše o seznam nápadů, které by nás při úvahách o architektuře sítě mohly inspirovat.

Všimněte si, že se oklikou mimo jiné vracíme k problematice wi-fi. Z hlediska vnitřního perimetru sítě je problémem zejména to, že nad těmito zařízeními nemáme prakticky žádnou kontrolu. Neprovádíme obvykle jejich předchozí registraci, zařízení přicházejí a odcházejí, pohybují se po areálu organizace, nebo minimálně v dosahu bezdrátové sítě a to z nich činí zařízení jen o něco málo bezpečnější než v případě všech zařízení na Internetu.

Na rozdíl od ostatních zařízení na Internetu se k připojení k bezdrátové síti musí zařízení alespoň nějakou formou autentizovat. Přesto úroveň důvěry, která tímto způsobem vzniká je poměrně malá, což vyžaduje pečlivé filtrování síťového provozu z a do takových zařízení.

Velká část odrážek v seznamu začíná slovem *oddělení*. Tím je myšleno, že určitou část sítě chceme řešit z pohledu bezpečnosti samostatně. Podívejte se na příklady dvou možných řešení filtrace sítě mezi běžnou sítí, automatizační sítí a důvěryhodnou zónou (servery na obr. 2.6 a 2.7).

V řešení předkládaném na obr. 2.6 je veškerý síťový provoz realizován prostřednictvím jediného firewallu, kterým musí síťová komunikace procházet. Jedná se o řešení, které je svým způsobem ele-



Obrázek 2.6: Síťový provoz mezi segmenty sítě filtrován pomocí jednoho firewallu

gantní a jednoduché. Konfiguraci pravidel síťového provozu provádíme na jediném místě, systém bude mít jediného správce, což jsou asi dvě nejvýznamnější výhody tohoto řešení.

Bohužel je s ním spojena také řada nevýhod. Veškerá komunikace prochází jedním uzlem, to prakticky znamená, že pokud uděláme chybu v konfigurace nebude v síti projde i taková komunikace, která by projít neměla. Z tohoto důvodu někdy preferujeme použití systém většího počtu firewallů, jak je naznačeno na obr. 2.7.

Změna je v použití více firewallů. Na obr. 2.7 odpovídá jeden firewall každé síti. V praxi tomu tak úplně být nemusí, základní princip zobrazený na obr. ale zůstává zachován. Myšlenka je taková, že každý firewall ošetřuje pouze síťovou komunikaci, která ma jít z a do této jedné sítě. Veškerá ostatní síťová komunikace je zakázána. To ma několik výhod:

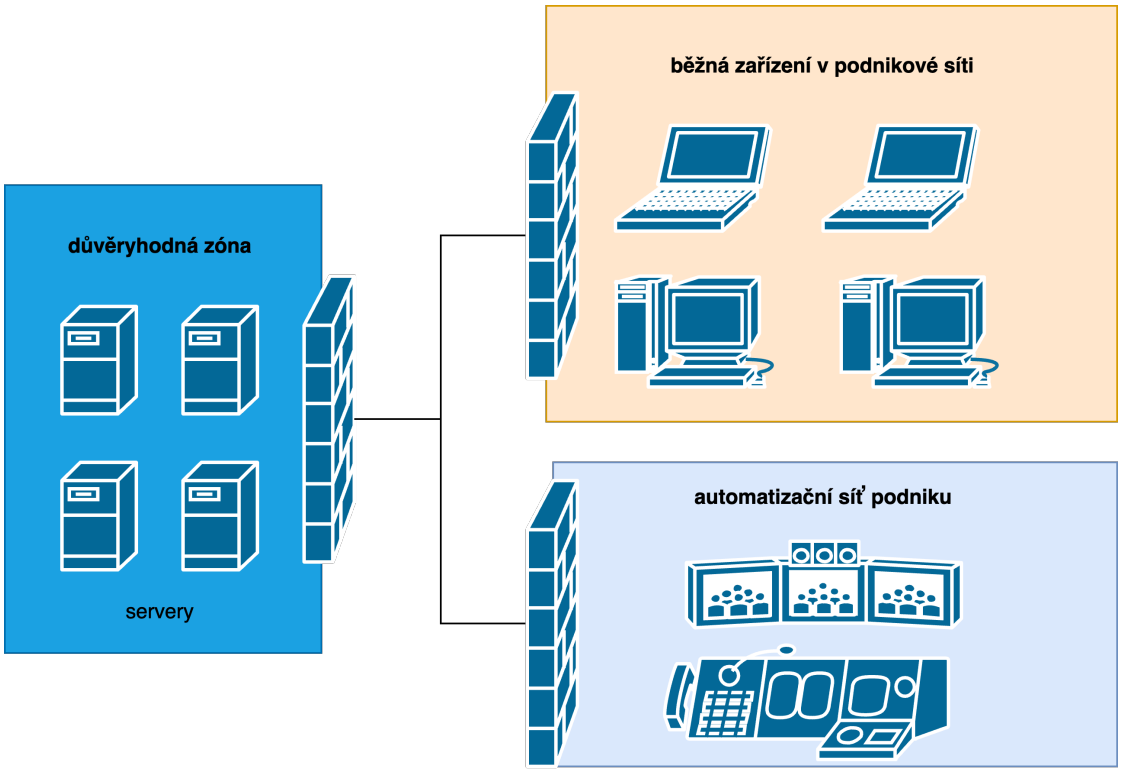
- sada pravidel na firewallu je menší a proto je lépe kontrolovatelná
- bezpečnost nezávisí na jediném člověku - každý firewall bude mít svého administrátora
- pro to, aby komunikace prošla do jiné sítě musí být povolena na dvou firewallech. I kdyby vinou chyby konfigurace prošla přes jeden, je nepravděpodobné, že stejnou chybu udělá i druhý administrátor. (odolnost vůči lidským selháním)

Nevýhodou tohoto přístupu je, že je dražší. Platíme fyzická zařízení (firewally) a to jednak jejich pořízení, tak také jejich provoz a také administrátory, kteří je budou muset spravovat.

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
- a jiná nositelná elektronika



Obrázek 2.7: Síťový provoz mezi segmenty sítě filtrován pomocí řady firewallů

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 nikdo jiný. Takže ani manželka/manžel, dítě ani náhodný kolemjdoucí jménem Ted. Toto omezení je pravděpodobně snadno pochopitelné. Jenomže pokud zařízení nemáme, jako organizace, fyzicky 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 taková bezpečnostní pravidla dodržují 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)

přičemž organizace obvykle usiluje o přiměřené využití obou výše uvedených nástrojů.

Z hlediska **šifrování** vlastně už nejsme úplnými nováčky. V Bezpečnostní informatice jsme společně nasáli základní principy fungování symetrických i asymetrických šifer včetně některých nástrojů, které je využívají. Proto se v tomto textu omezíme spíše jen na možnosti, které nám v tomto ohledu nabízejí jednotlivé operační systémy.

Windows ve verzích určených pro podniky (enterprise verze) poskytuje 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.

Pokud nepoužíváme Windows, nebo nemáme tu správnou verzi tohoto operačního systému, nebo prostě pouze chceme použít nějakou alternativu k Bitlocker - můžeme využít *VeraCrypt* [21].

VeraCrypt je open source nástupce legendárního šifrovacího programu True Crypt. Je dostupný pro všechny používané operační systémy, podporuje nejmodernější (nejbezpečnější) šifrovací algoritmy a jeho zdrojové kódy procházejí v pravidelných intervalech nezávislým auditem. Účelem je zvýšit úroveň důvěryhodnosti tohoto software.

Také ostatní operační systémy mají zabudován podporu šifrování disků. V případě operačního systému Linux je kromě možnosti použití VeraCrypt možno 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).

Moderní hardware dnes již má hardwarovou podporu šifrovacích algoritmů jako je Advanced Encryption Standard (AES) a další. To znamená, že aktivací šifrování nedochází ke znatelnému zpomalení práce operačního systému, ani nespotřebovává výrazně více elektrické energie.

Jaké šifrování použít?
Volba šifrovacího nástroje nebývá jednoduchá jelikož každý z těchto nástrojů má jisté výhody a nevýhody. Z tohoto důvodu můžeme nabídnout pouze určitá obecná doporučení stran šifrování:

- disky by měly být šifrovány
- šifrování by mělo být nastaveno na co možná nejvyšší nástrojem podporovanou úroveň
- pokud pracujeme jen a pouze s jedním operačním systémem, je efektivní použít šifrovací nástroj přímo v operačním systému
- systémový disk počítače může také být šifrován pomocí nástroje OS (předpokládáme spuštění daného počítače)
- pokud potřebujeme šifrovat přenosná média a přecházet s nimi mezi různými počítači lze doporučit použití nějaké specializovaného nástroje.
- **bez ohledu na to, co použijete, vždy musíte mít připravenou cestu zpět (obnova dat).** Bez klíče jsou data zcela bezpečná, jelikož je nepřečtete ani Vy jako oprávnění vlastníci.

Závěrečné upozornění k šifrovacím nástrojům v operačních systémech. Proces šifrování a dešifrování je hluboce zaveden přímo do operačního systému a způsobu jakým pracuje. Obvykle proces dešifrování začíná v okamžiku, kdy se uživatel přihlásí do systému. Přihlašovací údaje se použijí pro dešifrování symetrického šifrovacího klíče, kterým jsou šifrována data uživatele.

To je výhodou, ale zároveň také nevýhodou. Můžeme totiž uvažovat scénář, kdy uživatel zapomene své heslo. Takové věci se stávají ... bohužel. Řešení je reset hesla (jeho přenastavení administrátorem). Uživatel se pak do systému přihlašuje pomocí původního uživatelského účtu, ale s jiným heslem. Problém je, že původní heslo bylo použito pro zašifrování klíče potřebného pro dešifrování dat. Takže data zůstávají v takovém případě nedostupná.

Z hlediska bezpečnosti je takový výsledek v pořádku - data jsou bezpečná, nikdo je nepřečte. Z hlediska užitnosti se ale nejedná o optimální řešení. Potřebujeme proto vybudovat nějakou cestu k obnově dat pro případ nějakého katastrofálního selhání.

Řešením může být klíč vytisknout a uložit jej např. v trezoru, nebo na jiném bezpečném místě. Tady je ale potřeba zmínit jednu velmi důležitou věc: vždy je potřeba si uvědomit, před čím se potřebujeme vlastně chránit. Volbou zašifrování disku chráníme data na něm obsažená před zneužitím v případě odcizení zařízení/disku.

Pokud máme klíč bezpečně uložen ... někde. Otevíráme si možnost pro jeho případné nasazení pro obnovu dat z takového disku. Zároveň ale otevíráme možnost případnému útočníkovi ke kompromitaci tohoto hesla a jeho případné zneužití. Zde záleží na tom, jak cenná jsou vlastně uložená data. Z hlediska většiny jednotlivců lze říci, že pravděpodobně nebudou příliš cenná. V organizacích tomu tak ale být nemusí.

Může se jednat o velké množství intelektuálního vlastnictví, které může chtít získat např. naše konkurence. Může se jednat o velké množství osobních údajů, které jsou zneužitelné pro vydírání apod. Čím jsou data cennější, tím vyšší úsilí předpokládáme, že útočník vynaloží, aby k nim získal přístup.

Pro jednotlivce je tak nepravděpodobné např. fyzické vloupání do kanceláře za účelem získání takového hesla. Pokud se ale bavíme o průmyslové špionáži nebo dokonce špionáži jako takové nelze tuto možnost vyloučit.

Na úrovni *tabletů a mobilních telefonů* je šifrování již vlastně standardem. Moderní hardware mobilního telefonu/tabletu podporuje nejpoužívanější šifrovací algoritmy a tak je jejich použití rychlé a energeticky efektivní.

Na rozdíl od počítačů v případě přenosných zařízení používáme pro šifrování prakticky výhradně služby operačního systému. Proces dešifrování je tak spojen s procesem autentizace uživatele do systému. Metodám autentizace máme věnovanou jednu celou kapitolu, takže podrobnosti o bezpečnostních aspektech naleznete tam.

Možnosti vzdáleného výmazu zařízení

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. Telefony a tablety s operačním systémem Android je možno vzdáleně blokovat, smazat nebo hledat, pokud je toto zařízení připojeno ke Google účtu, přičemž v západním svetě jsou Android zařízení prakticky vždy připojena 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. Wi-Fi 7
6. WPA2, lepe však WPA3, pokud to připojená zařízení podporují
7. V podnikovém nasazení je často připojení do bezdrátové sítě je spojeno s autentizací proti jednotnému systému řízení identit uživatelů.

Kapitola 3

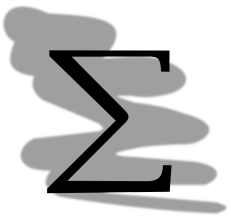
Autentizace a autorizace v počítačových systémech

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.



Předpokládané znalosti
Do této kapitoly vstupujeme s některými předpoklady o Vašich znalostech. Předpokládáme, že jste absolvovali předmět Bezpečnostní informatika, nebo jste se minimálně seznámili s jeho obsahem v oblasti šifrování a bezpečných hashovacích funkcí. Ná základě svého studia byste měli vědět:

- rozdíl mezi symetrickým a asymetrickým šifrováním
- základní algoritmy, které k tomuto používáme
- jak fungují certifikáty (elektronický podpis)

Tato kapitola úzce navazuje na kapitolu předchozí, tudíž byste ji měli prostudovat předtím, než se pustíte do kapitoly této.

Výše uvedené informace nebudou v tomto textu opakovány! Pokud si nejste jisti některým z výše uvedených pojmů doporučujeme před započetím dalšího studia Prostudovat znovu skripta z Bezpečnostní informatiky [72], nebo výše uvedené pojmy dohledat na Internetu.

3.1 Autentizace a autorizace

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

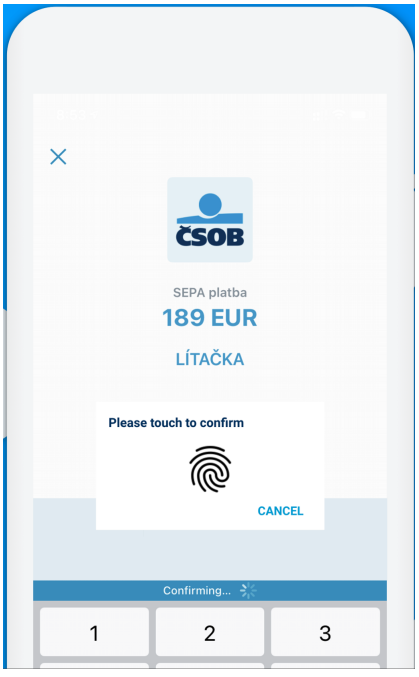
1. znalostí
2. vlastnictvím
3. vlastností

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 dokončení autentizace - uživatele tedy úspěšně prokázal systému svou identitu, ale vykonal v systému činnost takové závažnosti, že systém navíc vyžaduje autorizaci této činnosti. Nejjednodušší příklad, se kterým máme všichni praktickou zkušenost, je použití elektronického bankovnictví. Do bankovnictví se hlásíme pomocí svého uživatelského jména a hesla, pro provedení transakce jsme ale obvykle vyzváni k nějaké jiné formě ověření. V minulosti to bylo často přepsání kódu zaslaného bankou pomocí SMS na náš mobilní telefon, dnes je to častěji potvrzení činnosti v specializované aplikaci pro mobilní telefony.

Příkladem aplikace tohoto typu je ČSOB Smart Klíč, viz obr. 3.1. Dnes ale již téměř každá banka má obdobnou aplikaci.



Obrázek 3.1: Okno aplikace ČSOB Smart Klíč v operačním systému Android (převzato z [71])

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, 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.

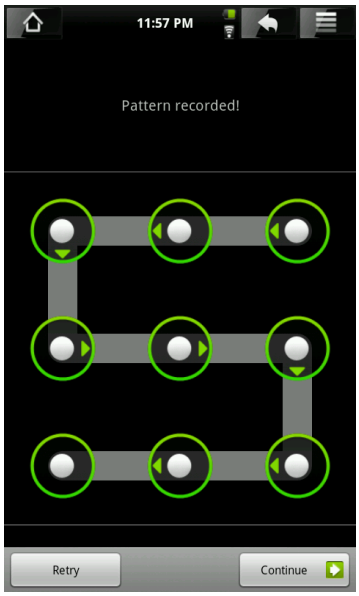
Prvním problémem je samotný display. Lidská kůže má totiž jednu nepříjemnou vlastnost - je mastná. Prakticky to znamená, že všechny dotykové displaye jsou do určité míry „zapatlané“. V těchto šmouhách je pak často možno identifikovat vzory, které pak lze využít pro odemknutí.

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. 3.2.

Tabulka 3.1: Možný počet kombinací - gesta vs PIN (převzato z [53])

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



Obrázek 3.2: Odemčení telefonu gestem (převzato z [53])

Výše uvedené metody autentizace jsou jinak 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):

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

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 silo 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 - $k = 99^8 = 9\ 227\ 446\ 944\ 279\ 201$

Ještě poslední poznámka k odhalování hesel číslo k v (3.1) představuje celkovou velikost prostoru všech možných hesel. Z praktického pohledu prolamování ale máme stejnou pravděpodobnost že hledané heslo bude v první i druhé polovině tohoto prostoru. Průměrně se tak z hlediska vyžadovaného počtu pokusů pro prolomení dostáváme na hodnotu $k/2$.

Alternativou k šifrování hesla je uložení hesla formou hashe - tedy výsledku jednocestné matematické kryptografické funkce.

Podobně jako šifrovací algoritmy, ani bezpečné hashovací funkce by pro Vás neměly být zcela nové. Proto pouze připomínáme, že 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 ale není - výsledkem je vždy textový řetězec o přesně stanovené délce odpovídající použitém algoritmu hashovací funkce.

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*.

Obecně slabé heslo je takové, které neodpovídá bezpečnostním doporučením na jeho délku a způsob konstrukce. Např. NIST SP 800-63B doporučuje minimální délku hesla 8 znaků, za předpokladu, že

takové heslo je náhodně generované. Problém u dlouhých hesel je to, že ve skutečnosti jsou obvykle sestavena velmi předvídatelným způsobem. Ve výsledku pak takové heslo nemusí nutně poskytovat úroveň ochrany, která by odpovídala čistě matematickému pohledu rovnic (3.1) a (3.2).

Slabé heslo je tedy 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.

Všimněte si, že útok v tomto případě není veden na přihlašovací údaje jako takové, ale zbývající části autentizačního mechanismu. To je logické, útočník si bude vždy vybírat tu nejjednodušší cestu pro dosažení svých cílů. Z tohoto důvodu je potřeba mít vhodně vyřešený tento problém jako celek, tedy všechny části autentizačního řešení musí být bezpečné.

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. Ve velkých organizacích mohou být takových účtů desítky tisíc nebo dokonce statisíce. Je proto statisticky nepravděpodobně, že v takovém množství účtů budou úplně všechny používat skutečně silná hesla, zejména pokud „sílu“ hesla nijak nekontrolujeme.

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, 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.

Rainbow tables je možno předpřipravit používat opakovaně.

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.

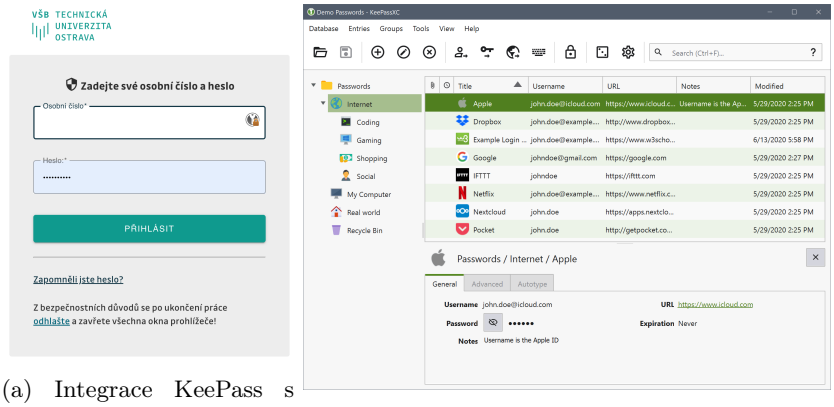
Silná hesla a možnost jejich ztráty

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.

Při diskuzi o heslech je potřeba také zmínit způsob jejich uložení a nyní nemáme na mysli jestli jsou zašifrovaná nebo je uložen jejich hash (ideálně osolený), ale spíše jaký software je k tomuto účelu využíván. Čistě statisticky je nejpoužívanějším softwarem pro ukládání hesel webový prohlížeč. Velká část služeb, které využíváme je totiž on-line a je proto logické, že uživatelé ukládají hesla právě zde.

Z pohledu bezpečnosti se nejedná o dobré řešení. Problém je zejména v tom, že pokud útočník kompromitoval daný počítač, pak pro něj budou tato hesla přímo přístupná. Webový prohlížeč z tohoto pohledu neposkytuje další úroveň ochrany (nad úrovní běžného přihlášení do systému).



(a) Integrace KeePass s webovým prohlížečem

(b) Základní GUI programu KeePassXC

Obrázek 3.3: Manager hesel KeePassXC a jeho integrace s webovým prohlížečem

Správný postup by bylo použít specializovanou aplikaci připojenou k webovému prohlížeči pomocí patřičného rozšíření. V případě potřeby zadat přihlašovací údaje bude uživatel vyzván k zadání hesla, které bude dešifrovat databázi hesel specializované aplikace. Tady už určitá přidaná hodnota existuje. Příklad takové aplikace je dostupný na obr. 3.3.

Pro uživatele je přístup do managera hesel vždy na vyžádání. Uživatel tedy musí kliknout na ikonu klíče, viz obr. 3.3a, zadá heslo do managera a ten pak vyplní heslo k zadanému uživatelskému jménu.

Různé managery hesel mají různé vlastnosti. Např. KeePassXC prošel auditem zdrojového kódu, a má vyřešenou ochranu proti dělání screenshotů. To je užitečné proti některým druhům malware, které tímto způsobem kompromitují údaje, se kterými uživatel pracuje.

Cena takových nástrojů je různá. KeePassXC [35] je dostupný zdarma (jedná se o open source), existují ale také komerční produkty. Základní funkcionalita je obdobná, rozdíly mohou být v některých dodatečných funkcích. Např. LastPass [30] ukládá hesla do cloudu a umožňuje jejich synchronizaci napříč různými zařízeními a to včetně mobilních.

Cloudová funkcionalita může být považována za výhodu nebo naopak slabinu řešení podle toho, jak na problém nahlížíte.

Použití managera hesel je každopádně doporučováno pro následující bezpečnostní benefity:

- konsolidace hesel na jednom, dobře zabezpečeném místě
- ochrana proti pořizování snímků obrazovky
- lepší komunikace bezpečnostních aspektů tvorby hesel, včetně generátoru bezpečných hesel
- podporuje základní bezpečnostní princip, že každá služba by měla mít samostatné heslo, s použitím manageru hesel si jej uživatel nebude muset pamatovat a bude proto náchylnější k tomu postupovat z hlediska bezpečnosti správně.

Další otázkou z pohledu bezpečnosti je *jak dlouho by mělo být zadané heslo platné*? Dlouho přijímaným faktem bylo doporučení na omezení délky platnosti hesla. Většina časových limitů bývá nastavována na úroveň několika měsíců až jednoho roku. Toto doporučení bylo odvozováno od představy, že v případě získání hesel v zašifrované podobě (nebo podobě osolených hashů) tak čím delší dobu útočník získá, tím vetší pravděpodobnost úspěšného prolomení bude mít. Tedy doporučení předpokládá útok hrubou silou na bezpečnost hesla jako základní bezpečnostní problém, který řešíme omezením platnost tohoto hesla.

Výše uvedená představa ale neodpovídá realitě, jelikož většina útoků nepostupuje hrubou silou, využívá ale různých zranitelností v systému nebo hledá slabá hesla. Paradoxně doporučení na pravidelnou změnu hesel bezpečnost může naopak zhoršit, zejména pokud je kombinováno s absencí implementace manageru hesel. Uživatelé totiž budou volit takové heslo, které si zapamatují, což může být např. původní heslo a číslo, např. pořadové nebo roku. Takové heslo ale není silné.

Z tohoto důvodu NIST SP 800-63B doporučuje heslo měnit ne častěji než jedenkrát za rok a nebo v případě, že došlo ke kompromitaci účtu nebo systému s potenciálem kompromitovat daný účet.

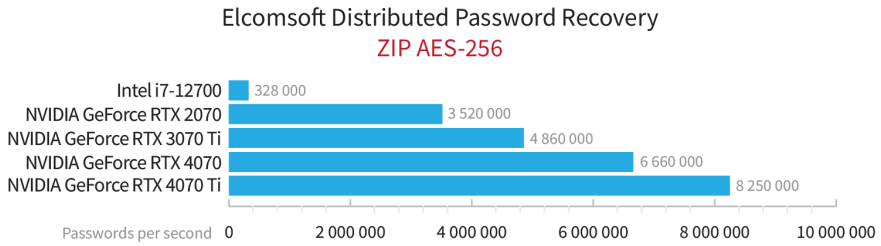
Každopádně délka platnosti hesla by měla být vynucována systémově. To znamená, že by ji v systému měl nastavit administrátor globálně pro všechny účty a systém by pak měl použít toto nastavení k automatickému upozornění uživatelů, kterým heslo v dohledné době expiruje a v případě, že ve

stanovené době toto heslo nezmění by daný účet měl být zablokován.

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 grafu společnosti Elcomsoft, která se zabývá vývojem software pro prolamování hesel do různých systémů, viz obr. 3.4.



Obrázek 3.4: Výkon louskání hesel pro ZIP AES-256 (převzato z [38])

Jediným představitelem CPU na obr. 3.4 je Intel i7-12700. Jedná se o procesor s 8-mi výkonnými jádry a 4-mi úspornými jádry. Maximální frekvence, které je procesor schopen dosáhnout je 4,9 GHz. Nejedná se o naprosto nejvýkonnější procesory, které jsou dostupné na trhu. Např. poslední generace procesorů firmy AMD Epyc 9004 (Genoa) určená pro servery má k dispozici až 96 jader, ale také nižší taktovací frekvence.

Všimněte si že pro srovnání jsou pak použity grafické karty vyšší střední třídy od společnosti NVidia. Lze říci, že výpočty na grafických kartách jsou řádově rychlejší. Při mezigeneračním srovnání pak dochází k téměř 2x zvýšení výkonu pro tento typ výpočtů.

Z komerčního hlediska pak můžeme udělat jednoduchý výpočet efektivity založený na současných cenách výše uvedených produktů, viz tab. 3.3. Pro zajímavost byla do tab. doplněn také procesor AMD Epyc 9004. Hodnoty ale v tomto případě byly pouze odhadnuty za předpokladu shodného Instruction Per Cycle (IPC) a škálované podle počtu jader a frekvencí.

Tabulka 3.3: Prolamování šifrování hrubou silou - úvahy o efektivitě (adaptováno z [38])

hardware	**výkon** (mil. pokus/s)	**cena**[1] (tis. Kč)	**efektivita** (mil. pok/tis. Kč)
Intel i7-12700	0,328	8	0,041
AMD Epyc 9004[2]	5,932	260	0,023
Nvidia GeFoce RTX 2070	3,52	13	0,271
Nvidia GeFoce RTX 3070 Ti	4,86	16,5	0,295
Nvidia GeFoce RTX 4070	6,66	16,5	0,404
Nvidia GeFoce RTX 4070 Ti	8,25	22	0,375

3.3 představuje alternativní pohled na problém prolamování hesel hrubou silou a to ekonomický. Případný útočník do prolomení musí investovat nemalé finanční prostředky a proto nejefektivnější způsob, jak tak učinit. Součástí úvah tak nejsou pouze úvahy o samotné rychlosti. Všimněte si brutální rychlosti AMD Epyc, ale při ceně procesoru 260 000,- Kč se prostě nejedná o efektivní řešení, pokud obdobné rychlosti mohu dosáhnout s použitím grafické karty RTX 4070 za 16,5 tis. Kč.

[1] ceny jsou k 29.6.2023
[2] odhad při 96 jádrech běžících na 3,7 GHz

Případný útočník tak musí velmi pečlivě kalkulovat, jak k problému přistoupí. Prosím neber3.3 jako úplně přesný benchmakr, spíše se jedná o orientační výsledky, na základě kterých si ale můžeme udělat jistou představu o výkonu na moderním hardware. Skutečný útočník, by pravděpodobně investoval více času a prostředků do podrobnějšího testování různého hardware ale také různých softwarových prostředků, které k tomuto účelu lze využít.

Různé softwary totiž potřebné algoritmy mohou mít implementovány s různou mírou efektivnosti a tak některé softwary mohou na určitém specifickém hardware být výrazně rychlejší, než na jiném.

Vzhledem k tomu, že předchozí tab. byla zaměřena na šifrování, uvádíme pro porovnání také některé testy s bezpečnými hashovacími funkcemi, viz tab. 3.4.

Tabulka 3.4: Prolamování bezpečných hashovacích funkcí hrubou silou - úvahy o efektivitě (adaptováno z [49])

hardware	**algoritmus**	**výkon** (mil. pokus/s)	**cena**[3] (tis. Kč)	**efektivita** (mil. pok/tis. Kč)
NVidia GeFoce RTX 2070 Super	MD5	34762,3	17,5	1986,417
	SHA1	11034	17,5	630,514
	SHA-256	4268,5	17,5	243,914
NVidia GeFoce RTX 3080 Ti	MD5	64368	20	3218,400
	SHA1	20632,8	20	1031,640
	SHA-256	8817	20	440,850
NVidia GeFoce RTX 3090	MD5	65079,1	54	1205,169
	SHA1	22757,6	54	421,437
	SHA-256	9713,2	54	179,874

Na stránkách společnosti Elcomsoft [44], 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 [11] 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

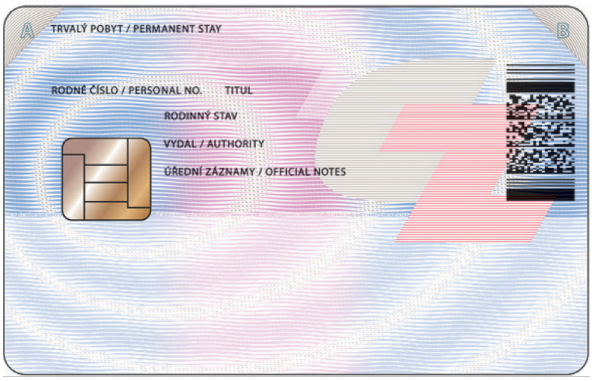
Příkladem **průkazu se strojově čitelnými údaji** je např. občanský průkaz. Strojově čitelná zóna je na zadní straně průkazu vpravo, viz obr. 3.5. V současnosti všechny vydávané občanské průkazy jsou zároveň také čipovými kartami schopnými uchovávat v šifrované podobě certifikáty, např. pro účely autentizace vůči různým webovým službám státní správy nebo pro účely elektronického podepisování dokumentů.

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.). Paradoxně oba čipy jsou více méně stejné. Protože jejich výroba je natolik levná, že se jejich výrobci nevyplatí vyrábět nějakou „odhlehčenou“, méně bezpečnou verzi.

Náhled vzhledu průkazu je na obr. 3.6.

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.

[3] ceny jsou k 29.6.2023 ovšem s tím, že RTX 2070 Super a 3090 se již běžně neprodávají, jedná se tak v jejich případě o poslední známou „retail“ cenu



Obrázek 3.5: Zadní strana občanského průkazu (převzato z [61])

Obrázek 3.6: Průkazka studenta (převzato z [67])

Představu o vzhledu tokenu je možno si udělat z obr. 3.7. 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.

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.

Výjimku v tomto smyslu představují různé smart klíče, které se doinstalovávají jako aplikace do mobilního telefonu, popř. tabletu. Jejich použití vyžaduje, aby uživatel prokázal svou identitu telefonu/tabletu, tedy odemknul jej a také aby aplikace byla vhodně nastavena. To obvykle vyžaduje její autorizaci v systému. Např. Google autentikátor je spojen s Google účtem, Smart klíč, který používá ČSOB vyžaduje spojení s Vaším účtem u této banky atd.

Tento způsob je relativně jednoduchý, levný a tak jej používá celá řada různých produktů a služeb. V posledních letech se pomalu propracovává také do podnikové sféry jako doplněk použití běžných přihlašovacích údajů, tedy jako jeden z faktorů dvou-faktorové autentizace.

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 au-

Obrázek 3.7: RSA SecurID SID800 token bez USB konektoru (převzato z [25])

tentizace vlastností se v praxi používají:

- sken siluety ruky
- snímání otisku prstu
- sken žilkování na dlani
- skenování oční duhovky
- skenování oční sítnice
- kontrola proti obrazu vlastníka

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. 3.8 jsou znázorněny příklady nejčastěji použitých snímačů v mobilních telefonech a noteboocích (viz obr. 3.9).

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 úplný otisk prstu a bylo tak jedno kterou částí prstu se snímače dotknete. Snímač Lenova na obr. 3.9 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.

Zajímavé je, že např. Apple iPad Air (a také Pro) v posledních generacích podporuje také autentizaci otiskem prstu. Ta je realizována do tlačítka pro zapnutí zařízení a velikostně tak není signifikantně

(a) Touch ID v iPhone 5s (převzato z [19] (b) Samsung Galaxy S5 snímač (převzato z [9])

Obrázek 3.8: Apple iPhone 5s (Touch ID) vs skaner otisku prstu Samsung Galaxy S5

Obrázek 3.9: Čtečka otisků prstů v notebooku Lenovo ThinkPad 430 (převzato z [12])

větší nežli senzor na obr. 3.9, přesto neočekává přejetí senzoru prstem. Sejme prostě tu část otisku prstu, která byla přiložena a provede porovnání na základě toho, co má k dispozici.

K tomu je ale potřeba dodat, že v takovém případě není vyhodnocován celý otisk prstu a proto je šance na chybné vyhodnocení, zejména ve smyslu autentizace neoprávněného uživatele vyšší. Bohužel ale nejsou k dispozici přesná čísla, která by toto byla schopna kvantifikovat.

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.

We Windows se tato technologie technologie nazývá Windows Hello. Podrobněji se touto technologií budeme zabývat v části věnované *Identity managementu* později v této kapitole.

Rozdílná kvalita senzorů
Mějme na paměti, že ne všechny senzory jsou si z hlediska spolehlivosti rovny. Rozdíly ve spolehlivosti tak jsou nejen mezi různými technologiemi zaměřenými na snímání různých biometrických vlastností člověka, ale také mezi různými způsoby snímání jednoho biometrického znaku, např. otisku prstu.

Dobrým příkladem jsou jedny z prvních senzorů, které Samsung začal používat ve svých mobilních telefonech v roce 2019 (jednalo se o modely S10 a Note 10). Tyto využívaly moderní snímač na bázi ultrazvuku, který ale při použití silikonové ochrany obrazovky autentizoval úplně každého. Později Samsung uvedl některé softwarové opravy operačního systému, které tento problém minimalizovaly, mobilní telefony s tímto senzorem byly i pote ale přesto náchylnější k chybnému vyhodnocování otisků prstů.

Jako alternativu k snímání otisku prstu je možnost **snímání žilkování na dlani**. Výhodou je, že

(a) PalmSecure Mouse (převzato z [45] (b) Fujitsu Lifebook S935 (převzato z [7])

Obrázek 3.10: Snímače žilkování na dlani v zařízeních společnosti Fujitsu

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. 3.10. 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. 3.11. 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 [46]. 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 [26], který je však byl komerčně dostupný pouze v Číně.

Ještě okolo roku 2015-2016 se zdálo, že že právě skenování duhovky nebo sítnice budou ultimátní biometrickou metodou, kterou budou používat všechny mobilní telefony, jenomže se tak nestalo. Obě technologie se v současnosti používají, ale spíše ve formě statických snímačů používaných např. při kontrole vstupu do prostoru s řízeným vstupem.

Technologií, která se naopak prosadila bylo **skenování celého obličeje**. Důvodem, proč se skeny oka neujaly je to, že takový sken vyžaduje snímek oka ve vysokém rozlišení. Zrealizovat takový snímek automaticky nebo poloautomaticky pomocí selfie kamery mobilního telefonu tak, aby snímek obsahoval alespoň nějaké detaily použitelné pro kvalitní ztotožnění není úplně triviální.

Co je ale možné udělat poměrně jednoduše je snímek celého obličeje. Konečně všichni občas nějaké selfie pořídíme. Pokud systém dokáže takovou informaci použít pro autentizaci uživatele, dostaneme do rukou rychlý, jednoduchý a spolehlivý autentizační mechanismus, který lze velmi jednoduše masově nasadit bez nutnosti používat specializovaný dodatečný hardware (senzory) pro sejmutí biometrického údaje.

Nejjednodušší způsob, jak postupovat je replikovat přesně postup načrtnutý výše. Takovou strategii přijaly první modely mobilních telefonů s operačním systémem Android, které takový mechanismus

Obrázek 3.11: Kontrola identity členů městské rady Bagdádu pomocí skenu oční duhovky (převzato z [64])

implementovaly. Tento postup má však jednu velkou slabinu. Foto obličeje, které je pořizováno během autentizace stejně jako to, vůči kterému je porovnáváno jsou jenom to, tedy jedná se o dvou rozměrný obraz.

Logicky mobilní telefon v takovém případě nemá schopnost rozlišit, zda foto během autentizace je pořízeno snímkem skutečné osoby nebo třeba její vytištěné fotografie nebo dokonce fotografie v jiném mobilním telefonu nebo obdobném zařízení. Takovou fotografii je přitom poměrně jednoduché získat. Úroveň ochrany je v tomto případě velmi malá.

Autentizaci pomocí obličeje však lze realizovat i mnohem bezpečnějším způsobem. Technicky je ale vyžadováno použití minimálně dvou kamer, z nichž jedna by měla být schopna snímat obraz také v infračerveném spektru. Obě kamery jsou vedle sebe. Tato drobná separace společně s odlišným spektrem umožňují zařízení vytvořit 3D model obličeje, který je pak porovnáván s záznamem uloženým v zařízení.

Nejpodrobnější model si vytváří iPhony pomocí technologie Face ID, ilustrační obrázek je dostupný níže, viz obr. 3.12.

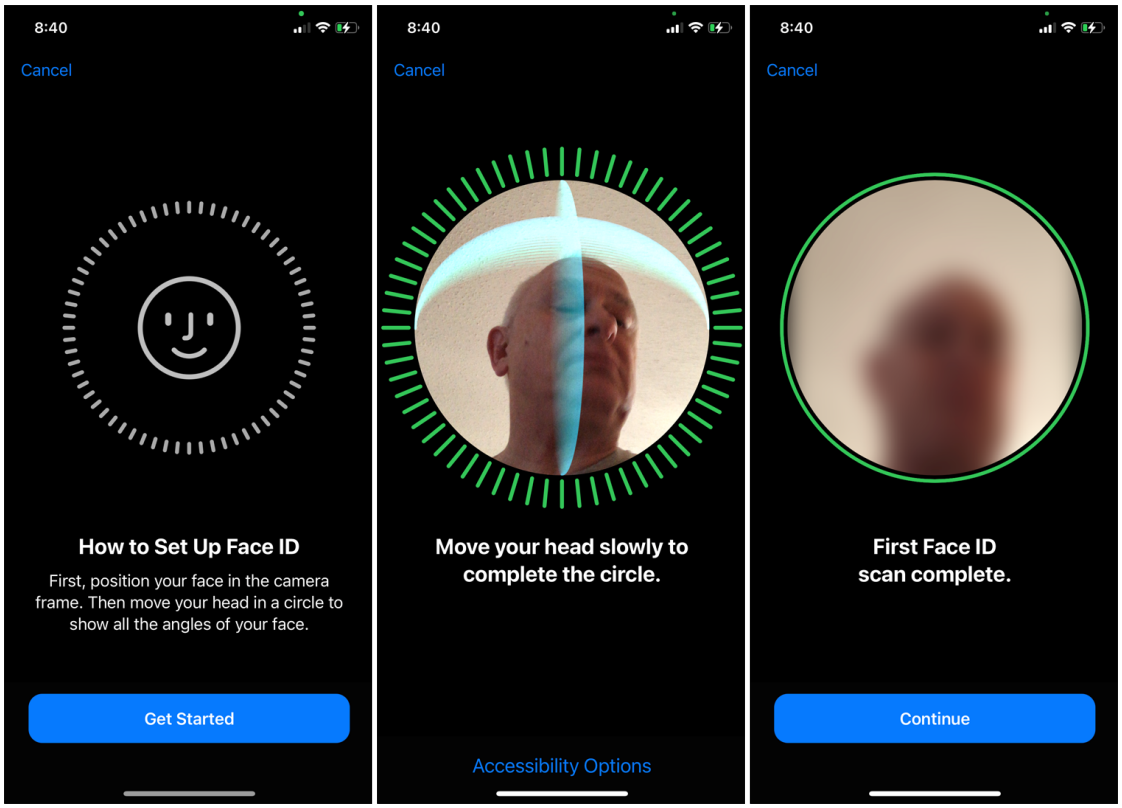
Obdobné požadavky jsou kladeny na autentizaci pomocí obličeje v systémech Windows pomocí Windows Hello.

3.1.4 Spolehlivost

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 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 [60]:

- Míra správného přijetí (True Acceptance Rate (TAR)) / Míra správného ztotožnění (True Match Rate (TMR)) - poměr reprezentuje schopnost biometrického systému správně identifikovat oprávněného uživatele.



Obrázek 3.12: Proces skenu v rámci Face ID (převzato z [70])

něného 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 [8], který v polovině roku 2015 zveřejnil více než 150 benchmarků pro více než 4 000 algoritmů vyhodnocování otisků prstů.

Zajímavé studie spolehlivosti realizovat také NIST pro rozpoznávání obličejů [48] a oticky prstů [68]. Chybovost vyhodnocení v tomto případě při hodnocení různých typů chyb jsou obvykle do 2 %. Cílová spolehlivost pro algoritmy se ale uvádí na úrovni 1: 100 000, což odpovídá chybovosti 0,001 %.

Pro porovnání přikládáme odhady potenciálu chyb při správném vyhodnocení dostupných markantů (rozlišovacích znaků).

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

Jedním z důvodů proč je chybovost tak velká je snaha výrobců zařízení zajistit, aby jejich uživatelé byli méně postihování neoprávněným odmítnutím přístupu. Problém je v tomto případě v poměru $TRR/TNMR$. Výrobci na základě svých průzkumů se jednoduše rozhodli, že pokud TNMR signifikantně narostlo, lidé by jej (resp. zařízení, která takto nastavené senzory používají) nepoužívali. Situace se tak sice postupně zlepšuje se zlepšováním spolehlivosti jednotlivých vyhodnocovacích algoritmů, přesto ale stále není dobrá.

Z hlediska bezpečnosti problematické je také nastavení mechanismu vypořádání se s chybou autentizace, zejména v případě použití mobilních telefonů. V případě, že identifikace pomocí biometrického údaje opakovaně selže, použije se autentizace pomocí PIN. Ta je ale obvykle považována ze ještě méně bezpečnou než je použití biometriky. Běžné chování tak odpovídá procesu: pokud selže autentizace pomocí bezpečného autentizačního algoritmu, použij autentizační algoritmus méně bezpečný.

Z pohledu bezpečnostnímu by ale situace měla být přesně opačná. Selhání jednoho autentizačního mechanismu by totiž mělo snížit důvěru v autentizovaného, proto na další pokusy by měly být používány důvěryhodnější autentizační mechanismy.

3.2 Identity management

3.2.1 LDAP a Active Directory (AD)

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 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.

Z hlediska strukturálního jsou objekty v IDM udržovány ve stromových strukturách. Ty mohou být někdy velmi složité. Na obr. 3.13 je dostupná jedno z možných řešení struktury TUO-NET. Upozorňuji, že v tomto případě se jedná pouze o ilustrační obrázek možného řešení, nikoliv toho jak přesně je strom navržen.

Důvodem je to, že reálné nasazení podléhá určitým dohodám a také způsobu, jak byl systém nastaven v minulosti, což se sice na jedné straně logické, ale bez hlubšího výkladu podrobností o těchto dílčích rozhodnutí by vlastně ani neplnil edukační úlohu. Proto se spíše zaměříme na teorii a pobavíme se o této problematice trochu obecněji.

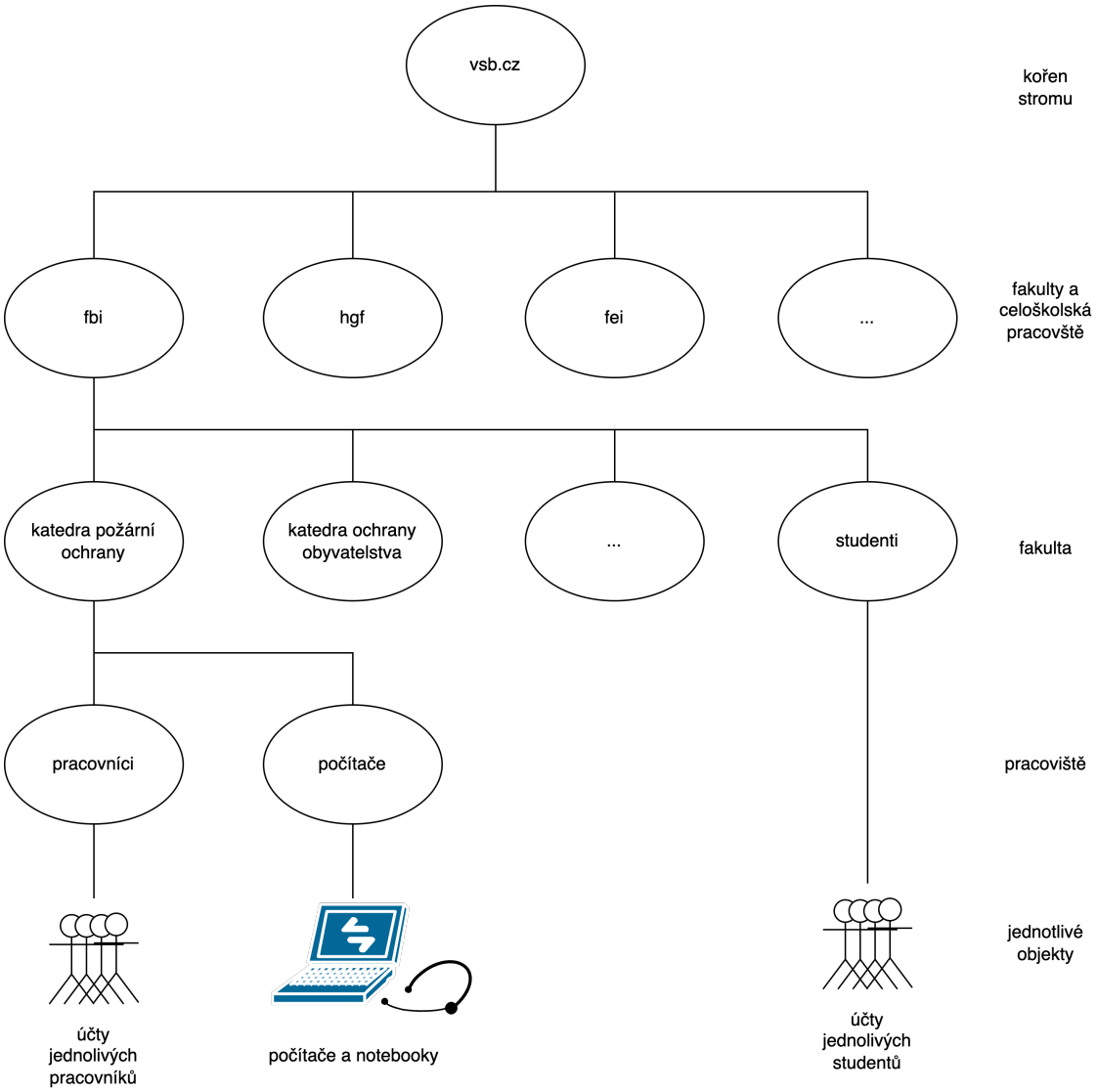
Nadnárodní společnosti mohou chtít používat jiné členění. Dokonce jim nemusí stačit jeden strom. V takovém případě ve výsledné struktuře (stále bude stromová) nehovoříme a stromu, ale o lesu. První úroveň v tomto případě bude tvořit právě les, další pak kořen jednotlivých stromů. Můžeme si to představit tak, že např. každý stát bude mít vlastní strom v tomto lese.

Změna v tomto případě není pouze terminologická, ale přímo technická. Tedy autentizace v rámci jednotlivých stromů bude probíhat pomocí samostatných IDM (LDAP/AD), které ale budou zapojeny právě do „lesa“.

V souvislosti s předchozí podkapitolo Vás možná napadne otázka, jak se do takového systému integruje **biometrika**. Zjednodušená odpověď je dost špatně. Existuje několik možností, ale každá z nich má některé slabiny. Zkusme se nejprve zamyslet jak taková autentizace vlastně vypadá.

Z předchozí podkapitoly máme jistou představu o způsobu jakým autentizace jako taková (v obecné rovině funguje). V této části textu se proto zaměříme již na specifika operačního systému Windows a integrace těchto metod v prostředí organizace.

Začněme tím nejjednodušším, a to autentizací pomocí biometrických údajů do Windows, s lokálním účtem. V tomto scénáři tedy paradoxně předpokládáme, že pracujeme s jednotlivcem nebo organizací, která nenasadila IDM, v tomto připadě Active Directory, což jde trošku proti smyslu této podklapitoly :-).



Obrázek 3.13: Možný příklad realizace stromu objektů v IDM pro VŠB-TU Ostrava

Nejjednodušší je v takovém případě použít přímo vestavěnou technologii Windows Hello, která je dostupná pro počítače s Windows 10 a 11. Snímek biometrického údaje je v takovém případě pořízen pomocí senzorů na daném počítači a spojen s uživatelským účtem (lokálně), ke kterému byl uživatel přihlášen, když povoloval Windows Hello. Ztotožnění tedy probíhá výhradně lokálně.

Takový přistup je ale při centralizované autentizaci vlastně nerealizovatelný, protože v takovém případě potřebujeme, aby biometrický údaj, proti kterému se bude uživatel ověřovat nebyl uložen lokálně ale na serveru - v systému IDM. To je problém, protože Active Directory instalované a provozované tzv. on-premise (tedy na vlastním hardware) takovou funkcionalitu nepodporuje. Musíme tak hledat alternativní řešení. Organizace může investovat do:

- samostatné platformy nějakého nezávislého dodavatele, která se do provozované infrastruktury ověřování uživatelů nějakým způsobem zapojí
- přechodu na cloudovou verzi Active Directory, na které je možno zprovoznit komponentu, která uvedenou funkcionalitu umožňuje

Pokud zvolíme alternativního dodavatele této služby budeme muset řešit ekonomické otázky nejen ve smyslu kolik nás bude stát pořízení licence na provoz této služby, ale také jakým způsobem budeme zajišťovat přihlašování uživatelů k této službě, otázky správy a také kompatibility s jednotlivými senzory.

Pro většinu organizací tak může být jednodušší druhá volba - přejít s autentizací do cloudu. V

současnosti lze jednoznačně říci, že je to trend, který Microsoft podporuje všemi možnými prostředky. Např. ve Windows 11, alespoň ve verzích určených pro domácnosti jsou již v tomto prostředí vytvářeny účty jednotlivých uživatelů. (Tento požadavek ale lze za určitých okolností obejít a i v takovém případě ... ale není to moc příjemné[4]). V korporátním prostředí toto Microsoft explicitně nevyžaduje, ale organizace se snaží k přechodu dotlačit absencí některých nástrojů, které jsou dostupné pouze v cloudové verzi.

Za určitých okolností může organizace dokonce již cloudové AD používat k jinému účelu, např. v případě že využívá služeb Microsoft 365 (původně Office 365). Integrace tak může dávat logický smysl a nemusí být ani příliš drahá.

Toto řešení má však také stinnou stránku - infrastruktura zajišťující vnitřní autentizaci uživatelů není v takovém případě ve vlastnictví dané organizace. Dokonce není ani umístěna fyzicky v síti dané organizace. Jako každá služba, může docházet k výpadkům, nebo být předmětem útoku. Byť v tomto případě Microsoft má zároveň mnohem lepší předpoklady (kapacity) se takovým útokům bránit.

A vzhledem ke „cachování uživatelských účtů“, není vyžadováno připojení k Internetu, tedy alespoň pokaždé když se uživatel hlásí do systému. Funguje to tak, že pokud existuje připojení k Internetu a služba AD běží na serveru uživatel se ověří vůči ví. V okamžiku ověření se přihlašovací údaje „nacachují“ a v okamžiku, kdy by došlo k pokusu o přihlášení bez připojení k Internetu nebo by služba AD neběžela dojde k ověření vůči právě těmto uloženým přihlašovacím údajům.

Z pohledu bezpečnosti se jedná samozřejmě o určitý kompromis. Lze si představit scénář, kdy je kompromitován účet, jeho oprávněný uživatel toto zjistí a změní heslo. Útočník, ale odpojí zařízení (PC/notebook), na kterém se uživatel v nedávné době přihlásil, od počítačové sítě a použije původní kompromitované přihlašovací údaje. Závažnost tohoto problému ale není úplně vysoká, jelikož vyžaduje fyzický přístup k zařízení. Pro omezení bezpečnostní dopadů je také obvykle omezen počet přihlášení, které provádějí takové ověření.

Celkově vzato se tedy jedná o poměrně efektivní nástroj pro překlenutí doby, kdy autentizační služba z nějakého důvodu není k dispozici.

Bez ohledu na to, jakou formu IDM máme některé logické cíle stran konfigurace uživatelských účtů, nebo chcete-li principy:

- princip nejmenších možných uživatelských práv
- přístup pouze k informacím, které uživatel potřebuje
- řízení přístupu na bázi rolí (Role-Based Access Control (RDAC))

Všechny tři výše uvedené principy spolu poměrně úzce souvisí. *Princip nejmenších možných uživatelských práv* je založen na tom, že každý uživatelský účet by měl mít nastavená pouze nezbytná práva, při kterých uživatel může vykonávat svou práci.

Jak jednoduché, že? Problém je, že každý uživatel v organizaci může mít trochu jiná práva. Pokud bychom proto realizovali takové nastavení u každého uživatele samostatně zvyšovala by se výrazně pravděpodobnost chyby a právě zde přichází na řadu dva zbývající principy.

Vzhledem k tomu, že uživatel by měl mít přístup jen k takovým informací, které nutně potřebuje pro výkon své práce musíme mít zmapováno s jakými daty/informacemi organizace manipuluje a jakým způsobem. Na základě této znalosti bychom měli být schopni mapovat vykonávané činnosti k těmto datům a informací a činnosti mapovat k jednotlivým uživatelům. Tento postup tvoří jádro jak *informační bezpečnosti*, tak *kybernetecké bezpečnosti*.

Již víme, že nastavovaní přístupových práv po uživatelích není efektivní. Proto bychom měli výše uvedené informace zobecnit k tzv. *rolím*.

Každý systém má obvykle dvě základní role: 1) administrátor, 2) uživatel. Přičemž administrátor má proti běžnému uživateli zvýšená práva do systémů. Je ale v našem zájmu, aby systém rolí být složitější.

V případě stromu 3.13 by např. bylo možné rozlišovat mezi administrativními, technicko-hospodářskými pracovníky a pracovníky vědy. Ke každé roli by mohl být přidělen nějaký úložný prostor a nastavena práva do určitých systémů.

Uživatelským účtům ve stromu pak přiřazujeme jednu nebo více rolí. Spolu s rolemi se pak účtu předělují (navyšují) práva. Jelikož rolí je mnohem méně než uživatelů, nastavit úroveň práv s nimi související není natolik složité z pohledu prvotního nastavení i jejich následné údržby. Z hlediska managementu je také výrazně jednodušší udržovat seznam uživatelů a jaká role mají mít přiděleny a přidělování rolí v IDM pak třeba automatizovat.

[4] proces je popsán např. v https://techbit.ca/2022/12/setup-windows-11-home-with-a-local-user-account/

Informační vs. kybernetická bezpečnost
Kybernetická a informační bezpečnost jsou úzce provázané problémy, byť je v praxi řešíme často samostatně. *Informační bezpečností* rozumíme snahu zajistit bezpečnost všech citlivých, nebo jinak cenných informací v organizaci.

Velká část těchto informací bude v elektronické podobě, což je předmět zájmu *kybernetické bezpečnosti*. Informace mohou být ale také ukládány např. v podobě listinné, nebo dostupné pouze jako know-how v hlavách zaměstnanců. Tyto dvě oblasti ale nejsou předmětem zájmu kybernetické bezpečnosti.

Naopak kybernetická bezpečnost se zabývá také bezpečnostními incidenty, které nemají potenciál narušit informační bezpečnost. Např. napadený počítač, který útočník využívá k těžbě kryptoměn nepředstavuje problém z pohledu informační bezpečnosti, pokud neobsahuje citlivé informace a útok nemůže eskalovat mimo hranice systému. Jedná se ale o problém z pohledu kybernetické bezpečnosti.

Mezi oběma pojmy tak existuje silný přesah a organizacím se tak často vyplatí oba problémy řešit integrovaně (společně), byť v praxi se tak ne vždy děje.

Informační bezpečnost vs. bezpečnost osobních informací
Další dva úzce propojené pojmy. Osobní informace jsou pouze podmnožinou všech informací, které jsou pro organizaci důležité. Dalo by se proto říci, že pokud správně zvládneme informační bezpečnost budeme mít zároveň automaticky zvládnutou také bezpečnost osobních informací.

Důvodem, proč ochranu osobních informací řešíme v podnikovém prostředí samostatně je to, že na jejich ochranu existuje řada přesně stanovených zákonných požadavků, které musí každá organizace zpracovávající takové údaje splnit. V Evropě všechny právní úpravy jednotlivých států vycházejí ze směrnice General Data Protection Regulation (GDPR).

3.2.2 Single Sign-On (SSO)

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. 3.14.

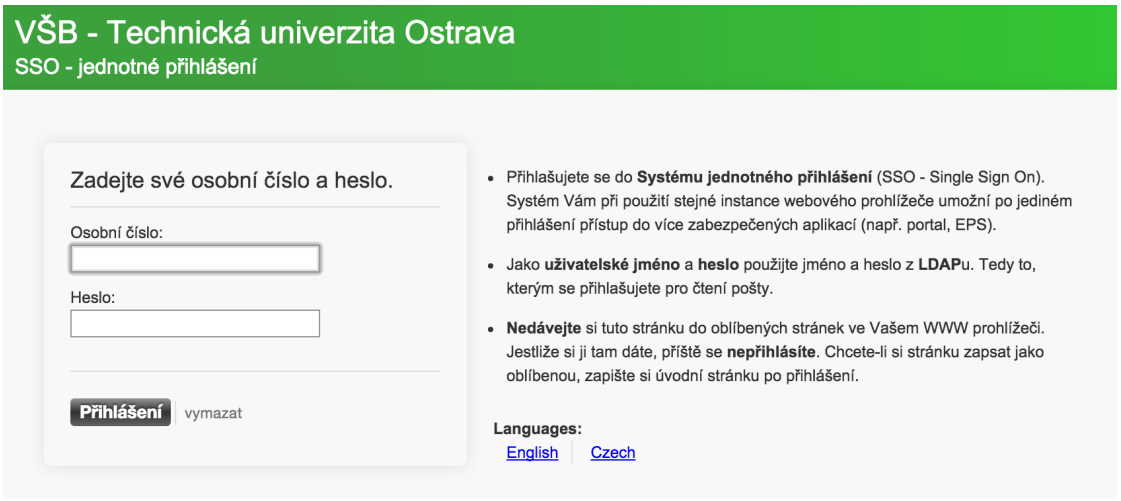
Použití SSO ale má také svou stinnou stránku, jelikož jedna kombinace uživatelského jména a hesla je využívána v řadě systémů organizace, kompromitace uživatelského účtu může mít dalekosáhlé následky. Útočník totiž získá přístup nikoliv k jedinému systéme, ale řadě systémů.

SSO je tedy opět do určité míry kompromisem mezi bezpečností a pohodlností. Tento kompromis, ale nemusí fungovat způsobem, který Vám možná napadne jako první. Na jedné straně sice budeme mít jediné uživatelské jméno a heslo v řadě systémů, na straně druhé ale nebudeme mít samostatná jméno a hesla v jednotlivých systémech organizace ... CO? Teď jsem Vás asi při čtení ztratil. Ale uvažujte nad tím.

Uvažujme scénář, ve kterém máme samostatný účet ke všem systémům organizace, např.:

- e-mail
- PC
- notebook
- nějaký informační systém (např. Edison)
- systém pro objednávání stravy
- apod.

Takových účtů může pak uživatel v organizaci potřebovat možná i několik desítek v závislosti na tom, co přesně dělá. Lze předpokládat, že ale většina lidí by tak v organizaci měla řekněme odhadem



Obrázek 3.14: SSO pro webové aplikace na VŠB-TU Ostrava

5 - 10 různých účtů. V každém z nich pak 1x ročně (nebo o něco častěji nebo méně často v závislosti na politice hesel) bude měnit heslo. Jak to asi dopadne?

- použije stejně stejné heslo napříč systémy
- použije hesla která jsou sice jiná, ale jsou všechna slabá
- pečlivě si je zapíše a uloží na dobře viditelném místě, aby k nim měl snadný přístup

Ano, bude existovat menšina uživatelů, kteří z pohledu bezpečnosti budou postupovat správně a žádnou z výše uvedených chyb neudělají. Útočník ale obvykle cílí na nejslabší článek, takže samostatnými účty se z hlediska bezpečnosti vlastně nepomůžeme.

Naopak SSO má některé výhody z pohledu bezpečnosti:

- zřizujeme jedno centralizované místo k autentizaci, které se nám bude lépe chránit
- tím, že si uživatel bude muset pamatovat jedno heslo je lepší předpoklad, že může být bezpečnější (silnější)
- v případě detekované kompromitace účtu můžeme na jednom místě změnit všechna hesla a tak zamezit dalšímu pokračování zneužití účtu a to aniž bychom zkoumali s kterým systém bylo s použitím účtu manipulováno
- pravděpodobně bychom mohli odvodit i další bezpečnostní výhody

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 evidovat 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.

Předpokládané znalosti
Předpokládáme, že jste zvládli základy počítačových sítí a šifrování, alespoň v rozsahu prvních dvou kapitol těchto skript.

Data jsou pro organizaci často to nejcennější, co má. Bez dat totiž nemohou procesy v organizacích fungovat. Nevěděli bychom třeba, co kdo objednal, jestli už zaplatil apod. Data jsou tedy živnou půdou fungování organizace. Při jejich ztrátě, popř. nedostupnosti organizace jsou nuceny řešit existenční problémy. To je také mimo jiné důvodem proč v posledních letech tak narostl počet útoků pomocí ransomware.

Útočníci předpokládají, že data jsou cenná a také, že zálohování nepokrývá úplně všechna data, která organizace potřebuje. Pokud by organizace měla vše dokonale zálohované, ransomware by ve skutečnosti pro ni byl relativně nevýznamný problém. Prostě by provedla obnovu ze svých záloh a mohla by pokračovat ve své dosavadní činnosti.

Úspěšnost ransomwarových kampaní (byť v poslední době zaznamenáváme drobná zlepšení situace v této oblasti) jasně ukazují, že v praxi je relativně jednoduché udělat chybu a data ztratit.

Z výše uvedeného nám vyplývají některé otázky, resp. problémové oblasti, na které se v této kapitole zaměříme.

1. zálohování (a obnova)
2. klonování disků
3. RAID a disková pole obecně

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. Přitom DVD je v této oblasti jednoznačně na ústupu.

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 [24])

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.

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.

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

Obrázek 4.1: Struktura DVD-R média (převzato z [6])

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 na DVD existovala speciální média jako je Data Trescor Disc [5], kde výrobce díky použití speciální kovové vrstvy uchovávající data předpokládá životnost 160 let, za ideálních podmínek. Za delší životnost média si uživatel samozřejmě připlatí. V současnosti, ale již tento typ médií a certifikovaných mechanik schopných na ně zapisovat nejsou v prodeji.

V oblasti optických disků ale je k dispozici pro tyto účely MDisc společnosti Verbatim. Výrobce u něj udává životnost až 1000 let ... ale očividně se jedná pouze o marketingový údaj, který bude platit pouze za určitých velmi specifických podmínek. Údaj 1000 let vychází z konstrukce vrstvy média, na kterou jsou zaznamenávána data. Použitý materiál se svými vlastnostmi blíží kameni a tak v čase téměř nedegraduje. A právě odtud vychází marketingově hezké číslo 1000.

Struktura média MDisc a běžného DVD je dostupná na obr. 4.2.

Technicky je MDisc médium BD-XL, poskytuje tedy úložnou kapacitu okolo 100 GB. V současnosti je ale rychlost zápisu omezena na 4x. Pro úplnost uvádíme také orientační ceny (k počátku roku 2023):

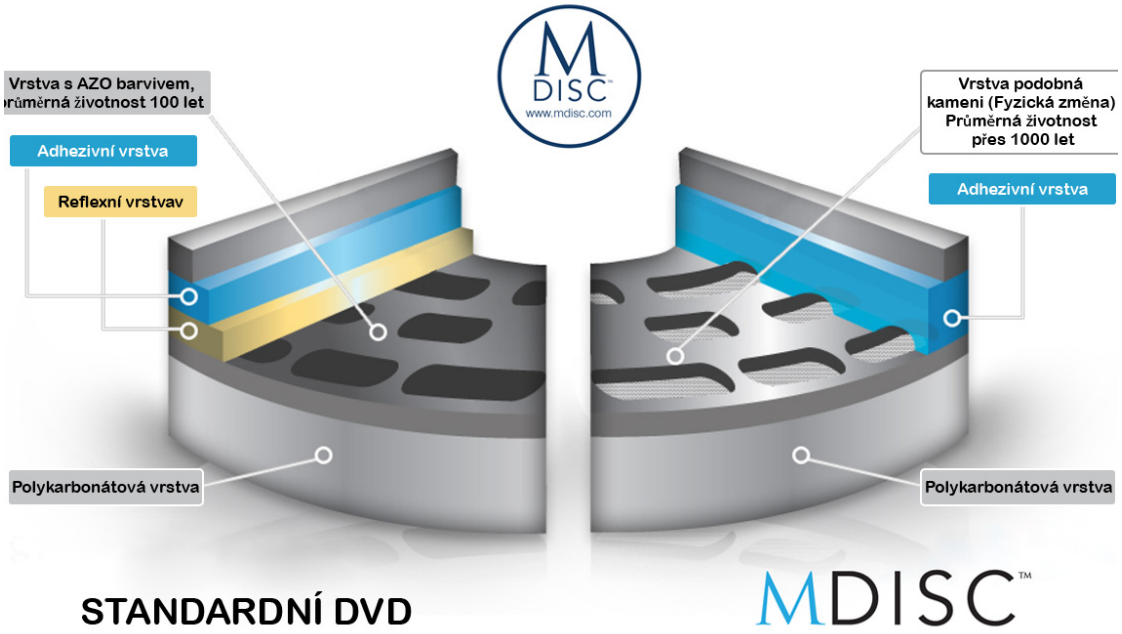
- 25 GB ... 100,- Kč/ks
- 50 GB ... 200,- Kč/ks
- 100 GB ... 431,- Kč/ks

Vypalovací mechanika s podporou MDisk formátu je dostupná v cenách okolo 2500,- Kč.

Výhodou záloh na optické disky je jejich malý rozměr a relativně dlouhá životnost, což umožňuje takto vytvořené zálohy dlouhodobě **archivovat**. Archivace je speciálním případem zálohování. Při archivování je naším primárním cílem dlouhodobá životnost takto vytvořené zálohy. Hlavním rozdílem mezi běžnou zálohou a archivací je způsob předpokládané práce s výsledkem.

K zálohování lze použít také pevné disky. Jejich výhodou je vysoká kapacita a také poměrně vysoké rychlost čtení a zápisu. Klasické pevné disky jsou založeny na magnetickém zápisu dat na diskové plotny. Tato technologie je s námi již řadu desítek let, ale v současnosti se pravděpodobně blížíme hranici (limitům jejich možností). Byť jsme stále svědky narůstajících kapacit disků. Přenosové rychlosti se již opravdu mnoho let nemění.

Toto omezení je založeno na technickém řešení hardisku a jeho připojení pomocí standardu SATA III. V tomto standardu je datová propustnost sběrnice okolo 600 MB/s. Této rychlosti ale pevné disky nejsou schopny dosáhnout.



Obrázek 4.2: Srovnání struktury DVD-R média a Verbatim MDisc (převzato z [65])

Zálohování vs archivace
V případě záloh předpokládáme, že s vysokou pravděpodobností dojde k nějakému problému, který se vyžádá obnovu dat z této zálohy. Zálohy proto pořizujeme opakovaně tak, aby reflektovaly aktuální stav dat v zálohovaném systému. Rychlost obnovy by pak měla být co možná nejvyšší tak, aby se omezily v maximální míře následky výpadku.

Oproti tomu v případě archivace předpokládáme, že data v praxi v budoucnu už možná nebudeme využívat. Například nahrazujeme provozovaný informační systém nějakým novým informačním systémem. Poté, co se ujistíme, že nový systém funguje tak, jak má, začneme původní systém odstavovat. Součástí tohoto odstavení bude také archivace všech dat, se kterými tento systém pracoval.

Nepředpokládáme, že tato data někdy budeme potřebovat, ale mohlo by se to stát. Hlavním cílem archivace je dlouhodobá životnost a snadnost skladování.

Z hlediska kapacit jsou dnes již běžně dostupné disky s kapacitami až 22 TB. Pokud budujeme velké záložní kapacity, např. prostřednictvím diskových polí, pak se orientujeme primárně na použití řad disků, které jsou k tomuto účelu určeny. Např. společnost Seagate má k tomuto účelu řadu disků IronWolf, Western Digital pak Red (popř. Red Pro). Fyzicky se tyto disky neliší od disků v řadách určených pro běžné nasazení, používají ale jiný firmware, který např. omezuje do určité míry vibrace, disky mají delší záruku a je k nim obvykle přibalována také bezplatná obnova dat v případě selhání disku (po dobu záruky).

Zálohování magnetickým zápisem mají jeden poměrně závažný nedostatek a tím je, že magnetické pole v čase slábne. Dochází tedy k samovolně demagnetizaci média a v tom důsledku také ke ztrátě dat. Tato demagnetizace je však velmi pomalá. Orientačně můžeme uvést např. hranici 20 let.

Výše uvedené je potřeba vnímat jako čas od posledního zápisu na disk. Např. disk vyjmeme z počítače a dáme do šuplíku.

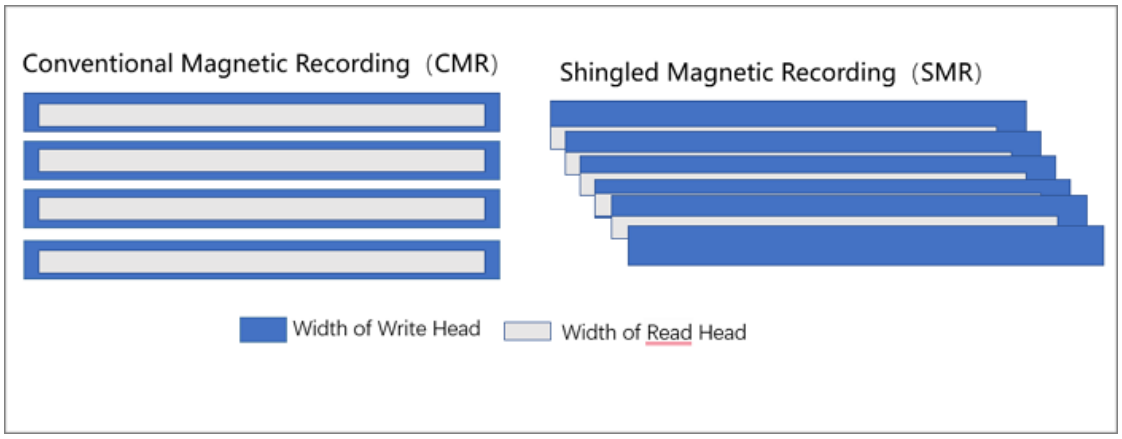
Na druhou stranu je potřeba dodat, že po uběhnutí tak dlouhé doby už může být vůbec problém nalézt počítač, ke kterému by bylo možné takový disk připojit.

Pevný disk můžeme připojit k počítači buďto přímo, lokálně - tedy přímo do chasi počítače nebo

CMR vs SMR
U názvu disků, popř. v podrobné specifikaci, je často uvedena také zkratka Conventional Magnetic Recording (CMR) nebo Shingled Magnetic Recording (SMR). Rozdíl mezi nimi je v zápisu a čtení.

CMR používá klasický zápis do jednotlivých stop na disku. SMR oproti tomu využívá toho, že hlava disku pro čtení je schopna číst data z užšího proužku, než na jaký je zapisováno. Disk pak pracuje dat, že při zápisu se část původní datové stopy překrývá. Mohli bychom si to představit třeba jako došky na střeše. SMR disky jsou pak logicky s vyšší kapacitou, ale za cenu nižšího výkonu při zápisu dat.

Vizuální představu o obou technologiích je možno si udělat z obr. 4.3.



Obrázek 4.3: CMR vs SMR (převzato z [32])

externě obvykle prostřednictvím USB kabelu. Zálohování v takovém případě je možno realizovat buďto pomocí specializovaných zálohovacích programů jako je např. *Acronis True Image*, nebo přímo pomocí funkcí operačního systému. Windows v posledních verzích obsahuje nástroj *Historie souborů* a v macOS je dostupný *Time Machine*.

V případě realizaci lokálních záloh může být ale výhodné místo magnetického zápisu použít spíše **Solid State Disc (SSD)** disky. V roce 2023 jsou na trhu dostupné SSD disky o kapacitách do 4 TB, ovšem s tím, že cena za TB je u SSD výrazně vyšší v případě kapacit HDD.

Z hlediska přenosových rychlostí jsou mezi SSD poměrně výrazné rozdíly v závislosti na technickém řešení disku a zejména pak způsobu jeho připojení do počítače. Paradoxně na první pohled tyto rozdíly nejsou patrné, jelikož všechny disky se připojují pomocí USB kabelu. Jenomže to, co vidíme jsou v zásadě pouze konektory, nikoliv kabel jako takový. Lišit se může také způsob, jakým bude se zařízením pracovat počítač.

Např. disky podporující USB 3.2 Gen 1 (původní označení USB 3.0) podporují přenosové rychlosti 440 MB/s - 1 GB/s, mnohem modernější USB 3.2 Gen 2x2 podporují rychlosti až 2 GB/s. Volba disku je pak vlastně řešení optimalizačního problému mezi potřebnou přenosovou rychlostí, kapacitou, cenou a předpokládanou životností.

Jelikož označování USB z hlediska vlastností může působit dosti zmatečně, připravili jsme pro Vás menší vysvětlující tabulku, viz tab. 4.2.

Ještě komplikovanější jsou pak konektory, které v rámci USB používáme, viz tab. 4.3.

K tabulce je navíc potřeba v některých aspektech doplnit komentář. Všimněte si např. označení standardu USB 2.0 revisited. Jedná se o revizi standardu USB 2.0, která ke standardnímu typ A konektoru přidává také micro-A, micro-B a micro-AB, které v původním standardu nebyly podporovány. Důvodem pro uvedení těchto konektorů byl nástup přenosných zařízení, která jsou relativně malá, natolik, že použití typ A konektoru v nich není možné.

Dále si povšimněte USB 3.2 standardu v tab. 4.2 a 4.3. USB 3.2 poskytuje za určitých okolností dvojnásobnou rychlost (20 GB/s) proti USB 3.1 a to přesto, že strukturálně svými kabely a konektory jsou oba standardy vlastně stejné. Rozdíl je způsoben odlišným využitím kabelu. Jde o to, že USB 3.2

Tabulka 4.2: Rychlosti, označování různých verzí USB (adaptováno z [37])

standard	**rok**	**označení**	**max. přenosová rychlost**
USB 1.0	1996	Low-speed	1,5 MB/s
USB 1.1	1998	Full-speed	12 MB/s
USB 2.0	2001	High-speed	480 MB/s
USB 3.0	2008	SS (Gen 1)	5 GB/s
USB 3.1	2013	SS+ (Gen 2)	10 GB/s
USB 3.2	2017	USB 3.2 Gen 2x2	20 GB/s
USB 4	2019	USB 4 Gen 3x2	40 GB/s
USB4 2.0	2022	USB4 Gen 4	80 GB/s

Gen 2x2 dosáhneme vyšších rychlostí při zasílání dat jedním směrem (např. na připojené zařízení). v USB 3.1 ale máme k dispozici 10 GB up a down.

Aby zmatkům nebyl konec používáme někdy také alternativní označení např. USB 3.2 Gen 1 pro USB 3.0 a USB 3.2 Gen 2 pro USB 3.1.

Dalším problematickým prvkem je, že typ-C konektor nepoužívá pouze USB standard, ale také Thunderbolt standard ve verzích 3 a 4. Thunderbolt je proprietální standard vyvinutý společností Intel za přispění společnosti Apple. Mezi USB a Thunderbolt existují poměrně značné rozdíly je ve vlastnostech. Maximální přenosová rychlost v Thunderbolt 3 je 40 GB/s, možnost napájení (power delivery) je pro oba standardy stejná 100 W, liší se ale podporované protokoly. Thunderbolt podporuje DisplayPort, USB, Thunderbolt a PCI express, zatímco USB 3.2 podporuje pouze DisplayPort a USB.

Zajímavá je zejména PCI Express funkcionalita, ta totiž umožňuje připojovat k počítači externí zařízení včetně třeba externích grafických karet, výkonných diskových polí apod.

Thunderbolt 4 vlastně není ani nijak významnou změnou oproti Thunderbolt 3. Je zvýšena maximální možná přenosová rychlost zařízení připojeným pomocí PCI Express (na 32 GB/s, tedy 2x v3) a standard je kompatibilní s USB 4.

USB 4 v2.0 je v době psaní tohoto textu (červenec 2023) horkou novinkou. Standardizace sice skončila v roce 2022, podpora v různých operačních systémech se ale začíná objevovat až nyní. Kromě vyšších přenosových rychlostí je ve 2.0 verzi také rozdíl v power delivery. Pro dosažení vyšších přenosových rychlostí je nutné použít aktivní kabel (s existujícími kabely to nebude možné). Z pohledu power delivery by měl být podporován až 140 W. USB 4 v2.0 také podporuje lepe připojování zařízení pomocí PCI Express.

Zatímco dosud platilo, že funkčně má Thunderbolt standard výhodu nad USB 4, verze 2.0 má potenciál toto změnit.

V případě zálohování velkých objemů dat z řady různých zdrojů neřešíme zálohování lokálně a na nějaké určené místo **na síti**. Výhodou je, že tímto způsobem lze do jisté míry zálohování centralizovat. Organizace se tam může zaměřit na budování diskových kapacit a lépe starat o konzistenci dat na nich uložených (obecně jejich bezpečnost).

Při volbě vhodné zálohovací strategie - určení čeho, jak a kam zálohovat se řídíme často jednoduchým principem 3-2-1. To znamená že vytváříme 3 kopie zálohovaných dat, z nichž 2 budou na lokální síti (ale ne na jednom zařízení) a minimálně jedna externí kopie.

Realizací takového přístupu získáváme velmi dobrou šanci, že bez ohledu na to, čemu bude daný systém vystaven, bude existovat minimálně jedna záloha, ze které bude moci být efektivně realizována jeho obnova.

Z tohoto pohledu:

- záloha na jiný disk zálohovaného počítače brání ztrátě dat způsobené selháním zálohovaného datového nosiče.
- záloha na jiný systém v síti nás chrání proti selhání zálohovaného počítače jako celku (např. selhání zdroje může vést ke vzniku přepětí, které zničí všechna zařízení v daném počítači)
- záloha do systému kompletně mimo síť organizace by měla zaručit, že v případě katastrofálního selhání na síti (vyřazení datového centra organizace např. v důsledku povodní) bude existovat nějaká další záloha, kterou bude možné použít.

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.

Zálohováním koncových zařízeních do NAS na síti nám na jednom místě vzniká poměrně velký objem dat, který ale je potřeba také chránit. Disková pole, která NAS obvykle využívá, jsou sice odolnější vůči náhodným selháním jednotlivých disků, ale to není úplná náhrada pro zálohování.

Také je potřeba rozlišit několik momentů - dosud jsme se bavili síti jako zálohovacím prostředku. K tomu je ale potřeba doplnit, že data uživatelů se mohou nacházet také přímo na síti, tedy že jejich lokální kopie nemusí vůbec existovat. Taková data je proto potřeba také zálohovat.

Jednou z mála možností, jak tak učinit, která na jedné straně poskytuje dostatečný prostor pro realizaci záloh, tak přijatelnou rychlost zálohování i případné obnovy jsou **pásky**. Zapisování i čtení je realizováno magneticky. 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. Tomu také odpovídají ceny a vlastnosti těchto zařízení.

Pro tento typ záloh, resp. pásky a mechaniky se vžila zkratka Linear Tape Open (LTO). V současnosti se používá 9. generace (LTO-9) tohoto standardu, která byla přijata v roce 2021. V minulosti generační inovační cyklus trval 3 - 4 roky, proto LTO-10 lze očekávat někdy okolo roku 2025, pokud se neobjeví nějaké nečekané problémy.

Vzhled takové pásky je dostupný na obr. 4.4, základní vlastnosti jednotlivých generací LTO jsou pak dostupné v tab. 4.4.

Obrázek 4.4: HPE LTO-9 Ultrium 45TB RW Data Cartridge (převzato z [34])

Pásku je možno přepsat přibližně 260x. Podporováno je až 5 000 založení pásky do mechaniky. Kapacitu s kompresí je potřeba brát orientačně. Ne všechna data jsou totiž dobře komprimovatelná. Např. video je prakticky nekomprimovatelné, oproti tomu text je velmi dobře komprimovatelný. Maximální kapacity s kompresí tak nutně nemusí být možné dosáhnout.

Výhodou páskových mechanik je možnost jejich škálování. Můžeme s páskami pracovat po jedné a celé ovládání realizovat ručně, existují ale také robotická řešení, která umí pracovat s celou knihovnou médií a podle potřeb je zakládat rotovat apod.

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 [13], Backblaze [2] nebo Carbonite [3].

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

[1] WORM = Write Once Read Many

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 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 - potřebujeme vytvořit tzv. *obrazu disku* pomocí nástroje pro klonování disků. Tyto fungují tak, že provedou kopii disku (přesněji řečeno diskového oddílu (disk partition) nebo oddílů). 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 plná funkčnost obnovovaného systému ihned po dokončení rozbalení obrazu na disku. Reinstalace počítače včetně software na něj nainstalovaného zabere přitom minimálně několik hodin a může se v některých případech protáhnout i na několik dní, pokud je vyžadována nějaká složitější konfigurace systému

Z hlediska technické realizace je výhodné, aby „datová“ a „programová“ část 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 [14] - má placenou i tzv. Community verzi, která je k dispozici zdarma pro osobní a nekomerční použití
- Acronis Cyber Protect Home Office [1] - původně známý pod názvem Acronis TrueImage
- CloneZilla [4] - open source nástroj pro klonování disků
- a řada dalších

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 je 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 málo minut.

Aby hromadné nasazení fungovalo s maximální efektivitou, musí organizace:

1. implementovat serverovou i klientskou část zvoleného 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 (každá z nich totiž bude vyžadovat samostatný obraz)

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.

Problematiky diskových polí jsme se již opakovaně dotkli. U síťových zařízení jsme např. hovořili o NAS. V zálohování jsme hovořili o možnosti realizace záloh na síť a velkých objemech dat, které je potřeba takto ukládat - mnohem větších, než jsou kapacity jednotlivých fyzických disků. Dokonce jsme identifikovali typy disků, které se k tomuto účelu hodí. Řešením je v takovém případě místo jednoho disku již použít více a propojit do právě do diskového pole.

RAID je jedním ze způsobů jak takového výsledku dosáhnout, není však jediný. Alternativní postupy jsou Redundant Array of Independent Nodes (RAIN), Storage Area Network (SAN) nebo použití softwarově definovaných diskových polí. RAIN a SAN jsou z pohledu IT znalostí poměrně komplexní problémy, které jsou velmi specifické. Softwarově definovanými diskovými poli se budeme ještě krátce zabývat v další podkapitole.

V rámci pole se propojené disky budou chovat vůči operačnímu systému, který je obsluhuje jako jeden disk. RAID pole jsou hardwarově realizované, to znamená, že obsluha pole je realizována pomocí řadiče disků. To umožňuje, aby práce disku byla velmi rychlá a také to, že operační systém se vůbec nemusí starat o to, jak diskové pole na daném systému vlastně funguje.

Velká kapacita pole je pouze jednou z výhod použití diskových polí, tou druhou je redundance. *Redundancí* rozumíme dostupnost dodatečných (paritních) informací, které se dopočítávají k datům ukládaným na jednotlivé disky. U diskového pole jsou zásadně využívány všechny disky. K zaplňování disků tak dochází rovnoměrně.

Není to tedy tak, že by se zaplnil jeden z disků v poli a teprve poté by se začalo pracovat s diskem dalším. Výsledkem takového přístupu by byl snížený výkon operací IO (input/output - čtení/zápis) a také nerovnoměrné opotřebení disků v poli (s vyšší pravděpodobností selhání disků, kde je nejvíce dat ... což je přesně to, co nechceme). Z tohoto důvodu zapisujeme data zároveň na všechny disky a doplňujeme k datům paritní informace.

Paritní informaci je následně možno použít k rekonstrukci dat v případě, že určitá část dat vypadne (např. selže disk), nebo je poškozena. Přítomnost paritní informace prakticky znamená, že obětujeme část diskových kapacit za účelem zvýšení odolnosti proti celkového řešení proti náhodnému selhání.

Pozor, RAID pole nejsou náhradou za zálohování a parita nechrání před všemi typy problémů, které mohou uložená data potkat.

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. Vzhledem k tomu, že tento typ pole nepracuje s žádnými paritami a proto z hlediska kapacity máme k dispozici úplnou kapacitu všech disků, tedy celková kapacita = součet kapacity všech disků.

Proč tomu tak je, lze odvodit z grafického pohledu na organizaci dat v poli, viz obr. 4.5.

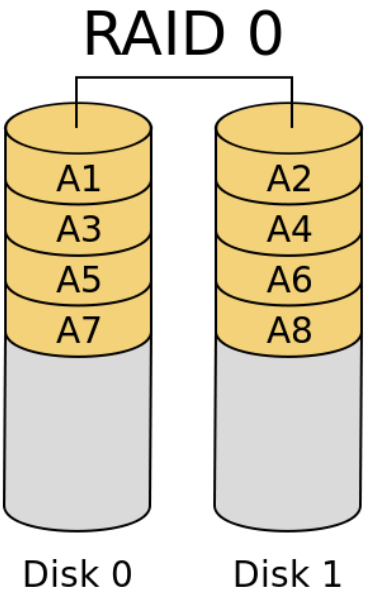
Jednotlivé soubory jsou rozdělovány do bloků a ty zapisovány postupně na jednotlivé disky „na přeskáčku“. Prakticky to znamená, že čtení i zápis mohou najednou pracovat se všemi disky zapojenými do pole. Tímto způsobem se minimalizuje význam některých úzkých hrdel v systému, zejména rychlosti jednotlivých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

Vzhledem k tomuto omezení se RAID-0 v samostatné podobě téměř nepoužívá.

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. 4.6. 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.



Obrázek 4.5: RAID-0 se dvěma disky tvořící jeden logický disk (převzato z [15])

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

K tomuto poli je ale potřeba dodat, že z hlediska využití diskového prostoru je vlastně stejně efektivní jako RAID-1 - tedy 50 % diskové kapacity je obětována. Z tohoto důvodu použití RAID-10 není také příliš časté, byť jak jsme uvedli před chvílí jisté využití v praxi má.

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 opět graficky, viz obr. 4.7.

Paritní informace je v tomto případě distribuována, tedy nenachází se na jednom disku. Paritní informace na obr. 4.7 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.

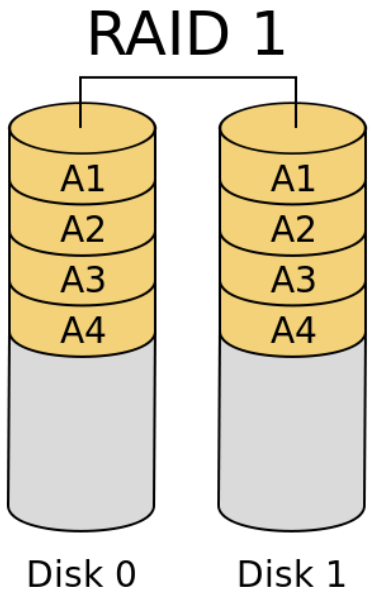
Z bloků dat se počítá paritní informace a zapisuje se na disky. Pozor paritní informace je ale distribuovaná na všechny disky. To znamená, že na všechny disky v tomto druhu pole ukládáme jak data tak paritní informace.

V případě selhání disku pak pole přestane fungovat ... tedy jistým způsobem. Pole bude fungovat v tzv. *degradovaném režimu*. V rámci něj můžeme data číst, a vlastně také zapisovat, ale se sníženým výkonem pole a rizikem, že v případě dalšího problému dojde k celkovému selhání pole. Správný postup je vadný disk vyměnit a pole by se, pokud budeme mít štěstí, mělo opravit. Tedy z dat na ostatních discích se dopočtu paritní informace, z dat a paritních informací na ostatních discích se dopočtou chybějící data.

Délka procesu zotavování je přímo úměrná množství dat uložených v poli a tedy také počtu použitých disků. Proces obnovy je také z jistého pohledu rizikový. Vzhledem k tomu, že rekonstrukce pole vyžaduje přečtení úplně všech dat z úplně všech disků, jedná se o proces, který je z pohledu operací IO velmi náročný. Je potřeba si přitom uvědomit, že disky v poli jsou pořizovány obvykle najednou. Pokud nám proto začne selhávat jeden (tedy pokud to není hodinách/dnech těsně po zprovoznění pole), pak lze předpokládat, že k tomuto selhání došlo v důsledku opotřebení a také že na ostatních discích bude toto opotřebení podobné.

Mezi disky samozřejmě budou drobné rozdíly v důsledku technologických tolerancí, které způsobě, že disky obvykle neselhávají v naprosto stejný čas. Na druhou stranu zvýšená zátěž během procesu obnovy je právě tím momentem, kdy je výrazně vyšší pravděpodobnost, že další disk selže, což z hlediska pole je fatální.

Mimochodem toto je společnou vlastností diskových polí všeho druhu, včetně RAID-6, které probereme za chvíli a softwarově definovaných polí v následující podkapitole.



Obrázek 4.6: RAID-1 se dvěma disky tvořící jeden logický disk (převzato z [16])

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), viz obr. 4.8.

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 v podstatě velmi podobným způsobem jako v případě RAID-5.

I v tomto případě, je parita distribuovaná, to znamená že paritní informace (obě) i data jsou rozprostřena po všech discích v poli. RAID-6 používáme tam, kde potřebujeme pracovat se skutečně velkými objemy dat, které vyžadují patřičně velké úložné kapacity. Zatímco v případě RAID-5 je minimální počet disků v poli 4, v případě RAID-6 je to už 5 disků.

Z hlediska kapacit disků je potřeba doplnit, že obvykle pracujeme se stejnými disky, tzn. disky od stejného výrobce se stejnou kapacitou. Obvykle v tomto případě, ale znamená něco trošku jiného, než by se mohlo na první pohled zdát. Jde o to, že disky pro pole nakupuje najednou. Logicky se proto ve chvíli nákupu díváme na existující nabídku na trhu a na jejím základě vybíráme patřičný model disku. Tím pádem se bude jednat o jeden typ disku od jednoho výrobce.

Technicky není problém, pokud by se jednalo o disky jiných výrobců, za předpokladu, že s nimi řadič disků bude schopen pracovat - bude kompatibilní.

Z hlediska kapacity je požadavek na velikost disku potřeba brát také s rezervou. Jde o to, že pole je limitováno nejmenším použitým diskem. Představme si scénář, kdy jsme si např. pro vlastní domácí účely poskládali malé diskové pole v NAS ze 4 disků s kapacitou 4 TB. Při použití RAID-5 tím získáme využitelnou kapacitu okolo 12 TB (12 TB data + 4 TB parita = 16 TB celkem).

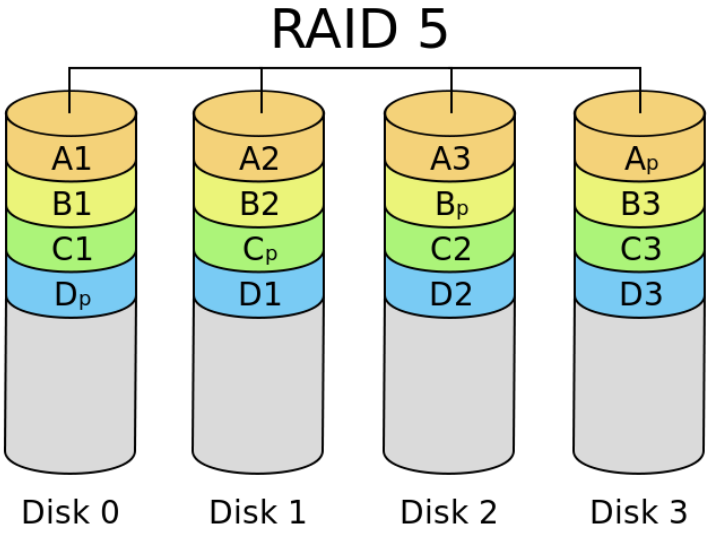
V případě selhání jednoho z disků musíme problémový disk nahradit diskem jiným s minimální kapacitou 4 TB. Pokud zvolíme disk menší, nebude to fungovat. Takový disk nelze použít. Zapojení disku s větší kapacitou ale fungovat bude. Použijme pro náš hypotetický scénář třeba disk s dvojnásobnou kapacitou, tedy 8 TB.

Po výměně bude ale disková kapacita pole stejná jako před ní, tedy 12 TB efektivní kapacity pro data. Použití bude jiné: 12 TB pro data + 4 TB parita + 4 TB nevyužitelný prostor.

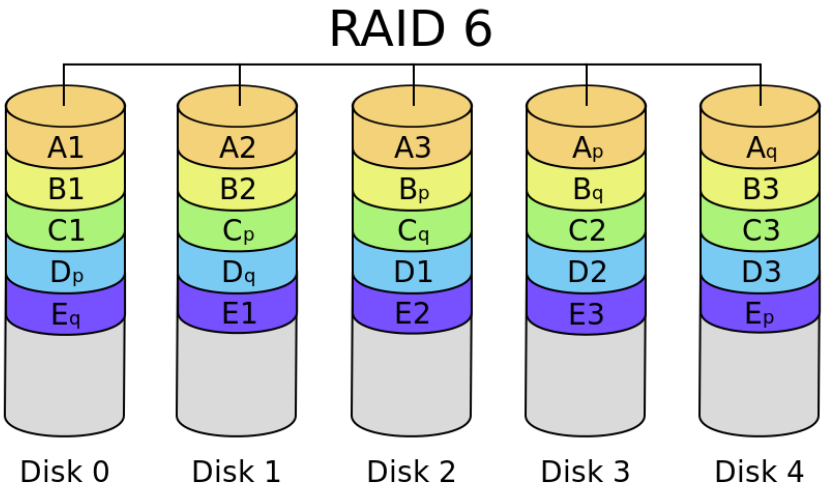
V případě polí RAID nelze ani uvažovat o scénáři, kdy tímto způsobem postupně vyměníme všechny disky, ve finále bychom tedy měli 4x 8 TB disků. RAID tedy nemá schopnost své kapacity takto flexibilně měnit.

Co by šlo udělat, je zazálohovat data z původního pole. Následně vytvořit pole nové, čímž bychom získali 24 TB pro data + 8 TB pro paritu a na toto pole obnovit data ze zálohy.

Prakticky je ale logičtější jiný postup - sestavit nové pole a data ze starého na něj prostě přenést.



Obrázek 4.7: RAID-5 se čtyřmi disky tvořící jeden logický disk (převzato z [17])



Obrázek 4.8: RAID-6 se pěti disky tvořící jeden logický disk (převzato z [18])

Po dokončení přenosu se staré pole odstaví, nebo případně poslouží pro nějaké méně důležité úkoly.

S.M.A.R.T.

Celkově vzato je lepší se hardwarovému selhání disku vyhnout. Technologie nám umožňují, aby v některých případech takové vyhnutí se problémům bylo možné. Většina moderních Hard Disc Drive (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.

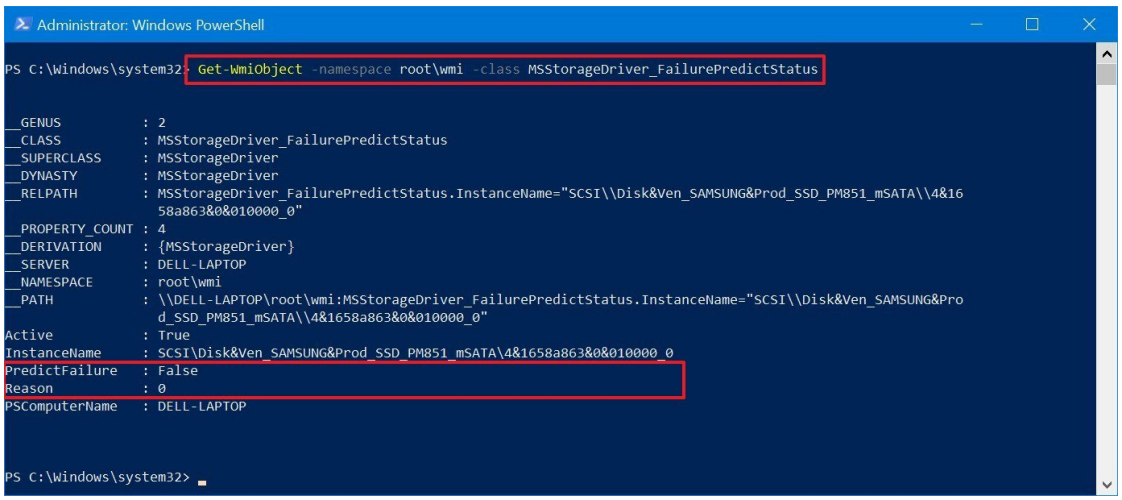
Je ale nutné upozornit, že S.M.A.R.T. není schopna identifikovat všechny typy problémů, které mohou vést k selhání disku. Statistiky ukazují, že přibližně pouze 2/3 disků, které selhaly, vykazovaly předem problémy detekovatelné pomocí S.M.A.R.T. 2/3 není málo, ale přesto zbývá třetina případů a to je poměrně dost.

Různé operační systémy pracují s informacemi ze S.M.A.R.T. rozdílně. Všechny operační systémy jsou schopny s touto informací pracovat, ale nemusí mít nutně úplně přímočarý způsob, jak tak učinit.

Např. ve Windows je možno se k těmto informacím dostat z příkazové řádky, PowerShellu nebo pomocí nástroje pro Monitoring výkonu. Všechny tři způsoby jsou hezky popsány např. v následujícím tutoriálu [50].

V podnikovém prostředí lze předpokládat shromažďování informací o discích nejspíše pomocí

PowerShell. Příklad použití pro tento účel je dostupný na obr. 4.9.



Obrázek 4.9: Zjištění S.M.A.R.T. informací pomocí PowerShell ve Windows 10 (převzato z [50])

PredictFailure parametr nám říká zda si S.M.A.R.T. myslí, že daný disk selže nebo ne. V našem případě je disk v pořádku.

V domácím prostředí je výše uvedený způsob možné využít také, ale pro osoby méně znalé se nemusí jednat o úplně příjemný způsob práce. V takovém případě se vyplatí pořídit nějakou aplikaci, která tyto informace zpřístupní. Uvedenou funkcionalitou disponují některé nástroje pro zálohování nebo třeba nástroje pro defragmentaci disku (např. Defraggler a řada dalších) nebo samostatných utilit jako je CrystalDiskInfo.

Jenom upozornění - defragmentaci disku neprovádíme na SSD discích. Defragmentace zde nepřináší navýšení výkonu a také v jejím průběhu se zbytečně opotřebovává disk. Takže nedefragmentovat.

Také problematika fragmentace dat na disku a S.M.A.R.T. spolu nesouvisí. Zobrazení S.M.A.R.T. informací je pro aplikaci spíše bonusová funkce.

Pro jednotlivé uživatele Windows počítačů bez nároků na pravidelné shromažďování, agregaci těchto údajů ke pravděpodobně CrystalDiskInfo [28] nejjednodušším způsobem. Aplikace je dostupná zdarma, je open source a poskytuje poměrně podrobné informace o stavu disku a to jak HDD, tak SSD.

Omezení RAID

Jak je patrno z předešlých stránek, jsou RAIDy poměrně zajímavou technologií, která poskytuje velmi silné nástroje pro řešení problémů s kapacitou a také zodolňuje infrastrukturu určenou pro ukládání dat proti určitým typům selhání. S použitím RAID se ale pojí také řada problémů, o kterých bychom měli minimálně vědět, než se do realizace těchto polí pustíme.

Vzhledem k tomu, že RAID je vždy hardwarově závislý, je hardware (tedy řadič disků) častým bodem selhání diskového pole. V tomto scénáři nám neselže disk nebo disky, ale řadič disků samotný. Diskové pole samozřejmě okamžitě přestane být dostupné. Zotavení ale v takovém případě nemusí být snadné, nebo dokonce možné.

Jde o tom, že mezi výrobci řadičů jsou drobné odlišnosti v implementaci podpory různých typů diskových polí. Pokud tedy nahradíme starý řadič novým od jiného výrobce nebude pole téměř jistě detekováno. Podobně nemusí být pole detekováno ani v případě, že nahradíme řadič stejným řadičem, ale disky zapojíme v jiném pořadí. Řadiče totiž nemají schopnost analyzovat disky a „rekonstruovat“ (konfiguračně) způsob jakým bylo pole sestaveno.

Dalším omezením je, že ani v případě, že disky i jejich řadič zůstanou v pořádku, nejsou data na nich uložená zcela v bezpečí. Za určitých okolností totiž data mohou být poškozena a to dokonce aniž by se s nimi manipulovalo (tzn. došlo např. k jejich přepsání). Tomuto fenoménu říkáme *bit rot*. Podrobnosti o tom proč tomu tak je jsou ale poměrně technicky náročné, takže mi buďto můžete věřit nebo se dále vzdělávat např. v [52] je v průběhu 20 minut poměrně jednoduše tato problematika shrnuta.

Pokud tedy je s použitím RAIDů spojeno tolik problémů, měli bychom je vůbec používat? Pokud ne, jaké jiné technologie máme k dispozici, abychom tuto problematiku, ideálně lépe vyřešili?

V dnešní době jsou klasické RAIDy spíše už reliktem „starých dobrých IT časů“. Postupně dochází k jejich nahrazování pomocí softwarově definovaných diskových polí, kterými s v krátkosti budeme zabývat v následující podkapitole.

4.4 Softwarově definovaná disková pole, nebo spíše ZFS

Z předchozí podkapitoly víme, že klasické RAIDy jsou do jisté míry závislé na hardwaru a tím pádem jsou s jejich provozem a spolehlivostí spojeny některé problémy.

Jedním z možných řešení, které získává stále větší popularitu, je použití *softwarově definovaných diskových polí*. Ta jsou specifická tím, že diskové pole v tomto případě je ovládáno přímo operačním systémem. Nejsou tedy závislá na hardware. K jejich použití jsou ale vyžadovány pokročilé souborové systémy.

Jedním z prvních souborových systémů, který umožňuje výše uvedený mód práce je ZFS. ZFS původně vyvinula společnost Sun Microsystem někdy okolo roku 2000 pro využití ve svém proprietálním operačním systému Solaris. V té době ale začala mít společnost finanční problémy. Jedním z pokusů, jak se s nimi vypořádat bylo uvolnění částí operačního systému včetně ZFS jako open source, za určitých poměrně specifických licenčních podmínek.

Sun byl následně odkoupen společností Oracle, která ukončila většinu Sunem rozjetých open source aktivit, ZFS ale získalo poměrně rychle nezávislou vývojářskou komunitu a vývoj pokračoval v OpenZFS, které je dnes masivně nasazováno pro řešení úložných kapacit. Po 20 letech vývoje lze říci, že OpenZFS obsahuje řadu pokročilých vlastností, které v původním ZFS nejsou dostupné. Dále v textu proto budu hovořit pouze o OpenZFS, pro zkrácení jej ale budu nazývat ZFS.

Výběr některých zajímavých vlastností:

- není závislé na hardware
- copy-on-write
- podpora komprese lz4
- schopnost rozdělit pole na oblasti podle druhu použití a nastavit odlišně způsob práce (v rámci jednoho diskového pole)
- podpora snapshotů
- podpora ARC pro indexaci souborů na discích a tak celkové zvýšený výkonu pole
- jednoduchá rozšiřitelnost kapacity bez nutnosti rekonstruovat pole
- stálá kontrola konzistence uložených dat na discích (scrub)
- a řada dalších

Zkusme jednotlivé vlastnosti postupně probrat. Nezávislost na hardware prakticky znamená, že o obsluhu pole se stará operační systém, který „umí“ ZFS. Prakticky to funguje tak, že pokud máme disky z nějakého existujícího pole, můžeme zadat příkaz k importu těchto disků. Operační systém si je prohlédne a na základě informací na těchto discích spolehlivě odvodí, jak má pole fungovat. Připomínáme, že realizovat výše uvedené byla jedna z gigantických slabin RAID.

Pokud pracujeme s daty, např. upravíme nějaký soubor, většina souborových systémů postupuje tak, že najde na disku umístění tohoto souboru a v tomto umístění jej přepíše. Pokud ale při zápisu nastane nějaký problém, pak může dojít k poškození tohoto souboru - původní už nebude existovat a nový není v pořádku. Copy-on-write pracuje odlišně. Při uložení souboru se soubor uloží do prázdného místa na disku a teprve poté se změní metadata, která budou odkazovat na novou verzi tohoto souboru. Pokud tedy při zápisu dojde k nějakému problému, např. výpadku elektrické energie. Budeme mít k dispozici alespoň původní, neupravenou verzi souboru.

ZFS také agresivně pátrá po chybách. V rámci RAIDů jsme se bavili o paritě a podobný způsob používá také ZFS (používá trochu jiné algoritmy pro výpočet parity) ovšem s tím, že RAID nepřepočítává parity. Tzn., že parity se spočtou a zaznamenají při zápisu dat, ale následně se použijí až dojde k procesu obnovy např. po selhání disku. Z tohoto důvodu je u tohoto typů polí tak důležitý problém tzv. bit rotu a z něj vyplývajícího poškození dat.

ZFS oproti tomu používá tzv. *scrub*. V rámci něj postupně prochází disk a kontroluje parity. V případě, že narazí na problém tak na nic nečeká a problém okamžitě opraví. V okamžiku, kdy je poškozený pouze blok dat nebo parita, je ještě tato obnova bez problémů možná a také není výpočetně náročná, jelikož se týká velmi malého množství dat.

Podpora snapshotů je další pokročilou funkcionalitou, kterou řada souborových systémů nepodporuje. Snapshotem rozumíme snímek stavu souborového systému. Ten nám může posloužit k tomu,

abychom se měli k čemu vrátit, pokud provádíme s polem operace, u kterých si nejsme jisti výsledkem. Snapshoty lze také přenášet mezi různými systémy. Toto lze použít např. pro replikaci diskového pole)

Problematika snapshotů je v tomto textu silně zjednodušena, je ale možno si z ní udělat základní představu o službě.

ARC je speciální index, který pole používá k tomu, aby efektivněji našlo data na discích. V rámci ZFS mohou fungovat dvě úrovně ARC, jedna je přímo v paměti (pro maximální rychlost), druhá tzv. L2ARC je na samostatném disku, obvykle NVMe SSD. Důvodem je zejména kapacita. Prostor v paměti nemusí zejména u velkých diskových polí postačovat pro celý index. SSD disky sice nejsou tak rychlé jako paměť, jsou ale rychlejší než klasické disky.

Pro zbývající funkcionalitu budeme muset lépe pochopit, jak je vlastně vnitřně pole organizováno.

Při vytváření diskového pole začínáme vytvořením tzv. *pool*. Do něj vložíme všechny disky, které mají být v poli obsaženy. V rámci poolu pak definujeme tzv. *datasety*. Datasety vytváříme podle potřeb/účelu. Výhodou je, že pro dataset specifikujeme nastavení, např. použití komprese. Můžeme mít třeba samostatný dataset určený pro multimédia (hudba filmy), u kterého nebudeme chtít zapínat kompresi. Jiný dataset může sloužit jako úložný prostor pro běžnou práci, která naopak komprimovatelná může být.

Pro pool samotný nastavujeme také režim diskového pole. ZFS může pracovat s jedním diskem bez jakékoliv redundance, což může být zajímavá možnost např. pro nasazení na běžném počítači, tedy pokud to operační systém na něm podporuje (což např. Windows neumožňují). Tam, kde je to podporováno, ale uživatelé získají lepší odolnost proti různým selháním, podporu snapshotů, komprese částí disku apod., tedy funkcionality, která není závislá na existenci parity.

Disková pole obvykle obsahují 3 - 9 disků. Máme přitom řadu možností jaký typ pole chceme sestavit. Souhrně se to označuje jako **RAID-Z**. Filozoficky můžeme hledat určitou podobnost s běžným RAID, porovnání je dostupné v tab. 4.5.

Omezení na 9 disků prosím berte jako orientační. Jde o to, že jsme probrali pouze pool a dataset v rámci naší krátké exkurze do tajů ZFS, a ne tzv. vdev. Prakticky v našem případě bychom měli 1 pool, v rámci něj bychom měli jeden vdev, ve kterém by byly všechny disky. „Soft“ omezení na 9 disků se týká vdev, nikoliv poolu.

Další kapacitu tak můžeme doplňovat přidáním dalších vdev (a v nich dalších X disků) do poolu.

Toto omezení je motivováno zvýšením pravděpodobnosti úspěchu zotavení pole po selhání některého z disků. Jelikož rekonstrukce pole je funkčně podobná rekonstrukci pole v rámci RAID, vztahují se na ni vlastně stejná omezení. Pro rekonstrukci musí být přečtena všechna data a parity na všech discích. Jak víme z předchozího textu, je to ten okamžik kdy se nám zvyšuje pravděpodobnost selhání dalšího disku. ZFS operaci obnovy označuje *resilvering*.

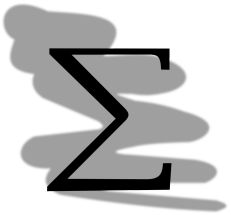
Zjednodušeně můžeme říci, že čím více disků ve vdev máme, tím je větší šance, že některý z nich při obnově selže. 9 disků je takový rozumný kompromis mezi kapacitou, režií na parity a schopností v případě problému obnovit svou činnost.

Rekonstrukce vs náhrada

Některé operační systémy určené přímo pro správu takových polí, jako je např. TrueNas umožňují pro disky „na odchodu“, které ale ještě neselhaly jejich výměnu odlišným způsobem.

Postupujeme tak, že nový disk přidáme do chasi a pak ve správě poolu nastavíme, že tento nový disk má nahradit ten odcházející. OS začne okamžitě z tohoto disku kopírovat data 1:1 na nový, aniž by jakkoliv manipuloval s ostatními disky. Ve výsledku dostaneme buď přesnou kopii disku který je automaticky zapojen do patřičného vdev, nebo v případě selhání disku v průběhu kopírování dostaneme částečnou kopii, kterou se můžeme pokusit zrekonstruovat.

V obou případech máme každopádně méně dat na přečtení a rekonstrukci a z toho nám vyplývá také lepší šance na úspěch.



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.

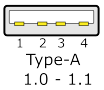
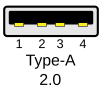
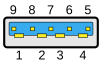
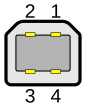
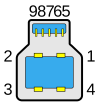
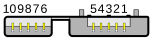
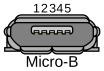
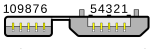
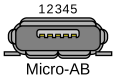
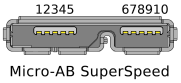
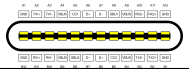
Kontrolní otázky

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, umožnůjící zotavení pole v případě výpadku některého z disků.

Tabulka 4.3: USB verze a konektory (adaptováno z [37])

konektor	vzhled	USB standard
Type-A 1.0 - 1.1		1.0, 1.1
Type-A 2.0		2.0
Type-A SuperSpeed		3.0, 3.1, 3.2
Type-B		1.0, 1.1, 2.0
Rype-B SuperSpeed		3.0, 3.1
Mini-A		1.1, 2.0
Mini-B		1.1, 2.0
Mini-AB		2.0 (revisited)
Micro-A		2.0 (revisited)
Micro-A SuperSpeed		3.0, 3.1, 3.2
Micro-B		2.0 (revisited)
Micro-B SuperSpeed		3.0, 3.1, 3.2
Micro-AB		2.0 (revisited)
Micro-AB SuperSpeed		3.0, 3.1, 3.2
Type-C		2.0, 3.0, 3.1, 3.2, 4, 4 V2.0

Tabulka 4.4: Vlastnosti různých generací standardu LTO

vlastnosti	**LTO-1**	**LTO-2**	**LTO-3**	**LTO-4**	**LTO-5**	**LTO-6**	**LTO-7**	**LTO-8**	**LTO-9**
rok	2000	2003	2005	2007	2010	2012	2015	2017	2021
kapacita [TB]	0,1	0,2	0,4	0,8	1,5	2,5	6	12	18
kap. s kompresí [TB]	0,2	0,4	0,8	1,6	3	6,25	15	30	45
rychlost [MB/s]	20	40	80	120	140	160	300	360	400
čas přepsání [h:m]	1:23	1:23	1:51	3:10	4:20	5:33	9:16	12:30	
WORM[1]	N					A			
šifrování	N			A					
cena [Kč/ks]				700	800	850	1300	1800	4300

Tabulka 4.5: RAID-Z vs RAID

RAID-Z	**RAID**	**min. disků**
RAID-Z	RAID-5	3
RAID-Z2	RAID-6	4
RAID-Z3	-	5

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 11 má 60 - 100 mil. řádků kódu, jádro operačního systému Linux pak okolo 30 mil. řádek kódu (leden 2022).

Přestože existují metody umožňující minimalizovat počet takových chyb 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/vzdělávání sebe sama nebo zábavu. Informace a možnosti, 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.

Úvahy tohoto typu nás přivedou v závěrečné kapitole k systémům řízení informační bezpečnosti jako procesního rámce, kterým se organizace může programově bránit různým typům útoků a problémů bez ohledu na to odkud pocházejí.

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 [51]. 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 jsou z pohledu zajištění počítačové sítě dané organizace a aktiv na ni připojených. Organizace sice mohou provést sebehodnocení dosažené úrovně bezpečnosti, avšak obrázek, který tímto způsobem získají bývá zkreslený. Mezi důvody řadíme především:

- provozní slepotu
- omezené zdroje na realizaci penetračního testu vlastními silami
- nedostatečné znalosti pro realizaci testu
- nedostupné specializované nástroje a zejména pak absence tréningu a zkušeností z jejich provozu
- a řada dalších.

Výsledkem výše uvedeného je, že pouze vnitřními zdroji není možné si udělat úplný, objektivní obraz o stavu bezpečnosti. Proto organizace obvykle kombinují interně a externě realizované testy. Externí se využívají především pro „kalibraci“ interních testů a také v případech kdy dochází ke skokové změně v systémech nebo způsobu jejich zabezpečení.

Externí audity/testy mohou být také vyžadovány na některé typy certifikací, např. pro zavedení systému ISMS dle ISO 27001, nebo mohou být užitečné pro prokázání souladu mezi požadavky legislativy a způsobem jakým tyto požadavky realizuje daná organizace.

Penetrační testování (i ostatní typy auditů a testů) 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 [23]. 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 (jak praví staré Klingonské přísloví). Pomsta, jako motivační faktor, je obzvláště nebezpečná, protože je vetšinou dlouhodobě naplánována s cílem ve finále způsobit maximální škody.

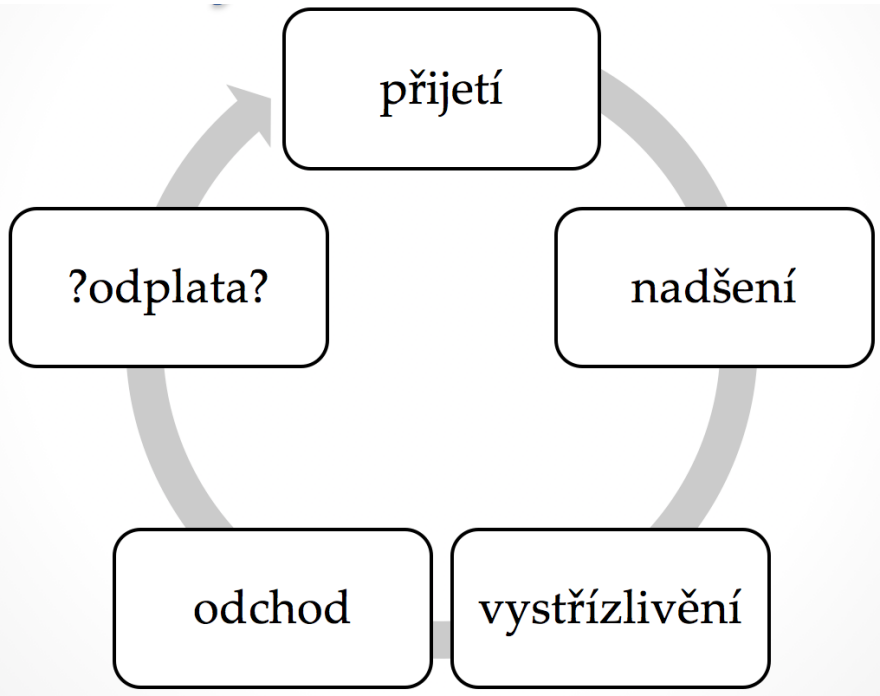
Je potřeba si uvědomit, že běžný člověk stráví v práci 8 nebo více hodin denně - to je podstatná část doby, po které je člověk vzhůru. V práci máme přátele, někteří lidé si v práci nalezli svého životního partnera, jiní ho (ji) kvůli práci ztratili. Proto každá křivda, ať už domnělá nebo skutečná, může 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 často záhy vezme za své a je nahrazeno šedivou realitou každodenní rutinní 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 a řízení pracovních procesů
3. odchod - korektní jednání, pečlivý monitoring činností odcházejícího



Obrázek 5.1: Působení zaměstnance ve firmě

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 předem 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.

Bezpečnosti v organizaci také přispívá, pokud daná organizace má vhodně „zprocesované své činnosti“. Tzn., že má jasnou, dokumentovanou představu, jakým způsobem se mají jednotlivé úkony/činnosti v organizaci vykonávat a je schopna je komunikovat směrem k zaměstnancům, kteří je vykonávají. Požadavky na existenci procesů, jejich formální dokumentaci a proškolování existují v řadě norem. Jako příklad můžeme uvést systémy řízení jakosti ISO 9000, systémy řízení informační bezpečnosti ISO 27000 a další,

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

Existují dvě z pohledu bezpečnosti extrémně rizikové skupiny zaměstnanců a těmi jsou 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.

Výše identifikované dvě obzvláště citlivé skupiny zaměstnanců je potřeba brát s rezervou. Pokud např. organizace nerozlišuje role a poskytuje všem zaměstnancům zvýšena nebo dokonce administrátorská práva do systémů bude taková organizace muset brát jako obzvláště citlivé všechny zaměstnance.

Také je potřeba brát v úvahu, že každá organizace je jiná. K tomu je potřeba vždy přihlédnout. Organizace také může mít některé klíčové osoby se specifickým know how, nebo extenzivním přístupem k systémům (z různých důvodů). Takové osoby je potřeba také identifikovat a chovat se k nim obdobně.

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.

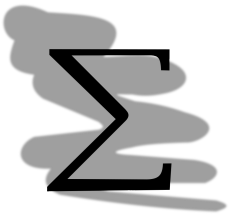
V minulosti byly provedeny některé studie popisující charakteristiky hrozeb plynoucích od insiderů, viz např. zpráva [41] zabývající se hrozbou insiderů pro finanční sektor USA. Studie ukázaly, že pomsta není realizována z náhlého popudu, rozhodnuté zraje v zaměstnance dlouhou dobu. Podobně i doba přípravy 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)
- mít zvládnuté pracovní procesy
- 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 jako 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, zpracování požadavků na straně serveru a také možnostmi ochrany proti nim. V těchto skriptech se nebudeme zabývat technickými podrobnostmi jejich provedení 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 webová sídla, která bývají častým cílem útoků DDoS jelikož ze své podstaty musí být veřejně dostupný může být řešením také cachování webových stránek. Jedná se o službu kterou poskytují společnosti jako Cloudflare a řada dalších. Funguje to tak, že veškeré požadavky na webové stránky jsou směřovány přes poskytovatele této služby. To má několik výhod:

- umožňuje požadavky na web nejprve zkontrolovat a požadavek
  - v případě identifikace jako součást útoku odmítnout
  - zpomalit
  - poslat dál
- v případě nedostupnosti webu poskytnout kopii stránek v cache služby

Kontrola na to, zda požadavek je součástí útoku nebo ne je vykonávána na základě analýzy některých vlastností požadavků, především [40]:

- některé vlastnosti paketů jako je IP adresa zdroje požadavku, port zdroje, cílová IP adresa, cílový port, použitý protokol, vlajky protokolu TCP, pořadové číslo požadavku, jejich nastavení a rychlost příchodu packetů
- metadata požadavků HTTP jako jsou hlavičky HTTP, user agent řetězec, text požadavku, cesta, hostitel, HTTP metoda, HTTP verze, verze TLS a rychlost příchodu takových požadavků
- metriky odpovědí HTTP jako jsou vracená chybová hlášení apod.

Cloudflare pro účely ochrany proti výše uvedené indikátory analyzuje v reálném čase, což mu umožňuje identifikovat DDoS útok již v počátcích a minimalizovat jeho dopady ještě předtím, než síťová komunikace dojde k cílovému systému.

Druhou metodou, kterou Cloudflare pro ochranu používá je zpomalení. Výše uvedené metriky totiž nutně nevedou k jednoznačnému rozlišení toho, zda se jedná o oprávněný požadavek nebo o součást útoku. V takovém případě služba vrátí stránku upozorňující, že zadaný požadavek je analyzován a po uplynutí pár sekund je požadavek poslán na cílovou adresu a dojde tedy k navrácení skutečné stránky. I toto drobné zpomalení má obrovský význam z pohledu efektivity útoku.

Typický útok totiž takových požadavků generuje ohromně množství, což je naopak pro běžné požadavky atypické. Řekli jsme si, že útok DDoS je distribuovaný, nikdy ale není natolik distribuovaný, aby z každého zdroje útoku šlo pouze několik málo požadavků. Pokud v průběhu krátké doby, po kterou se čeká na vyhodnocení přicházejí z daného zdroje další a další stejné požadavky posiluje se důvěra služby v to, že se jedná skutečně o součást útoku a tak je tuto komunikaci možno bězpečně „zaříznout“.

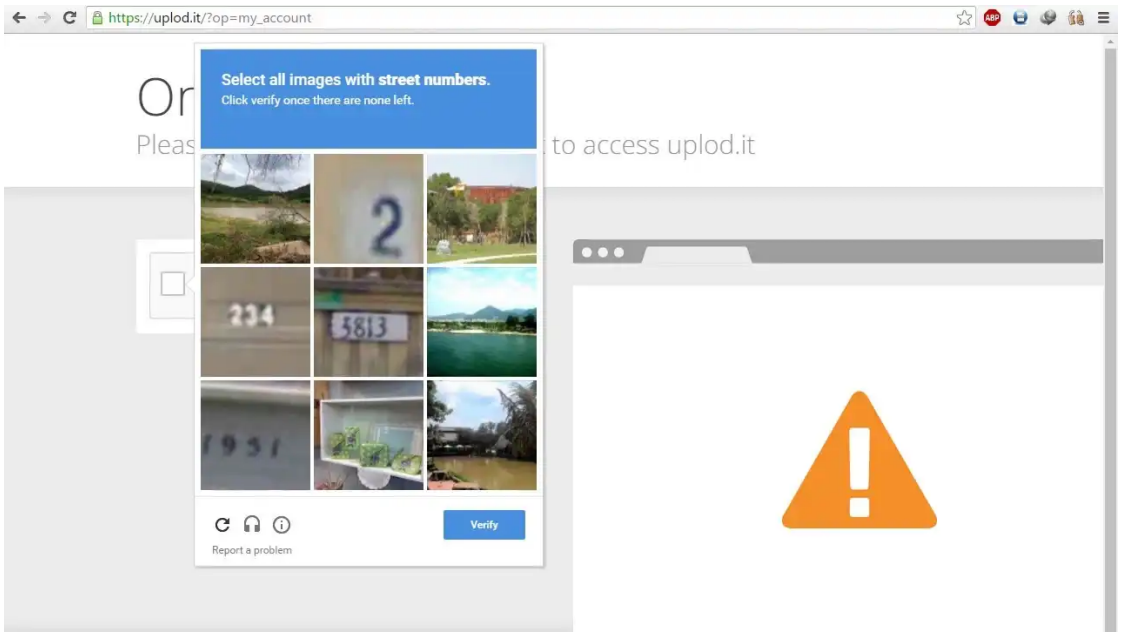
Pro oprávněné požadavky je zpomalení nepříjemné, ale není fatální.

Zpomalení má v tomto případě ještě jednu variantu, kdy místo zcela automatického propuštění komunikace, nebo jejímu zamezení je zobrazena výzva s CAPTCHA. Jejím vyplněním uživatel prokazuje, že je člověk a tudíž není součástí útoku, viz obr. 6.1.

CAPTCHA ale rozhodně není „všespásná“. Předně je možno ji použít pouze na stránkách, kde předpokládáme použití čistě člověkem. Dobrým příkladem jsou právě webové stránky organizací. Naopak je nelze použít pro webové aplikace, kdy se serverem komunikuje právě aplikaci, nikoliv přímo uživatel. Může se jednat např. o tenké klienty informačních systémů, nebo aplikace pro mobilní telefony, které konzumují nějaké externí data z různých zdrojů a něco s nimi dělají.

Tyto se totiž s CAPTCHA neumí přirozeně vypořádat.

Problém může být také v nastavení služby jako takové. Jak moc má být citlivá? Kolik požadavků může být zasláno než se začnou aplikovat nějaká restriktivní opatření. I CAPTCHA samotnou lze



Obrázek 6.1: Použití CAPTCHA na Cloudflare (převzato z [27])

nastavit různým způsobem. Bude požadováno řešení pouze jednoho úkolu (jak je třeba znázorněn na obr. 6.1) nebo celé série. Ačkoliv řešení CAPTCHA je obvykle jednoduché pro uživatele, pokud práce se systémem vyžaduje řadu interakcí s ním a při každé bude CAPTCHA požadována bude to mít poměrně drastické dopady na uživatelský zážitek.

Při špatném nastavení služby tak může dojít až k znehodnocení poskytované služby.

Výše uvedené nastavení pak není nutně otázkou pro IT, ale spíše pro management, popř. osoby zodpovědné za chráněný systém, aby vhodně popsaly způsob jakým je daný systém využíván a z toho se následně odvodily parametry pro nastavení ochrany.

Takové podrobné nastavení je ale dostupné pouze pro platící zákazníky služby Cloudflare.

Cloudflare přitom vnímejte prosím jako určitý modelový příklad řešení tohoto problému. Existuje celá řada firem, které poskytují obdobné služby.

Content Delivery Network (CDN)

Existují dva výklady zkratky CDN a to Content Delivery Network a Content Distribution Network. Jedná se o sítě, jejichž základním účelem je poskytnout svým zákazníkům efektivní nástroje pro distribuci obsahu. Myšlenka je taková, že obsah by měl být co možná nejblíže u zákazníka a to právě zajišťuje CDN.

Cloudflare je právě poskytovatelem CDN.

Pro určité typy útoků může jít řešení úplně nad rámec běžných možností firmy. Pokud takovou funkcionalitu potřebují, pak si ji obvykle nakoupí jako službu od poskytovatele CDN, viz box.

Existují ale některé organizace, které mají čistě regionální působnost z hlediska služeb, které poskytují. Uvažujme třeba chytré měřidla pro odečet spotřeby např. vody. Měřidlo v takovém případě zasílá údaj do své síťové infrastruktury (může být server nebo cloud) a odtud jsou zasílaná data zpracovávána pro dosažení cílů dané organizace, např. pro účely vyúčtování. Jelikož je taková služba silně regionální lze lépe řídit síťový provoz, který se k ní snaží dostat. Není např. důvod pro to, aby k této infrastruktuře přistupovaly systémy/počítače z jiných států.

Takových organizací ale není tak mnoho. Možnosti takových omezení se budou týkat především subjektů kritické infrastruktury a to konkrétně v řídících systémech této infrastruktury.

Může se to týkat také významných informačních systémů, dle platné legislativy. Tyto systémy mají přesně specifikovaný model použití, tedy kdo, kdy a jak k nim má přístup a vše ostatní by mělo být explicitně zakázáno.

Ochrana KI
V těchto skriptech není prostor jít příliš do podrobností o této problematice. V případě zájmu konzultujte proto skripta z předmětu *Bezpečnostní informatika* [72] 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 údaje 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 není směřován na koncové vlastnictví postiženého postiženého ale na provozovatele DNS.

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 jedné osoby a to oprávněného vlastníka. Certifikát použitý pro podepsání žádosti musí být platný a musí jej vydat důvěryhodný poskytovatel certifikačních služeb (PCS).

Důvěryhodný je v tomto případě rozuměno z pohledu provozovatele DNS. Důvěryhodnost v tomto případě není řešena legislativou. eIDAS směrnice sice pracuje s webovými certifikáty, pod které by pravděpodobně tato problematika mohla spadat, ale požadavky zde uvedené nejsou povinné a v praxi se jimi nikdo neřídí.

Každopádně elektronický podpis, pokud je správně použit, je velmi silným zdrojem důvěry ve validitu zaslaného požadavku.

Použití DNSSec společně se správnou verzí šifrování komunikace jsou základní metody, jak daný uzel na síti zabezpečit, navíc způsobem, který je viditelný alespoň částečně pro koncového uživatele, tedy odběratele služby. V okamžiku, kdy se ke službě připojí pomocí moderního WWW prohlížeče, dostane vizuální upozorně, 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. 6.2.

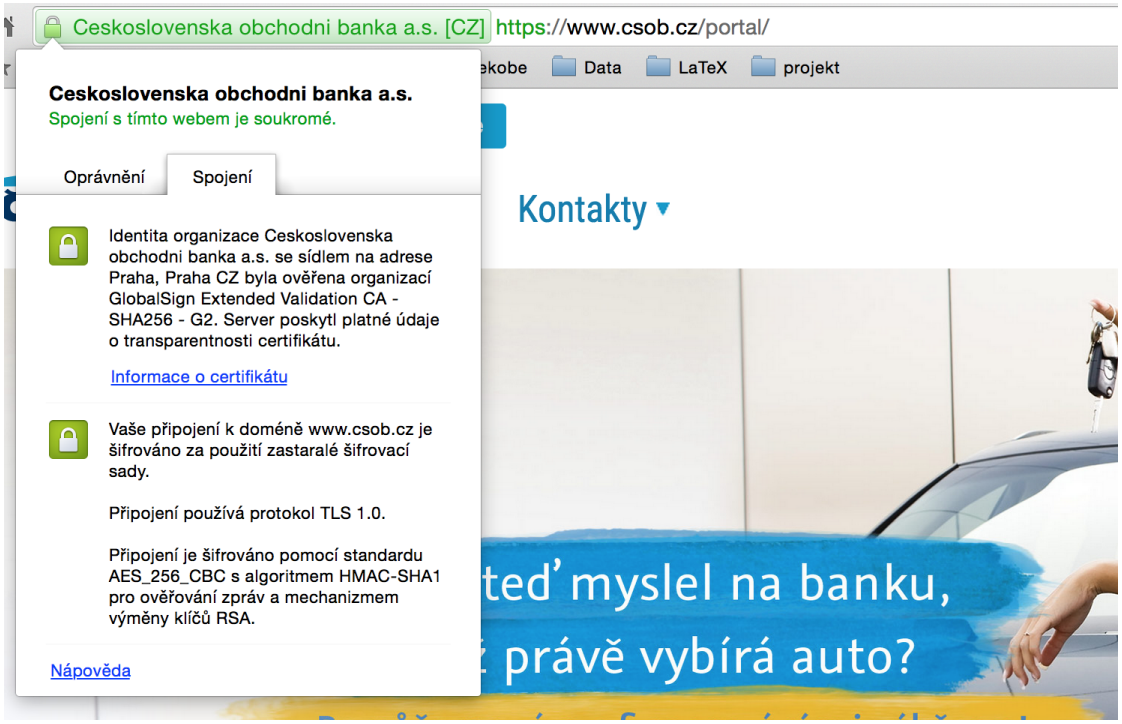
K výše uvedenému je potřeba říci, že v poslední době se trošičku mění pohled na komunikaci tohoto typu informací koncovým uživatelům. Moderní přístup je spíše takový, že při dobré úrovni zabezpečení prohlížeč nesignalizuje nic. Naopak při detekci nějakého problému v zabezpečení je na to uživatel výrazněji upozorňován.

Tento nový způsob je pravděpodobně z pohledu bezpečnosti lepší, jelikož upozornění je vytvořeno v případě, kdy se od uživatele očekává nějaká reakce.

V roce 2023 pak Chrom provede další změnu, kdy místo dosud užívané signalizační ikony zámku použije ikonu jinou, umožňující podrobnější nastavení chování webové stránky, viz obr. 6.3.

6.3 SQL injection

Útoky typu SQL injection využívají slabin v ošetření příkazů v jazyce Structured Query Language (SQL), kterým se manipuluje v záznamy v databázích. Jedná se o útok, který je realizován pomocí



Obrázek 6.2: Příklad bezpečného spojení pomocí WWW prohlížeče Chrome 45 na web ČSOB

běžného rozhraní aplikace často WWW rozhraní, 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 útok 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';
```

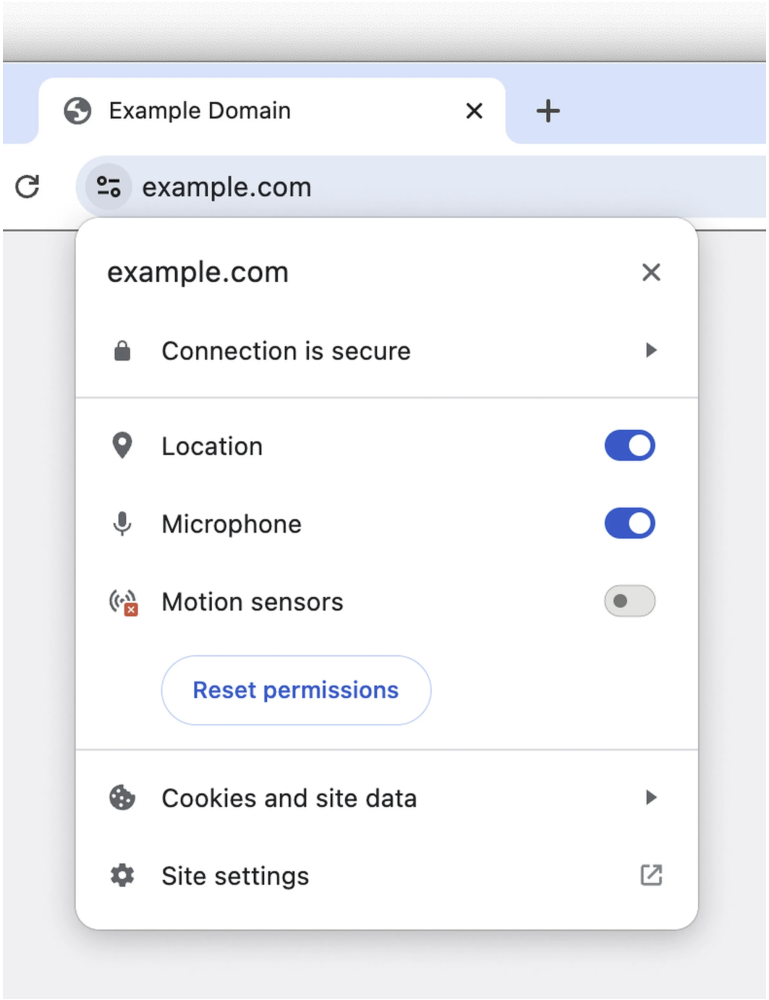
Zadané jméno se přejímá z formuláře - to co tam bude napsané je tedy pod kontrolou případného útočníka. Ten se může rozhodnout místo zkoušení různých jmen a hesel zadat např. následující řetězec: `a' OR 'b'='b`. Systém pak sestaví následující SQL příkaz:

```
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, tedy přímo v aplikaci. Mělo by přitom platit, že údaje zadávané uživatelem



Obrázek 6.3: Změna signalizace bezpečnosti v Google Chrome v roce 2023 (převzato z [69])

Webové aplikace - změny v pohledu na bezpečnost
Signalizace bezpečnostních aspektů provozu na obr. 6.2 a 6.3 jsou pouze průvodními jevy hlubších změn, kterých jsme v posledních letech svědky v ekosystému aplikací. Aplikace dnes jsou navrhovány odlišným způsobem. Webový prohlížeč je často tou platformou, která je využívána pro provoz aplikace. Je to logické rozhodnutí, protože takové aplikace jsou agnostické vůči operačnímu systému, což zjednodušuje jejich vývoj.

Na druhou stranu to otevírá některé otázky, které jsme dosud nemuseli řešit. Jednou z nich, demonstrovanou na obr. 6.3 je k jakému hardware má mít taková aplikace přístup. Toto nastavení nelze realizovat globálně. Globální nastavení by pro všechny stránky přístup k v tomto případě kameře a mikrofonu mohlo povolit nebo zakázat, což ale není žádoucí.

Velmi podobná situace je také s rozšířeními prohlížeče. V roce 2023 začne být v prohlížečích nasazován tzv. manifest v 3, který umožňuje jednotlivá rozšíření povolovat/zakazovat opět na úrovni jednotlivých domén/aplikací.

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 - tyto postupy se souhrnně nazývají *sanitace vstupů*

Z pohledu firemního by měl být kladen důraz na aplikování vhodných postupů vývoje, pokud takové 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.

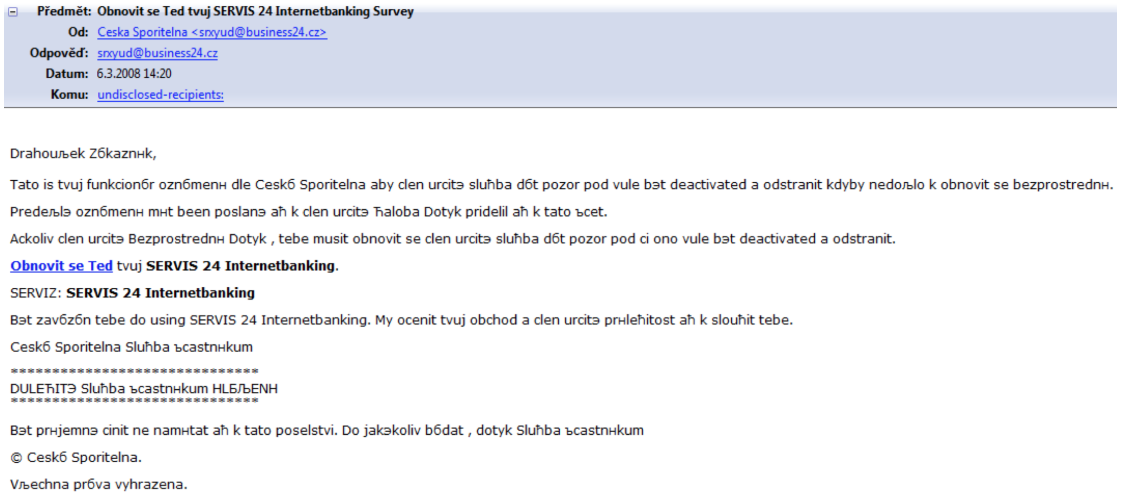
Často používanou metodou pro získávání citlivých informací je *phishing*. V češtině se používá také název *rhybaření*. Útočník kontaktuje budoucí oběť obvykle pomocí e-mailu, ve kterém jej přesvědčuje, že je v jeho nejlepším zájmu sdělit mu osobní nebo jiné citlivé údaje. Phishingové útoky jsou realizovány velmi často na zákazníky bank. Jeden z prvních phishingových útoků v ČR byl dnes již legendární „drahoušek zákazník“, viz obr. 6.4, 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 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.

V alternativním scénáři úročník směřuje uživatele pomocí zaslaného odkazu na podvrženou přihlašovací stránku vypadající jako běžné okno k přihlašování dané organizace. Útočník si dá obvykle práci a zajistí, že toto okno vypadá skutečně jako přesná kopie, aby u uživatelů nevzbudil podezření.



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

Drahoшьek Zбkaznнk,

Tato is tvuj funkcionбr oznбmenн dle Cesk6 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 prнleћitost aћ k slouћit tebe.

Ceskб Sporitelna Sluћba ъcastnнkum

****
DULEЋITЭ Sluћba ъcastnнkum HLБЪENH
****

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

© Ceskб Sporitelna.

Vљechna prбva vyhrazena.

Obrázek 6.4: Drahoušek zákazník - jeden z prvních zaznamenaných phishingových útoků v ČR

Tímto způsobem v současnosti začíná až 90 % útoků na organizaci. Masové rozeslání takových mailů způsobí, že šance, že se někdo chytne je poměrně velká i u ne úplně dobře realizovaných phishingových kampaní. Útočník přitom nepotřebuje kompromitovat mnoho účtů. Stačí mu pár, aby se mu otevřely dveře do vnitřní sítě organizace. Následně může pokračovat v útoku už použitím technických prostředků a slabin v operačních systémech pro eskalaci přístupových práv a tzv. *laterální pohyby*, kdy útočník kompromituje další systémy na síti.

Vhodnou obranou je obezřetnost a zajištění včasných aktualizací software používaného na počítačích v organizaci, tak aby se riziko zneužití známých zranitelností minimalizovalo, což se sice dobře říká, ale realizovat to také prakticky není úplně snadné. Opatření by tak měla fungovat následovně:

- proškolování uživatelů v tomto případě na rozpoznávání phishingových hrozeb a správná reakce na ně
- příprava infrastruktury pro reportování phishingových mailů, které prošly až do schránek koncových uživatelů
- příprava reakce na tento typ incidentů - především ve smyslu schopnosti identifikovat rozsah útoku a nakolik byl úspěšný, identifikace kompromitovaných účtů a jejich blokace, apod.

Výše uvedené kroky a postupy jsou ve skutečnosti poměrně obecné a lze je tak adaptovat na téměř každý typ útoku. Důvodem, proč jej máme rozebrány právě zde je to, že phishing je skutečně dominantním typem útoku, se kterým se uživatelé a organizace, kde jsou zaměstnáváni, musí být schopna rutinně vypořádat.

Pro maximální účinnost výše uvedených opatření je potřeba aby jejich realizace byla formálně upravena. To znamená, že v organizaci by měl existovat formální systém školení, s evidencí frekvence, s kterou mají být jednotlivá školení absolvována. Činnosti by měly být „zprocesovány“ a tyto procesy by měly být formálně popsány a dodržování postupů by mělo být kontrolováno.

Výše uvedené není možné bez poměrně obsáhlé báze vnitropodnikových předpisů. Úvahami tohoto typu se postupně dostáváme k systémům řízení informační bezpečnosti, kterým ale budeme věnovat samostatnou kapitolu.

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, vetšinou USB, v očekávání, že jej někdo najde a podívá se co, je na něm obsaženo, čímž dojde k napadení počítače. Útočník počítá s jednou základní vlastností člověka, a tou je zvědavost.

Správným postupem je v takovém případě nosič sebrat a odevzdat na patřičném místě v organizaci. Může to být administrátor, nebo např. vrátnice/strážní služba, která by měla být vyškolena na to, co s takovým nosičem dál dělat (vyhodit nebo předat dál určené osobě).

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, kam by rozhodně za normálních okolností přístup mít neměl. Technika funguje velmi jednoduše - útočník počká až někdo půjde do zájmové dané oblasti a jde za ním. Oprávněná osoba spustí autentizační proces, útočník ale projde „společně“ s takovou osobou a autentizační proces tak obejde.

I tento útok je založen na přirozeném chování člověka jako „společenského zvířete“. Naše schopnost spolupracovat nás přirozeně nutí, abychom třeba při vstupu do budovy přidržely dveře další osobě, která jimi prochází apod. Z pohledu společenského se jedná o pozitivní vlastnost, z pohledu bezpečnosti je ale jednoznačně jedná o problém.

Řešením je realizace takových opatření, aby každá osoba vstupující do takových oblastí prošla předepsaným autentizačním procesem. Takové prostory by pak měly být viditelně označeny tak, aby každý vstupující člověk jednoznačně věděl jak se má správně chovat.

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* [55].

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 (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 [10]
- 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:

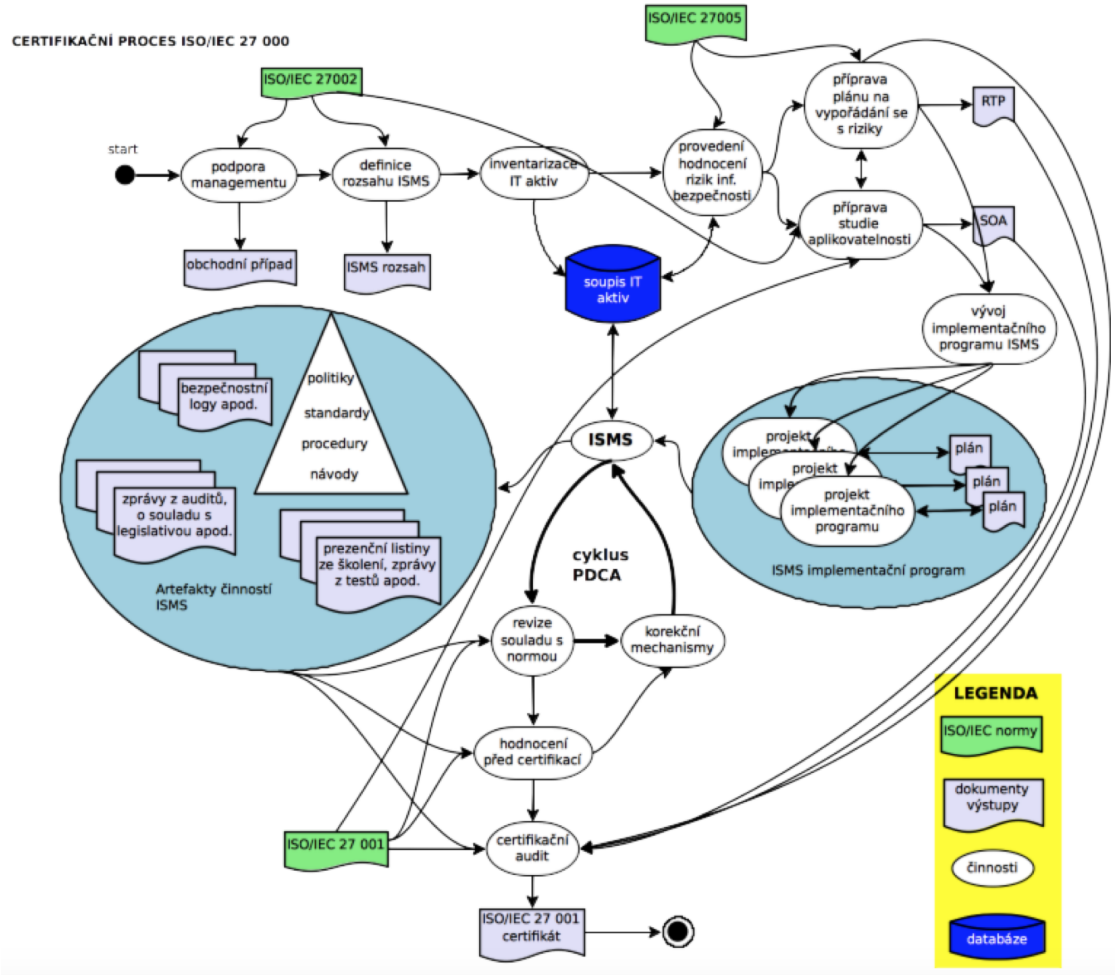
- ISO 27003 - návod pro návrh a zavedení ISMS v souladu s ISO 27001.
- ISO 27004 Information technology - Security techniques - Information security management - Measurement
- ISO 27006 Information technology - Security techniques - Requirements for bodies providing audit and certification of information 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. 8.1.



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.

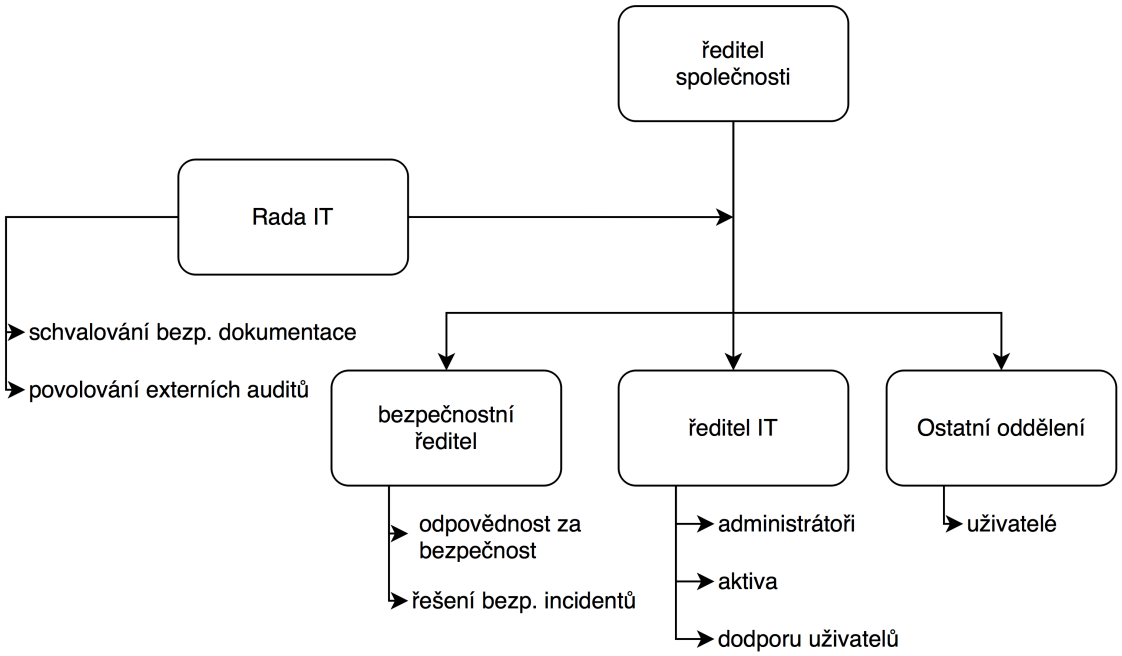
7.3.4 Organizace informační bezpečnosti

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. 8.2). 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.

Kapitola 8

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 (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 [10]
- 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:

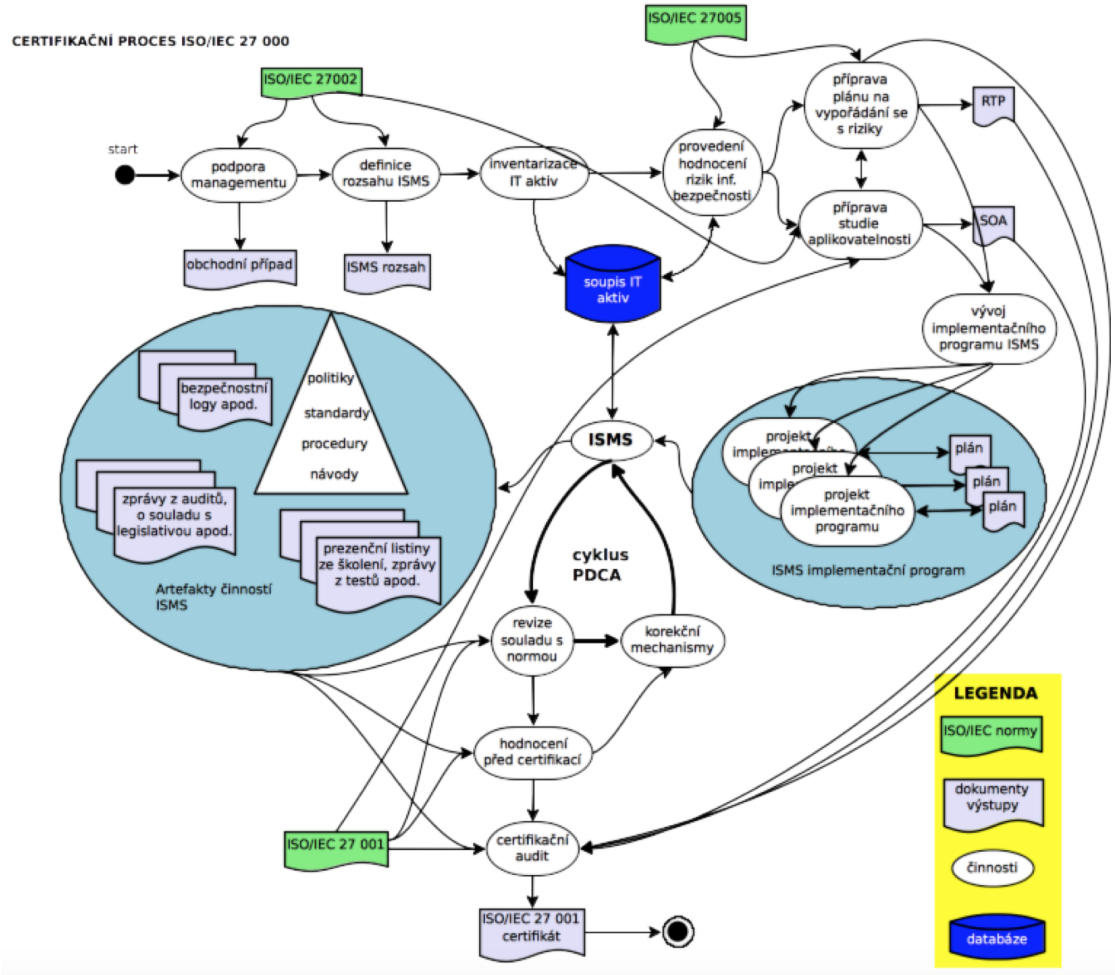
- ISO 27003 - návod pro návrh a zavedení ISMS v souladu s ISO 27001.
- ISO 27004 Information technology - Security techniques - Information security management - Measurement
- ISO 27006 Information technology - Security techniques - Requirements for bodies providing audit and certification of information 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. 8.1.



Obrázek 8.1: 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 (RTP) a studie aplikovatelnosti (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.

8.1 Politika ISMS

8.1.1 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.

8.1.2 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.

8.2 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.

8.3 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.

8.3.1 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.

8.3.2 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
- **garant** - osoba zodpovědná za IT aktivum
- **IS** - informační systém
- **IT** - informační technologie

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

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).

8.3.3 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.

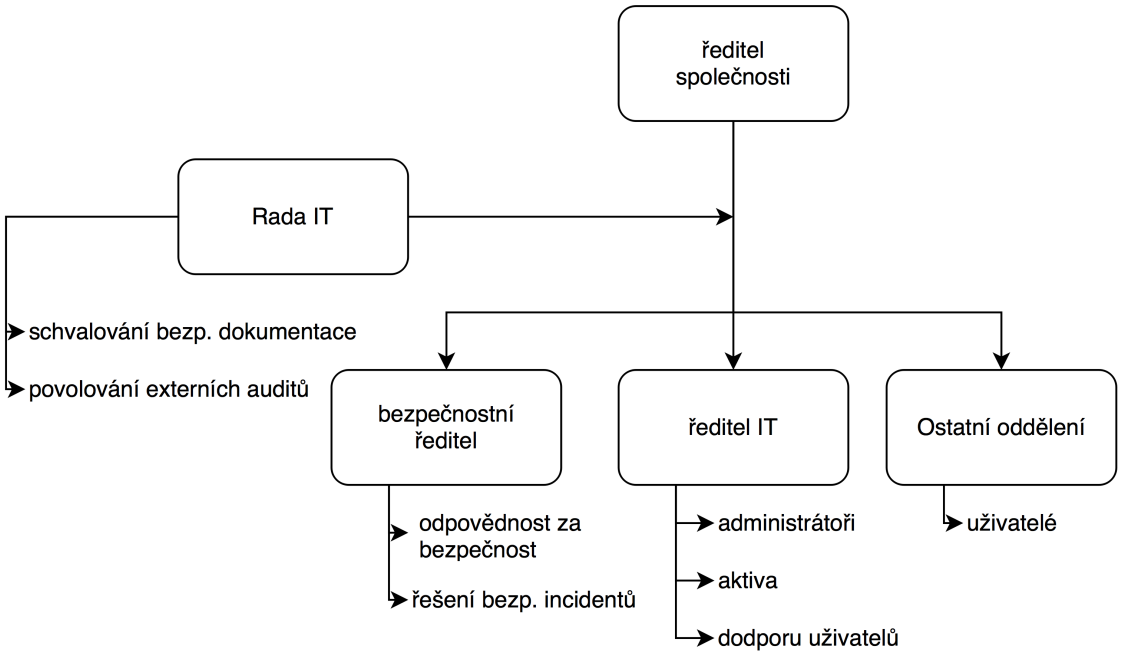
8.3.4 Organizace informační bezpečnosti

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. 8.2). 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 8.2: 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 závažnému bezpečnostnímu incidentu, především v případech, kdy došlo k úniku obchodního tajemství společnosti nebo úniku osobních údajů.

Bezpečnostní rada IT

[2]předpis ABCD:2015 - Rozsah ISMS

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.

8.3.5 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].

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

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.

8.3.6 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.

8.4 Případová studie Bezpečnostní politiky IT aktiva

Komentář

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

8.4.1 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.

8.4.2 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.

8.4.3 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.

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

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.

8.4.4 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.

8.4.5 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.

8.4.6 Přílohy

Komentář

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

Literatura

[1] Acronis TrueImage 2016.

[2] Backblaze Online Backup.

[3] Carbonite.

[4] Clonezilla.

[5] Data Trescor Disc.

[6] DVD-R Information.

[7] Fujitsu Lifebook S935: Notebook, který vám čte z ruky [test].

[8] FVC-onGoing: on-line evaluation of fingerprint recognition algorithms.

[9] Galaxy S5 fingerprint scanner can easily be fooled, hacked.

[10] *ISO/IEC 27 000 Information technology - Security techniques - Information security management systems - Overview and vocabulary.*

[11] John the Ripper benchmarks.

[12] Lenovo ThinkPad T430.

[13] Online Data Backup - Offsite, Onsite, & Cloud - CrashPlan Backup Software.

[14] Paragon Backup & Recovery 2014.

[15] 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.

[16] 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.

[17] 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.

[18] RAID 6 with five disks.

[19] Touch ID.

[20] TPLINK TL-SG1024, switch, 24x10/100/1000 Mbs | SUNTECH Computer - prodej počítačů, elektroniky a spotřebního materiálu.

[21] VeraCrypt.

[22] Wifi Analyzer.

[23] Wikileaks.

[24] CD and DVD writing speed, March 2015. Page Version ID: 653495926.

[25] RSA SecurID, August 2015. Page Version ID: 674333656.

[26] ZTE Grand S3 Release Date, News, Price and Specs, March 2015.

[27] Stay away from CloudFlare, 2017.

[28] CrystalDiskInfo - Crystal Dew World [en], January 2018.

[29] Docker: Accelerated, Containerized Application Development, May 2022.

[30] #1 Password Manager & Vault App with Single-Sign On & MFA Solutions - LastPass, 2023.

[31] Application and Desktop Delivery | Parallels RAS, 2023.

[32] CMR vs. SMR Hard Drive: Which One is Better to be Choosen?, February 2023. Section: Knowledge Center.

[33] Dell PowerEdge M1000e Chassis with 16x M640 Blade Server, 2023.

[34] HPE LTO-9 Ultrium 45TB RW Data Cartridge | AB-COM.cz, 2023.

[35] KeePassXC Password Manager, 2023.

[36] List of TCP and UDP port numbers, June 2023. Page Version ID: 1160288993.

[37] USB, July 2023. Page Version ID: 1162979608.

[38] Oleg Afonin. Elcomsoft Lab: Benchmarking Password Recovery Speeds, June 2023.

[39] Cloudflare. Cloudflare DNS | Authoritative and Secondary DNS, 2023.

[40] Cloudflare. How DDoS protection works · Cloudflare DDoS Protection docs, May 2023.

[41] Adam Cummings, Todd Lewellen, David McIntire, Andrew P. Moore, and Randall Trzeciak. *Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector*. Software Engineering Institute, Pittsburgh, 2012.

[42] Datart. Komplexní Wi-Fi systém TP-Link Deco XE75, AXE5400 WiFi6E Mesh, (1-pack)..., 2023.

[43] Datart. Router Asus RT-AXE7800 (90IG07B0-MU9B00) černý, 2023.

[44] Elcomsoft. Ecomsoft News 2015-06-24.

[45] Fujitsu. PalmSecure® Mouse.

[46] Fujitsu. Fujitsu Releases ARROWS NX F-04g, May 2015.

[47] Google. Public DNS, 2023.

[48] Patrick Grother, Austin Hom, Mei Ngan, and Kayee Hanaoka. Face recognition vendor test (FRVT) part 7 :: identification for paperless travel and immigration. Technical Report NIST IR 8381, National Institute of Standards and Technology (U.S.), Gaithersburg, MD, July 2021.

[49] David Amrani Hernandez. Cracking Passwords is Faster than Ever Before, May 2022.

[50] Mauro Huculak. How to check if a hard drive is failing using SMART on Windows 10, August 2019.

[51] Lukáš Kovanda. Génius John Nash nemohl ani zemřít normálně.

[52] Level1Techs. Hardware Raid is Dead and is a Bad Idea in 2022, 2022.

[53] Alexander Lobkovsky Meitiv. Are Android unlock patterns as secure as numeric PINs?, April 2010.

[54] Mironet cz a.s. Intel Wi-Fi 6E AX210, 2023.

[55] Kevin Mitnick and Wiliam L. Simon. *Umění klamu*. HELION, Praha, 2003.

[56] Netcraft. Web Server Survey May 2023, 2023.

[57] Dmitry Nosachev. File:Supermicro SBI-7228R-T2X blade server.jpg - Wikipedia, October 2015.

[58] O2. O2 Smart Box 2, 2023.

[59] Oracle. Oracle VM VirtualBox, 2023.

[60] Andrew S. Patrick. Fingerprint Concerns: Performance, Usability, and Acceptance of Fingerprint Biometric Systems, June 2008.

[61] Jiří Peterka. Nové e-občanky, co nejsou „e“, January 2012.

[62] Proxmox. Proxmox VE - Virtualization Management Platform.

[63] QNAP. TVS-671.

[64] Michael Q. Retana. Iris recognition, July 2015. Page Version ID: 669758854.

[65] Verbatim. MDISC, 2023. Section: MDISC.

[66] VMWare. Introducing VMware Cross-Cloud Services, 2023.

[67] VŠB-Technická Univerzita Ostrava. Studentský průkaz.

[68] Craig I. Watson, Gregory P. Fiumara, Elham Tabassi, Wayne J. Salamon, and Patricia A. Flanagan. Fingerprint Vendor Technology Evaluation. Technical Report NIST IR 8034, National Institute of Standards and Technology, December 2014.

[69] Jess Weatherbed. Google is retiring the lock icon in Chrome, May 2023.

[70] Lance Whitney. How to Set Up and Use Face ID on Your iPhone, 2022.

[71] ČSOB. ČSOB Smart Key - Apps on Google Play, 2023.

[72] Pavel Šenovský. *Bezpečnostní informatika 1.* VŠB-TU Ostrava, Fakulta bezpečnostního inženýrství, Ostrava, 10 edition, 2022.

Slovník

AD Active Directory.

AES Advanced Encryption Standard.

AP Access Point.

BD Blu-ray Disc.

CD Compact Disc.

CDN Content Delivery Network.

CMR Conventional Magnetic Recording.

CTU Český telekomunikační úřad.

DDoS Distributed Denial of Services.

DHCP DynamicHost Cache Protocol.

DMZ Demilitarizovaná zóna.

DNS Domain Name Server.

DoS Denial of Services.

DSL Digital Subscriber Line.

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.

GDPR General Data Protection Regulation.

GUI Graphical User Interface.

HDD Hard Disc Drive.

HIPS Host Intruder Prevention System.

HPKR Havarijní plánování a krizové řízení.

HTTP Hyper Text Transfer Protocol.

IDM Identity Management System.

IDS Intruder Detection System.

IoT Internet of Things.

IPC Instruction Per Cycle.

IPS Intruder Prevention System.

ISMS Information Security Management System.

ISP Internet Service Provider.

LAN Local Area Nework.

LDAP Lightweight Directory Access Protocol.

LTO Linear Tape Open.

MAC Media Access Control.

MAN Metropolitan Area Network.

MIC Message Integrity Check.

MLO Multi-Link Operation.

MU-MIMO Multi-User Multiple-Input and Multiple-Output.

NAS Network Attached Storage.

NAT Network Address Translation.

NFS Network File System.

NGFW Next-Generation Firewall.

NIPS Network Intruder Prevention System.

PCS poskytovatel certifikačních služeb.

PDF Portable Document Format.

PEAP Protected EAP.

QAM Quadrature Amplitude Modulation.

RAID Redundant Array of Independent Discs.

RAIN Redundant Array of Independent Nodes.

RDAC Role-Based Access Control.

RPC Remote Procedure Call.

RTP Risk Treatment Plan.

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

SAE Synchronous Authentication of Peers.

SAN Storage Area Network.

SMR Shingled Magnetic Recording.

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.

TKIP Temporal Key Integrity Protocol.

TMR True Match Rate.

TNMR True Non-Match Rate.

TRR True Rejection Rate.

UTP Unshielded Twisted Pair.

VLAN Virtuální LAN.

VPN Virtual Private Network.

WAN Wide Area Network.

WEP Wired Equivalent Privacy.

WPA Wi-Fi Protected Access.

[title=Seznam zkratek]

Rejstřík