Bezpečnost a zabezpečení firemních dat

Pavel Pokorný

Bakalářská práce
2014

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2013/2014

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Pavel Pokorný**
Osobní číslo:	**A11196**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Bezpečnost a zabezpečení firemních dat**

Zásady pro vypracování:

1. **Vypracujte pojednání na téma bezpečnost a zabezpečení firemních dat.**
2. **Zaměřte se zejména na přístup k datům.**
3. **Vysvětlete používání firemních ICT pro privátní účely.**
4. **Vysvětlete používání soukromých ICT pro korporátní účely.**
5. **Jmenujte možnosti jednotlivých OS a mobilních platforem.**
6. **Stanovte základní rámec systému řízení bezpečnosti informací.**
7. **Navrhněte bezpečnostní politiku firmy v souladu s normami ČSN ISO/IEC 27001 a 27002.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **PUŽMANOVÁ, Rita. Bezpečnost bezdrátové komunikace: jak zabezpečit wi-fi, bluetooth, GPRS či 3G. Vyd. 1. Brno: Computer Press, 2005, 179 s. ISBN 80-251-0791-4.**
2. **MCCLURE, Stuart. Hacking bez tajemství. 3. aktualiz. vyd. Brno: Computer Press, 2003, XXIV, 612 s. ISBN 80-722-6948-8.**
3. **STANEK, R. Microsoft Windows Server 2003: kapesní rádce administrátora. 1. vyd. Brno: Computer Press, 2003, 535 s. ISBN 80-722-6839-2.**
4. **SMITH, Ben a Brian KOMAR. Zabezpečení systému a sítě Microsoft Windows. 2. vyd. Brno: Computer Press, 2006, 700 s. ISBN 80-251-1260-8.**
5. **DOSTÁLEK, Libor, Marta VOHNOUTOVÁ a Miroslav KNOTEK. Velký průvodce infrastrukturou PKI a technologií elektronického podpisu. 2., aktualiz. vyd. Brno: Computer Press, 542 s. ISBN 978-80-251-2619-6.**

Vedoucí bakalářské práce: **doc. Ing. Martin Sysel, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání bakalářské práce: **7. března 2014**

Termín odevzdání bakalářské práce: **10. června 2014**

Ve Zlíně dne 7. března 2014

prof. Ing. Vladimír Vašek, CSc.
děkan

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

ABSTRAKT

Tato práce se zabývá bezpečností dat při používání informačních a telekomunikačních prostředků a právy na ochranu soukromí jejich uživatelů. Teoretická část je rozdělena na dvě základní kapitoly, které se věnují dvěma základním problematickým situacím vlastnictví a užití zařízení. Jde o střet zájmu mezi soukromím uživatele a bezpečností korporátních dat. Poslední kapitola uvádí principy bezpečnosti z pohledu jednotlivých platforem, které jsou na trhu nejběžnější. V praktické části bakalářské práce je navržen text bezpečnostní politiky, který by se mohl stát univerzální šablonou pro zpracování interního předpisu „Bezpečnostní politika informací“ ve firmách a organizacích a vzory interních směrnic.

Klíčová slova: BYOD, MDM, bezpečnostní politika, ochrana soukromí.

ABSTRACT

This work is concerned with data security in the use of information and telecommunication devices and the rights to privacy of their users. The theoretical part is divided into two basic chapters which deal with two fundamental problematic situations of ownership and use of equipment. It is a conflict of interest between the user privacy and security of corporate data. The last chapter presents the principles of safety in the individual platforms that are most common in market. In the practical part of the bachelor's work is proposed text of the security policy, which could become universal template for processing of the internal regulation "security policy of information" in companies and organizations and templates of internal directives.

Keywords: BYOD, MDM, Security Policy , Privacy Policy.

Poděkování

Tímto bych chtěl poděkovat vedoucímu mé práce doc. Ing. Martinovi Syslovi, Ph.D. za odborné vedení, cenné rady, věcné připomínky a vstřícnost při konzultacích a vypracování bakalářské práce.

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo, bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

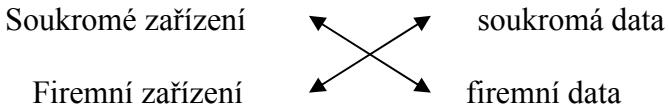
OBSAH

ÚVOD

Počítač, notebook, tablet, mobilní telefon. Zařízení, bez nichž si dnes nikdo nedokáže představit svůj osobní ani pracovní život. Informační technologie jsou nedílnou součástí každodenního života. Je pryč doba, kdy byly doménou pouze firemních prostředí. S jejich klesající cenou a tím i dostupností zaplavují privátní sféru, stávají se běžným pomocníkem a pronikají do všech věkových kategorii a sociálních vrstev. Ruku v ruce s dostupností mobilních zařízení jdou i možnosti mobilního připojení. K čemu by také bylo mobilní zařízení bez připojení k internetu. WiFi, GPRS, EDGE, UMTS, LTO jsou všudypřítomné. Umožnují nám být neustále ve spojení s přáteli, se svoji prací, s celým světem. SMS jsou dnes téměř minulostí. Kdo nemá email nebo profil na sociální síti, jakoby nežil. Kdo by však chtěl u sebe nosit od každého zařízení po dvou kusech. Jedno firemní a jedno soukromé. A toto je právě místo, které umožnuje na jedné straně snižovat náklady, na straně druhé kříží zájmy bezpečnosti firemních dat a soukromí uživatelů ICT. Každá mince má rub i líc. Ani v tomto případě tomu není jinak. Do popředí zájmu se tedy dostávají nejen finanční zájmy, ale i právní aspekty a technologické možnosti. Z pohledu bezpečnosti korporátních dat se v principu jedná o dodržení třech základních aspektů, kterými jsou:

- Důvěrnost
- Dostupnost
- Integrita

Tato práce se bude zabývat dvěma hlavními problematickými spojeními ve vztahu vlastnictví versus ochrana.



Ostatní dvě možnosti, což je soukromé zařízení pro soukromé účely a firemní zařízení pro firemní účely nejsou z hlediska střetu zájmu relevantní.

I. TEORETICKÁ ČÁST

1 POUŽÍTÍ FIREMNÍCH ICT PRO PRIVÁTNÍ ÚČELY

Z pohledu firemních hodnot bývají nejdůležitějším a nejcennějším aktivem firmy její data. Informační a komunikační technologie (dále jen ICT) mají také svoji hodnotu, obzvláště tu pořizovací, ale data byla, jsou a vždy budou tím nejcennějším aktivem. ICT jsou však prostředky pro jejich zpřístupnění a práce s nimi. Z tohoto důvodu jsou z pohledu bezpečnosti a ochrany dat nejkritičtějším místem.

Žádný zaměstnavatel nevynakládá finanční prostředky k tomu, aby nakoupil zařízení, jež bude zaměstnanec používat pouze pro svou vlastní potřebu. Vždy je pořizuje pro zajištění činností souvisejících s provozem firmy. Podle bezpečnostní politiky firmy je pak více či méně jejich uživatelům umožněno jejich používání nad rámec firemních účelů, tj. pro pokrytí privátních potřeb jejich uživatelů.

Z hlediska mobility se rozlišují firemní zařízení na dvě základní skupiny

- **Nepřenosná**. Tato zařízení jsou stabilně připojena do interní LAN firmy a neopouštějí brány firmy. Jedná se převážně o desktopové počítače a servery.
- **Přenosná**. Říká se jim také mobilní. Jsou to ta zařízení, kterým to dovolí jejich konstrukce a jsou převážně určena pro práci v terénu. Sem se řadí mobilní telefony, notebooky, tablety, ale také přenosné harddisky, flash paměti, SD/microSD karty, a jiné.

1.1 Rizika

Rizika, která vznikají, vyplývají z jisté nekontrolovatelnosti zařízení, když jsou mimo firmu, nebo při jejich neodpovědném používání uvnitř společnosti. Jejich uživatelé je připojují do různých privátních sítí s negarantovanou bezpečností obvykle s úmyslem se zdarma připojit k Internetu. Takové volné WiFi připojení však nemusí být vždy poskytováno s dobrou vůlí jako bezplatná služba pro zajištění konektivity v některé lokaci, ale může jít o úmyslně poskytovanou konektivitu s cílem získat kontrolu nad sítovým provozem jejich uživatelů. Stejně tak se ale může škodlivý kód dostat do prostředku ICT,

který sice fyzicky prostory firmy neopustil, zato jeho neodpovědný uživatel navštívil nedůvěryhodné webové stránky nebo otevřel podezřelou přílohu ve svém emailu.

Na základě metod uvedených v knize *Hacking bez tajemství* [1] lze odvodit nejběžnější rizika, kterými jsou:

- Napadení škodlivým kódem
- Převzetí kontroly nad zařízením
- Krádež, editace či zničení firemních dat
- Možnost šíření z jednoho nakaženého zařízení na další prostředky v interní síti
- Odposlouchávání elektronické komunikace
- Zjišťování autentizačních a autorizačních údajů
- Omezení dostupnosti služeb
- Zneužití technických prostředků k páchání další činnosti

V odborném světě se pro některé metody útoků na ICT nebo elektronická data zavedly a ustálily jejich odborné názvy. Nelze zde vyjmenovat všechny, navíc se jejich seznam každým dnem rozšiřuje. Ty nejznámější jsou tyto:[1]

- Cracking – označení metody pro narušení informačního systému zvenčí
- Hacking – narušení bezpečnosti či stability počítačových sítí
- Phreaking – bezplatné využívání telefonních linek
- Phishing – metody získávání a zneužívání personálních a autentizačních údajů
- Pharming – odposlouchávání elektronické komunikace a získávání údajů pomocí změny v DNS záznamech
- Social engineering – metoda pro získávání informací za účelem napadení informačního systému
- Spamming – nevyžádaná pošta
- Malware – škodlivý kód, sloužící k narušení či ovládnutí funkčnosti a služeb jednotlivých prostředků ICT. Dělí se na
    - Viry – škodlivý kód likvidující funkce prostředků ICT
    - Trojské koně – nosný SW pro infikaci počítačů jiným škodlivým kódem
    - Adware – jde o SW k podpoře získání a odposlechu informací z koncových zařízení
    - Spyware – SW pro utajené odesílání údajů o uživateli
- Bombing – zahlcování poskytované služby velkým množstvím paketů

- Defacement – nahrazení originálních stránek jejich podvrženou variantou
- DoS – při tomto útoku je server nebo služba zahlcena velkým množstvím requestů
- DDoS – forma DoS útoku prováděna soustředěně z velkého množství stanic
- MiM – forma odposlouchávání elektronické komunikace
- Ransomware – útok, kdy útočník znepřístupní data jejím majitelům a vyžaduje „výkupné“
- Sniffing – útok založený na odposlouchávání paketů
- Spoofing – útok založený na falšování identity zdroje

1.1.1 Nepřenosná zařízení

U těchto zařízení se na první pohled zdá, že jim žádné riziko nehrozí. Jsou přece připojena stále pouze do interní sítě a jsou pod kontrolou specialistů-administrátorů. Jistá míra pravdivosti by v tomto případě platila za předpokladu, že ze zařízení není možné komunikovat s okolním světem. V takovém případě by rizika spočívala pouze v úmyslném jednání zaměstnance. Toto však není předmětem této práce.

Běžnější je případ, kdy je zařízení připojeno do Internetu nebo je v něm používáno emailových služeb. Zde jsou rizika zavlečení škodlivého kódu již zřejmá. Následující seznam uvádí přehled nejčastějších činností uživatelů, které vedou ke snížení bezpečnosti používaných prostředků a elektronických dat, v krajním případě až k ohrožení všech prostředků a dat uvnitř interní sítě.

- Spouštění podezřelých příloh
- Návštěva webových stránek se škodlivým kódem
- Vypínání bezpečnostních opatření (lokální FW, antivir, atd.)
- Běžná práce s uživatelským oprávněním „administrátor“ nebo „root“
- Používání neschválených SW
- Připojování neznámých medii (flash disk, CD/DVD, atd.)
- Odkliknutí hlášek a upozornění bez jejich důkladného přečtení
- Ponechané přihlášené pracovní stanice bez dozoru
- Obcházení proxy serveru

1.1.2 Přenosná zařízení

V dnešní době je trendem, že každý manažer či specialista dostane pro výkon svých pracovních činností a plnění úkolů od zaměstnavatele mobilní telefon, notebook, případně tablet. Obvykle nakonfigurovaný pro vzdálené připojení do LAN prostředí svého zaměstnavatele. Je to zcela nezbytné, jelikož používat zařízení v off-line režimu, by bylo neefektivní. Obvyklými požadovanými službami jsou email, file systém v podobě sdílených disků, databáze a firemní aplikace jako například Intranet. V ideálním případě využívají zaměstnanci těchto zařízení pouze pro firemní účely dle stanovených interních předpisů. Mnohem běžnější je ale stav, kdy zaměstnanci využívají tato zařízení i pro své soukromé aktivity. Je to zcela logické. Komu by se chtělo také nosit u sebe dva kusy od každého zařízení. Dva mobily, dva notebooky, atd. Je-li pominuto morální hledisko, je zcela běžné, že si zaměstnanci ve své pracovní době občas vyřídí své soukromé záležitosti, stejně tak se počítá s tím, že zaměstnanec vybavený mobilní technikou svého zaměstnavatele bude občas pracovat i ve svém volnu. Jsou zde sice určité možnosti rozpočítávání nákladů za soukromé a služební hovory, případně existují mobilní telefony na dvě SIM karty, tudíž může zaměstnanec mít jedno zařízení, které mu umožní provádět služební hovory ze služební SIM a soukromé hovory ze soukromé SIM. Jak ale zajistit rozlišení na notebooku zda zaměstnanec dělá některé činnosti v rámci svého pracovního nasazení nebo pro svou vlastní potřebu? Toto rozpoznat nelze. Rozpočítání nákladů na pořízení a provoz těchto zařízení je pouhou druhotnou záležitostí. Primárním úkolem je zajistit bezpečnost firemních dat uložených off-line a bezpečnost firemního interního prostředí při vzdáleném připojení. Díky jejich mobilitě se také zvyšují i bezpečnostní rizika. Kromě rizik uvedených u nepřenosných zařízení jsou tu ještě další:

- Změna hesla lokálního administrátora (při bootování z CD se specializovaným SW nástrojem)
- Krádež zařízení
- Používání zařízení neoprávněnou osobou, například rodinným příslušníkem
- Připojování zařízení do privátních a veřejných sítí
- Úpravy routovacích tabulek
- Odpozorování zadávaných autentizačních údajů

1.2 Ochrana firemních dat

Je logické, že každá firma se snaží přiměřeným způsobem chránit svoje data a informace. A nejde jen o zákonem definované informace. V mnoha případech se totiž jedná o nejcennější aktivum firmy. Materiálové ztráty bývají v porovnání se ztrátou citlivých firemních informací nepodstatné. Materiál se dá lehce koupit znovu. Důvěra dodavatelů a klientů však nikoliv. Prozrazení firemního „Know How" může vést i k jejímu zániku. Co za taková data a informace lze považovat? To je dost rozdílné. Záleží převážně na povaze a podnikatelském zájmu daného subjektu. Mezi hlavní, z pohledu firmy chráněné informace patří:

- Informace o zaměstnancích
- Informace o klientech
- Finanční informace
- Know How
- Informační zdroje
- Informace o nových projektech
- Licenční a patentové informace
- Zdrojový kód
- Marketingové strategie
- Zákonem chráněné informace. V praxi se jedná převážně o osobní a citlivé údaje klientů a zaměstnanců [2], ale i informace definované zákonem na ochranu utajovaných skutečností [3].

Z pohledu bezpečnosti samotných ICT jsou ale předmětem zájmu ochrany také:

- Konfigurace zařízení a síťových prvků
- Používané technologie a jejich verze
- HW zdroje
- Autentizační údaje
- Licence
- DRP/BCP

Účelem bezpečnostních opatření není jen ochrana před jejich zcizením. Mnohdy stejné dopady může mít i jejich pouhá nedostupnost. Samozřejmostí je i ochrana jejich důvěryhodnosti a autentičnosti neboť i pouhé poškození důvěryhodnosti a image firmy, může mít katastrofální následky.

Formy ochrany vycházejí především z procesních, režimových, legislativních a technických možností a opatření. Při výběru vhodných opatření se musí vycházet z analýzy rizik, bezpečnostní politiky organizace a především z předpokladu, že investice vynaložené do bezpečnosti nesmí překročit hodnotu chráněných informací.

1.3 Právní aspekty

Mezi zaměstnavateli a zaměstnanci přežívá názor, že firemní zařízení a vše co je v nich, patří zaměstnavateli, který má právo na jejich ochranu a kontrolu. Na ochranu bezpochyby, nicméně s kontrolou to tak již jednoznačné není. Stejně tak jako zaměstnavatel nemůže své zaměstnance bezdůvodně svlékat, aby se přesvědčil, zda nevynáší firemní materiál, i v oblasti výpočetní techniky má kontrola své hranice nejen etické a morální, ale i právní. Argument, že si zaměstnanec nemá do počítače ukládat soukromá data zde neobstojí. Interním předpisem se sice může takovýto zákaz prosadit, ale co data, která si zaměstnanec sám do počítače vědomě neuloží a přesto mají privátní charakter? Ano, i tato situace může nastat. Typickým příkladem je soukromý email. I přestože došel na pracovní emailovou adresu, jedná se stále o privátní soukromou korespondenci. V tomto případě nepomohou žádné interní předpisy, směrnice, zákazy. Takový email může dojít, aniž by to zaměstnanec mohl ovlivnit. Restrikce na seznam povolených odesílatelů nám také nepomohou. Nejen, že by byli omezeni zaměstnanci v jejich možnostech komunikace, což by bylo zřejmě na úkor pracovních výsledků, ale i adresát uvedený na whitelistu může poslat email s privátním obsahem. Situace je však ještě mnohem složitější než se zdá. Za elektronickou komunikací a elektronickými daty se neskrývají jen soubory a emaily uložené v osobních počítačích a telefonech. Spadá sem celá problematika monitorování provozu, logování, archivování, atd. Zaměstnanci mají právo na své soukromí, ale jak zařídit, aby přidělených prostředků nezneužívali pro své soukromé účely, neohrožovali bezpečnost firemních dat, ba dokonce je nepoužívali k páchání trestné činnosti, obzvláště k interním fraudům?

Co říká trestní, pracovní a obchodní zákoník? Které zákony řeší ochranu firemních dat? Na konferenci Security 2012, pořádané firmou AEC v Praze, vystoupil se svoji přednáškou na téma „Právní aspekty DLP a monitoringu“ advokát JUDr. Tomáš Sokol z advokátní kanceláře Brož & Sokol & Novák. Během své přednášky doporučil především tyto zákony[4], [5], [6], [7], [8].

- **Zákoník práce - § 316**

(1) *Zaměstnanci nesmějí bez souhlasu zaměstnavatele užívat pro svou osobní potřebu výrobní a pracovní prostředky zaměstnavatele včetně výpočetní techniky ani jeho telekomunikační zařízení. Dodržování zákazu podle věty první je zaměstnavatel oprávněn přiměřeným způsobem kontrolovat.*

(2) *Zaměstnavatel nesmí bez závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele narušovat soukromí zaměstnance na pracovištích a ve společných prostorách zaměstnavatele tím, že podrobuje zaměstnance otevřenému nebo skrytému sledování, odposlechu a záznamu jeho telefonických hovorů, kontrole elektronické pošty nebo kontrole listovních zásilek adresovaných zaměstnanci.*

(3) *Jestliže je u zaměstnavatele dán závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele, který odůvodňuje zavedení kontrolních mechanismů podle odstavce 2, je zaměstnavatel povinen přímo informovat zaměstnance o rozsahu kontroly a o způsobech jejího provádění.*

- **Zákoník práce - § 301**

Zaměstnanci jsou povinni
a) pracovat řádně podle svých sil, znalostí a schopností, plnit pokyny nadřízených, vydané v souladu s právními předpisy a spolupracovat s ostatními zaměstnanci,
b) využívat pracovní dobu a výrobní prostředky k vykonávání svěřených prací, plnit kvalitně a včas pracovní úkoly,
c) dodržovat právní předpisy vztahující se k práci jimi vykonávané; dodržovat ostatní předpisy vztahující se k práci jimi vykonávané, pokud s nimi byli řádně seznámeni,
d) řádně hospodařit s prostředky svěřenými jim zaměstnavatelem a střežit a ochraňovat majetek zaměstnavatele před poškozením, ztrátou, zničením a zneužitím a nejednat v rozporu s oprávněnými zájmy zaměstnavatele.

- **Zákoník práce - § 302**

Vedoucí zaměstnanci jsou dále povinni
a) řídit a kontrolovat práci podřízených zaměstnanců a hodnotit jejich pracovní výkonnost a pracovní výsledky,
b) co nejlépe organizovat práci,
c) vytvářet příznivé pracovní podmínky a zajišťovat bezpečnost a ochranu zdraví při práci,
d) zabezpečovat odměňování zaměstnanců podle tohoto zákona,
e) vytvářet podmínky pro zvyšování odborné úrovně zaměstnanců,
f) zabezpečovat dodržování právních a vnitřních předpisů,
g) zabezpečovat přijetí opatření k ochraně majetku zaměstnavatele.

- **trestní zákoník - § 220**

(1) Kdo poruší podle zákona mu uloženou nebo smluvně převzatou povinnost opatrovat nebo spravovat cizí majetek, a tím jinému způsobí škodu nikoli malou, bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti.
(2) Odnětím svobody na šest měsíců až pět let nebo peněžitým trestem bude pachatel potrestán,
a) spáchá-li čin uvedený v odstavci 1 jako osoba, která má zvlášť uloženou povinnost hájit zájmy poškozeného, nebo

b) způsobí-li takovým činem značnou škodu.

(3) Odnětím svobody na dvě léta až osm let bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 škodu velkého rozsahu.

- **obchodní zákoník - § 17**

Předmětem práv náležejících k podniku je i obchodní tajemství. Obchodní tajemství tvoří veškeré skutečnosti obchodní, výrobní či technické povahy související s podnikem, které mají skutečnou nebo alespoň potenciální materiální či nemateriální hodnotu, nejsou v příslušných obchodních kruzích běžně dostupné, mají být podle vůle podnikatele utajeny a podnikatel odpovídajícím způsobem jejich utajení zajišťuje.

Toť litera zákona.

Z výše uvedených citací je zřejmé, že práva jsou na obou stranách, stejně tak ale i povinnosti. Kde je však hranice mezi nezbytnou kontrolou a špehováním? Jednoznačná odpověď neexistuje. Nejen, že záleží na jistém etickém a morálním přístupu k věci, ale i na odpovědném přístupu k svěřené věci stejně tak i výkladu právníka, který bude tu kterou stranu zastupovat. Proto i zde platí, že nejlepší je se na všem předem domluvit a využívat všeho s mírou. Ať již svěřeného majetku zaměstnancem, tak i práv a pravomocí zaměstnavatele.

Rozumným kompromisem jistě bude, když zaměstnavatel bude činnosti zaměstnanců logovat a pro své potřeby používat agregovaná data, jako jsou například statistiky vytěžování linek, prostorová obsazenost úložišť, množství přenesených dat za jednotku času, navštěvované URL (ale bez uvedení jména uživatelů), množství SPAMU, množství zachyceného malware, počty bezpečnostních incidentů, atd. V případě, že zaměstnavatel na základě nasbíraných statistických dat pojme podezření, že dochází k neúměrnému využívání svěřených prostředků, které neodpovídá pracovním činnostem, měl by o jeho zjištění informovat zaměstnance a upozornit je, že v případě, že nedojde ke zlepšení stavu, využije svého práva na ochranu majetku a zavede detailnější sledování. V každém případě však musí ctít právo na ochranu soukromí zaměstnanců. Číst soukromou korespondenci nebo odposlouchávat soukromé hovory rozhodně nesmí. Toto opatření smí být použito jen v případě podložených podezření ze spáchání trestné činnosti a to jen orgány činnými v trestním řízení na základě písemného souhlasu soudce. Proto je ve sporných případech lepší raději využívání svěřených prostředků pro privátní účely zabránit než sledovat jejich zneužívání. Takovým vhodným opatřením může být například odebrání administrátorských práv, nebo zavedení proxy serveru s webovým filtrem.

V praxi se také osvědčuje myslet dopředu na případy, kdy zaměstnanec ukončí pracovní poměr. Jelikož ochrana soukromí platí i po skončení pracovního poměru. Jak se ale dostat na pracovní emaily a pracovní dokumenty uložené v profilu bývalého zaměstnance? Jak poznat, která data jsou pracovní a která firemní aniž bychom si je přečetli? Takovým vhodným způsobem je například interním předpisem definované pojmenování složek nebo předem udělený písemný souhlas zaměstnance se zpřístupněním emailové schránky. Dobrým řešením je zavádět emailové adresy na základě funkce a pracovního zařazení než na základě jména uživatele. Když například organizace zavede emailovou schránku recepcni@firma.cz, ucetni@firma.cz, skladnik@firma.cz je již z názvu patrné, že slouží k pracovní korespondenci a smí do ní dostat přístup každý, kdo dostane od jejího majitele,

kterým je v tomto případě zaměstnavatel, souhlas. Pokud se místo této konvence využívá osobních jmen zaměstnanců tak je majitelem schránky uvedená osoba a vztahuje se na ni poštovní zákon. V tomto případě by šlo o poštu ekvivalentně určenou do rukou adresáta.

Zaměstnavatel musí mít také na paměti, že pokud zaměstnanec bude chtít zneužít svých přidělených oprávnění či pravomocí, může tak učinit různými způsoby, tudíž bude zřejmě neefektivní zavádět restrikce na odeslanou poštu, nebo investovat nemalé prostředky do řešení na analýzu logů s cílem zjistit, zda zaměstnanec nevynáší z firmy důležitá data cestou emailové komunikace, když ví, že tak může zcela snadno učinit třeba nahráním dat na externí paměťové medium nebo si důležité dokumenty ofotit.

Zaměstnanci zase musí vědět, že veškeré jejich počínání může být nebo je sledováno. Z tohoto důvodu je důležité nesdělovat například autentizační údaje svým kolegům, jelikož ti je tak mohou snadno využít k provedení činností, které by si pod svým identifikátorem netroufli učinit.

Jakými způsoby, metodami a opatřeními lze zajistit ochranu firemních dat, jaké jsou technické, režimové a procesní možnosti se věnuje následující kapitola.

1.4 Způsoby ochrany firemních dat

Technické možnosti v dnešní době, ať již HW nebo SW jsou stále důmyslnější a výkonnější. Bohužel neslouží pouze nám, ale i těm, kteří je dokáží využít proti nám. Pryč jsou doby, kdy se někdo pokoušel prolomit ochranu vlastními silami. V dnešní době jsou k těmto účelům používány roboty, které dělají hrubou práci za své tvůrce. Proto bývá ochrana skládající se z více článků, i když samostatně slabších, mnohem účinnější než ochrana jedním zdánlivě silným opatřením. Útočníka spíše odradí sada bezpečnostních opatření, kterými musí projít, než jedna jediná zábrana, kterou může například prolomit hrubou silou reprezentující výpočetní výkon počítače, který má k dispozici. Stačí takový stroj naprogramovat k tomu, aby zkoušel generovat možné kombinace znaků nebo dešifrovat/uhádnout šifry, hash. V takovém případě je limitujícím faktorem pouze čas.

Chránit firemní data, prostředky a prostředí lze mnoha způsoby. Zde se nabízí nepřeberné množství právních, procesních, režimových a technických opatření. Zde jsou

popsány ty nejdůležitější a nejzásadnější, vycházející ze seznamu opatření uvedených v normě ISO 27001 [9].

1.4.1 Vzdělávání

Základním pravidlem a bezpodmínečnou nutností při jakékoliv ochraně je vzdělávání a školení vlastních zaměstnanců. Nejenže tato činnost je z hlediska nákladů téměř zanedbatelná, ale je zcela nezbytná. *Bezpečnost informací uložených na přenosných počítačích a na mobilních zařízeních je závislá především na tom, nakolik vážně berou uživatelé zabezpečení těchto aktiv a nakolik se řídí zásadami či bezpečnostními politikami pro ochranu notebooků* [10]. Školení lze provádět externími odborníky nebo i vlastními silami. Důležité je spíše, aby tyto vzdělávací aktivity byly účelné, pravidelné, a byly následně zaměstnanci dodržovány. K těmto účelům je možné použit více forem. Osvědčenými formami jsou:

- **Kodex** - Jedná se o dokument, ve kterém jsou shrnuty základní principy. Zaměstnanci musí být s těmito principy obeznámeni a musí je přijmout za své. Obsah takového kodexu se s časem nemění.
- **Školení** - Úkolem školení je obnovit zapomenuté znalosti, prohloubit je, případně naučit účastníky kurzu věcem novým. Je potřeba, aby školení reflektovala vývoj v daném směru poslední doby a připravila posluchače na nové možnosti, v tomto případě na hrozby.
- **E-learning** - V poslední době oblíbená forma školení. Jde o elektronickou formu školení, která má přinést vyšší efektivnost díky častějším periodám a nižším nákladům. Výhodou je možnost pružně propagovat novinky a upozornění.
- **Testy** - Například test sociálního inženýrství, nebo penetrační testy. Jde o metody etického hackingu, které jsou prováděny interními nebo externími specialisty. Jejich účelem je na praktické ukázce demonstrovat slabiny a navrhnout nová nebo upravit stávající bezpečnostní opatření.

1.4.2 Interní směrnice

Směrnice, nařízení, prováděcí pokyny. Jedná se o soubor závazných firemních opatření, jejichž znalost musí být zaměstnanci písemně potvrzena. Tyto směrnice musí být zaměstnancům kdykoliv k dispozici. Jejich vznik a editace musí podléhat schválení a okamžitému internímu zveřejnění. Musí odrážet místní legislativu. Je vhodné je psát v duchu některé doporučující normy. (ISO 9001, ISO 27001, atd.) Příkladem může být směrnice pro přístup k osobním údajům klientů, má-li organizace udělen od UooU (úřad na ochranu osobních údajů) souhlas ke zpracování osobních údajů. Obvykle má každá větší organizace zpracován ucelený soubor interních předpisů, které vycházejí z bezpečnostní politiky podniku.

1.4.3 Procesní/režimová opatření

Vhodná preventivní opatření snažící se eliminovat možnosti vzniku některé z hrozeb. Obvykle slouží k zákazu nebo nařízení některých opatření tam, kde nelze tyto prvky vynutit technickými opatřeními nebo na některá omezení předem upozornit. Příkladem může být zákaz vnášení fotoaparátů, zákaz vynášení elektronických medii, atd.

1.4.4 Logování

Jde o metodu ochrany, která má za úkol zaznamenávat stav událostí a zajistit tak případné důkazy a v případě nastavených korelačních pravidel zasílat upozornění. Logování má z pohledu bezpečnosti více významů, proto bude tato problematika probrána trochu podrobněji.

1.4.4.1 Druhy logů

Každý SW musí z důvodu bezpečnosti umět logovat veškerou svoji aktivitu. Příkladem jsou auditní a provozní logy OS, DB, APP. Každý SW může typy logů pojmenovávat svoji jmennou logikou, v principu se však jedná o tyto základní aktivity.

- **User management** - Logování aktivit správy uživatelských účtů a jejich autentizaci. Logovat se musí úspěšné i neúspěšné operace. Úspěšné jako důkazy

o provedení operace daného uživatele. Neúspěšné autorizace nám signalizují pokusy o prolomení autentizačních prvků

- **Net flow** - Záznamy o sítovém provozu
- **Audit log** - Záznam aktivit uživatelů. Zaznamenává operace prováděné samotnými uživateli. Kam přistupovali, která data měnili
- **System log** - Stejný typ jako audit log, ale zaměřený na záznamy aktivity uživatelů s vyššími oprávněními. V tomto případě jsou zaznamenávány události související s nastavováním a parametrizací samotného SW
- **DB log** - Typ logu zaměřený na databázové systémy

Je-li zajišťován v organizaci vysoký stupeň bezpečnosti, musí se zajistit, aby logy byly ukládány na jiné místo, než kde jsou pořizovány a přístup k nim nesmí mít pro jejich editaci ti uživatelé nebo administrátoři, jejichž aktivity jsou logovány.

1.4.4.2 Využití

Využití logů je velmi široké, přitom v praxi často opomíjené. Umožnuje nejen zpětně zjistit konkrétní událost, ale i hlásit podezřelé aktivity. S jeho pomocí dokážou zkušení specialisté vyhledat důvody nestability SW a vyladit jeho možnosti. Je nenahraditelným důkazním materiálem v oblasti ICT. Jejich použití se dá rozčlenit do dvou základních rolí.

- **Dle osob:**
  - User - Méně často používané. V praxi se spíše používá pouze omezený výpis z logu vztahující se k aktivitě daného uživatele. Například poslední přihlášení
  - Admin - Účelem je poskytnout správci SW dostatek informací k řešení nenadálých stavů a potíží
  - Auditor - Principem je dát auditorům možnost zpětné kontroly aktivit uživatelů nebo samotného SW
  - Security - Z pohledu bezpečnosti nejzajímavější oblast. V logách, pokud jsou správně nastaveny, se skrývá mnoho užitečných informací, ze kterých lze vysledovat bezpečnostní incidenty, případně zasílat upozornění na tyto aktivity

- **Dle účelu:**
  - Řešení potíží/chyb. Viz dělení dle osob: admin
  - Získávání důkazů. Viz dělení dle osob: security
  - Controlling: Viz dělení dle osob: auditor

1.4.4.3 Struktura a formát

Aby bylo možné se v logách vyznat a byly účelné, je důležité zajistit jejich správný formát a strukturu. Struktura logu musí být dodržena v každé zaznamenané položce v daném logu. Nejdůležitějšími položkami ve struktuře každého logu jsou:

- **Kde** - V kterém SW, DB, tabulce, APP. V podstatě určuje zdroj logu.
- **Kdy** - Kdy přesně k uvedené události došlo. Optimální je zaznamenávat datum a čas s přesností na vteřiny.
- **Kdo** - Obvykle login, username, uder ID, atd.
- **Co** - Logovaná událost. Rozumné je předem si stanovit, které události jsou pro daný účel logování relevantní. Selekcí událostí se zajistí lepší datová průchodnost, velikost logů a jejich přehlednost.
- **Jak** - Obvykle se loguje použitá syntaxe příkazu, technologie, oprávnění atd.
- **Typ** - Read, change, edit, write, delete, create, atd
- **Status** - Accept, false, error, OK, 0, 1, deny, atd.
- **Hodnota** - Doplňující relevantní informace. Textový nebo číselný řetězec.

Log, ve kterém se nikdo nevyzná, je k ničemu. Aby bylo možné logy číst a automaticky zpracovávat, je nutné dodržovat nějaký zavedený standard. Samozřejmě lze použít i svůj vlastní formát, ale v takovém případě je nutné k němu dodat podrobný manuál a v případě že bude potřeba použít nějaký typ automatického zpracování, bude nutno vytvořit i nějaký konektor do SIEMu. Zavedenými formáty na poli logování jsou:

- SYSLOG – Systémové
- DB – Databázové
- CSV – Tabulkové
- LOG, TXT - Textové

1.4.4.4 SIEM - Nástroje pro automatické zpracování

Logy obsahují velké množství informací. Mohou obsahovat miliony událostí a co do objemu dat zabírat i řádově GB (GigaByte). V takovém množství informací by se těžko hledalo bez vhodných automatizovaných nástrojů. Ty slouží nejen pro sběr a agregaci logů, ale i jejich archivaci, vyhledávání informací v nich a pro manažery bezpečnosti i důležitý reporting. V případě, že jsou nastavena potřebná pravidla, může tento nástroj vyhledávat automatizovaně podezřelé aktivity a o výskytu těchto událostí informovat. Způsoby informování jsou dány technickými možnostmi daného nástroje. Obvykle se jedná o grafické, emailové, či SMS notifikace. Nejznámějšími nástroji v tomto oboru jsou podle Gartnerova magického kvadrantu produkty QRadar od IBM, ArcSight od HP.

1.4.4.5 Zálohování/archivace logů

Aby logy mohly plnit svůj účel, musí být k dispozici nejen kdykoliv, ale i z období, které nás právě zajímá. Požadovaná doba archivace je u každého logu různá. Záleží na důležitosti logovaných informací, legislativních nařízení, možnostech a kapacitách zálohovacích medii, a požadovaném účelu, který mají logy plnit. V případě že se logují události pouze z důvodu ladění systému, bude nám stačit uchovávat logy řádově ve dnech. Archivace síťových logů se pohybuje řádově v měsících. Auditní a systémové logy je vhodné mít k dispozici po dobu cca 1-2 let. Naopak historie bankovních transakcí se například musí, dle nařízení ČNB, uchovávat 10 let od 1. ledna následujícího roku, kdy došlo k ukončení smluvního vztahu.

1.4.5 Monitoring

Na rozdíl od logování, kde se sledují aktivity uživatele, představuje monitoring sledování stavu HW a SW prostředků. Příkladem může být sledování dostupnosti služby (IIS, Apache, Windows services, atd.) nebo HW (dostupnost/průchodnost linky, dostupnost serveru, sítového prvku) případně jejich vytížení a stav. Typickým příkladem je vytížení procesoru nebo zaplnění HDD. Průběžné, či on-line sledování stavu může v raných fázích zachytit náhlou změnu stavu, která nemusí být vždy způsobena jen technickými problémy,

ale může signalizovat podezřelou aktivitu škodlivého kódu, hackera, DoS útoku, atd. Stejně jako u logování, je možné doplnit monitoring o automatickou notifikaci v případě, že některá sledovaná entita překročí definovanou hodnotu.

1.4.6 Autentizace/autorizace

Snad nejznámější a nejpoužívanější typ ochrany informací a dat, založený na seznamu uživatelů s definovanou úrovní přístupu.

1.4.6.1 Autentizace

Je proces ověření identity uživatele, který se přihlašuje k danému systému. Pro tyto účely je možné použít mnoho způsobů. Pro zajištění vyšší bezpečnosti je vhodné kombinovat dva a více způsobů. Tomu se říká dvoufaktorová a vícefaktorová autentizace. Podle autorů knihy *Velký průvodce infrastruktury PKI* [11] jsou způsoby autentizace rozděleny na 4 skupiny.

- **Něco znám**
    - Heslo - Nejznámější metoda. Jelikož je tato metoda stále nejrozšířenější, jsou v kapitole 3.1.1 bezpečnostní zásady uvedeny jejich základní pravidla.
    - PIN - Řetězec obvykle numerických znaků. Typická délka je 4-6 čísel. Vhodná metoda pro dvou faktorovou autentizaci ve spojení s autentizačními kartami a čipy.
    - Bezpečnostní otázky - Tato metoda se nejčastěji používá jako náhradní metoda pro autentizaci v případě zapomenutí hesla. Typickou otázkou je „Jméno vaší matky za svobodna“. Pro zajištění rozumné úrovně bezpečnosti je nutné volit otázky a odpovědi, jež zná pouze ten, který je definuje. Odpovědi uživatel definuje obvykle při procesu zakládání účtu, což bývá jeho největší slabinou. Od té doby obvykle uběhla již dlouhá doba, a uživatel si již nepamatuje odpovědi.

- Obrázky - Moderní metoda založená na zapamatování si určité sady obrázků z dané množiny. Její bezpečnější forma využívá i možnosti jejich správného pořadí.
- Gesta - Metoda, která se rozšířila díky mobilním telefonům. Uživatel pro autentizaci musí nakreslit zvolený čárový obrazec.

- **Něco mám**
  - Magnetická karta - Informace o uživateli je uložena v magnetickém proužku
  - Čipová karta - Modernější verze identifikačních karet. Informace jsou uloženy v elektromagnetickém čipu. Výhodou je bezkontaktní použití.
  - HW/SW token - Metoda využívající generování unikátního řetězce znaků v čase. V praxi to znamená, že při každém použití se vygeneruje nový unikátní řetězec. Tato metoda je obzvláště vhodná jako nástroj při odposlouchávání elektronické komunikace. I když útočník zachytí použitý kód, nemůže ho při příští autentifikaci použít.
  - Certifikát - Skládá se z veřejného a privátního klíče. V asymetrické kryptografii jde o digitálně podepsaný veřejný šifrovací klíč. Je-li vydán důvěryhodnou certifikační autoritou a je-li zabezpečen heslem, stává se rozumným kompromisem mezi bezpečností a investicí.
- **Něčím jsem –** nejčastěji biometrický údaj. Tyto metody jsou známé díky science fiction filmům. V dnešní době jsou však již běžně dostupné. Nevýhodou této metody je, že jejích použití se musí řídit dle legislativy na ochranu osobních údajů.
  - Papilární linie – metoda využívající papilárních linii na prstech končetin.
  - Žilní řečiště – používá se žilní řečiště dlaně
  - biometrie oka – metoda využívající oční sítnici a duhovku
  - Bipedální lokomoce – metoda vyhodnocení chůze a kroků
  - Hlas – Tato metoda je svým způsobem ojedinělá, jelikož jako jediná z biometrických údajů, se dá použít na dálku. Tohoto začínají využívat některé bankovní instituce pro identifikaci klientů při volání na Call Centra.
  - Obličej – metoda, při které se používá geometrie celého obličeje.

- **Něco umím**
    - Podepsat se. Metoda vyhodnocující nejen obrazovou stránku podpisu, ale i rychlost a dynamiku psaní, přítlak, atd.

Z podstaty skupin je pak logické, kterým útokům daná metoda odolává. Například v případě metody „něco znám“ odolávám fyzické krádeži autentizačního prvku, třeba karty. V případě metody „něco mám“ odolávám vzdálenému odposlouchávání zadaných údajů. Proto je tak důležité kombinovat obě z těchto metod.

1.4.6.2 Autorizace

Je proces ověření, zda k dané operaci nebo přístupu má daný autentizovaný uživatel oprávnění či nikoliv. Oproti autentizaci, kde dochází k identifikaci uživatele, se v případě autorizace ověřují jeho přístupová oprávnění a role. V praxi se jedná o ověření, zda daný uživatel má nejen oprávnění přístupů k informacím, ale též i způsob s jejich nakládáním. Například read, write, edit, create, atd. Známou metodou autorizace je také členství ve skupinách jako například users, administrators, editors, atd.

1.4.7 Symetrická a asymetrická kryptografie

Metody jsou rozšířené díky elektronickým certifikátům, které lze dnes pořídit v ceně již od cca 150 - 300 Kč. Jde o nejběžnější metody pro zajištění integrity a důvěrnosti dat. Slouží především pro:

Podepisování - Má za úkol zajistit, aby bylo garantováno od koho, případně z jakého zdroje data a informace pochází a bylo garantováno, že během přenosu nemohlo dojít k jejich editaci bez toho, aby to cílová strana věděla. Nejznámější použití je při podepisování emailů a elektronických dokumentů odesílaných na úřady státní správy.

Šifrování - Zajišťuje to, aby data nebo komunikace nebyla pro nepovolané osoby čitelná. Že je komunikace šifrovaná lze rozpoznat podle použitého protokolu, například HTTPS, FTPS, atd.

Druhou možností je šifrování statických dat. Méně známé, zato velmi užitečné, je šifrování obsahu celého paměťového media. Šifrovat lze obsah HD, flash disků, přenosných disků, atd. Jde o velice účinnou formu ochrany informací pří ztrátě nebo zcizení mobilních zařízení. K obsahu paměťového media se uživatel dostane pouze po správné autentizaci. Bez jeho znalosti zůstává obsah šifrovaný. Díky moderním a silným algoritmům se jedná o bezpečnou metodu ochrany dat a informací. Kromě komerčních řešení je v poslední době hodně mobilních zařízení obsahujících možnosti šifrování standardně jako součást jejich OS.

HASH - Velmi důležitou funkci při ochraně dat představuje tzv. HASH (otisk). *Otisk je jednocestná funkce, která nám z libovolně dlouhého textu vytvoří krátký řetězec konstantní délky* [11]. Mezi nejběžnější hašovací funkce současnosti patří SHA-2. Různé protokoly, například TLS, SSL, SSH, S/MIME, IPsec používají SHA-2 k zajištění některých svých funkčností. Dá se říct, že jde o nástupce hašovací funkce MD5.

1.4.8 Antivir

Toto řešení není snad nutné představovat. Jde o software pro operační systémy, který má za úkol detekovat a odstraňovat počítačové viry a jiné škodlivé kódy. Pro běžné uživatele jde o nutné zlo, které jim zpomaluje počítač a stále zobrazuje nějaké informace na monitoru. Pro poučené uživatele užitečný nástroj a pro odborníky zcela nepostradatelná součást každého OS. V korporátní sféře se o instalaci, distribuci aktualizací a celkovou správu starají obvykle správci sítě. Pro jejich snadnější vzdálenou správu existují od dodavatelů těchto SW management console. Ty umožnují správcům centrálně spravovat veškeré klienty. Nejznámějšími firmami na trhu jsou Avast, Symantec, Eset, AVG, Kasperski, McAfee, Norton, atd. Platí pravidlo, že není tak důležité od jakého výrobce je pořízený antivirový SW, ale to, aby byl pravidelně aktualizován, správně nastaven a stále v činnosti. Antivirové nástroje současnosti jsou komplexním souborem mnoha nástrojů, hlídajících nejen souborový systém uživatele, ale i jeho internetové aktivity, emailové přílohy a další užitečné nástroje. V případě detekce viru nabídne tři základní možnosti:

- Opravit/vyléčit. Tato možnost může při jejím zvolení být úspěšná či nikoliv
- Karanténa. Tato možnost zablokuje infikovaný soubor pro jeho další použití
- Smazání. Nenávratně odstraní nakažený soubor i s virem

1.4.9 FireWall

Jedná se o HW/SW nástroj pro řízení síťového provozu. Jde o zařízení, které spojuje různé sítě s různou důvěryhodností. Zjednodušeně se dá říct, že kontroluje každé spojení a na základě definovaných pravidel je buď propustí nebo zamítne. FW jsou zařazeny do několika kategorií dle jejich schopnosti analyzovat do hloubky procházející spojení.

- **Paketový filtr.** FW s nejjednodušší logikou. Kontroluje provoz pouze na základě zdrojové a cílové IP adresy a portu. Kontrola probíhá na 3 a 4 vrstvě OSI modelu
- **Aplikační brány**. Říká se jim také proxy firewally. Rozdělují spojení na dvě samostatná. Klient se nejprve připojí na aplikační bránu, ta požadavek zpracuje, a pokud není zamítnut, tak vytvoří k cílové adrese nové spojení, kde klientem je IP adresa aplikační brány. Výhodou je vyšší bezpečnost, nevýhodou HW náročnost.
- **Stavové paketové filtry s kontrolou protokolů**. Tyto FW umí dynamicky otevírat porty na základě požadovaných spojení u složitějších protokolů.

Firewally nejsou doménou pouze sítových specialistů s inženýrským titulem a Cisco certifikací, kteří spravují rozsáhlé LAN a WAN. Základní firewally, tedy spíše paketové filtry, dnes existují i jako free nástroje třetích stran pro pracovní stanice nebo mohou být i součástí operačních systémů. Nastavování pravidel však vyžaduje základní znalosti sítových protokolů. Proto je většina běžných uživatelů nevyužívá.

1.4.10 Proxy/Web filtr

Problematika proxy je sice složitější, ale postačí, když bude vysvětlen základní účel. Proxy se používá pro oddělení lokální sítě od Internetu. Nejčastějšími důvody pro jeho nasazení jsou filtrování provozu, cachování provozu, logování a samozřejmě bezpečnost. Vlastností proxy také využívají útočníci pro směrování provozu přes jejich kontrolovanou proxy, která je schopna provoz zachytit a analyzovat. Z tohoto důvodu je důležité pro citlivá spojení, například do internetového bankovnictví, používat zabezpečené protokoly.

Nejznámější využití proxy je centrální přístupový bod pro přístup k Internetu. Tím, že je zavedena povinnost přístupu na internet přes řízenou proxy, může se na ni nejen pomocí

cachování urychlit načítání stránek, ale hlavně definovat pravidla a nasadit takzvané webové filtry.

Webové filtry jsou SW nástavby, které umí řídit přístup k jednotlivým webovým stránkám na základě jejich obsahu nebo definovaného black/white listu. S jednoduchým webovým filtrem je možno se setkat přímo v některých internetových prohlížečích. Zde se jim říká rodičovská kontrola. V korporátní sféře se však používají sofistikovaná a placená řešení s širokou škálou možností. Kromě blokování stránek umí umožnovat přístup na základě autentizace, řadu reportů a statistik, které lze využít při analýze využívání internetu zaměstnanci. Představitelem těchto komerčních řešení je například Kernun web filtr.

1.4.11 VPN/IPsec

Pro bezpečné propojování různých ICT existuje velký výběr různých nástrojů, protokolů a jejich rozšíření. Hlavními principy, na kterých jsou založeny, jsou tunelování a šifrování. Z dostupných metod a prostředků jsou zde uvedeny dvě základní, reprezentující obě metody.

IPSEC – Jde o rozšíření IP protokolu, které k zajištění bezpečnosti používá autentizaci a šifrování všech IP datagramů.

VPN – Z anglického Virtual Private Network je dobře odvoditelný princip. Jde o propojení počítačů do lokální virtuální sítě, které se využívá pro bezpečné propojení PC přes nedůvěryhodnou síť. V principu jde o tunelové spojení. To znamená, že se mezi dvěma body naváže tunel, obvykle přes internetové spojení a uvedené dva body následně komunikují přes tento tunel. Spojení se uskutečňuje na základě digitálních certifikátů a je šifrované. Tato metoda je hojně využívána pro připojení notebooků do lokální firemní sítě.

Instalace a konfigurace těchto prvků patří do pracovních činností firemních IT specialistů. Vzhledem k tomu, že tyto metody umožnují bezpečný přístup do firemní LAN, je nutné, aby jejich uživatelé byli seznámeni s pravidly a riziky. Nejlépe nějakým předávacím protokolem nebo interním předpisem. Často se totiž stává, že si uživatelé význam neuvědomují a přenáší si tyto prvky na privátní zařízení nebo v případě služební techniky ji zapůjčují k práci jiným osobám. Z těchto důvodů zavádí správci obvykle sekundární opatření, jakými mohou být třeba dodatečná autentizace nebo seznamy MAC adres.

1.4.12 Klient/server

Jde o síťovou architekturu, jejímž cílem je oddělit role. V tomto případě server plní roli poskytovatele služeb a klient je pouze prostředek pro jejich zpřístupnění. Klient a server spolu komunikují přes počítačovou síť. Klientem může být grafické uživatelské rozhraní (GUI) nebo i celý HW, například terminálová stanice. V praxi se používají dvě verze klienta:

- **Těžký klient** (fat client) – aplikace vyvinutá pro daný účel. Pro danou aplikaci existují instalační balíčky. Nevýhodou bývá omezení na zařízení, na kterém je aplikace instalována a případné licenční podmínky. Na stranu druhou mívá těžký klient obvykle více funkcí a možností než jeho „lehčí“ varianta.
- **Tenký klient** (thin client) – jde o počítač nebo program, který pro poskytnutí dané služby silně závisí na serveru. V poslední době velmi oblíbená varianta z důvodu její univerzálnosti. Ve většině případů však poskytuje omezenější možnosti. V případě SW varianty se nejčastěji používá pro připojení ke službě internetový prohlížeč.

Význam pro bezpečnost je zřejmý. Data jsou umístěna na firemním serveru, který je obvykle ve správě datového specialisty, tudíž jsou relativně zabezpečena. Na klienta se tak kromě dodržování základních bezpečnostních pravidel nekladou žádné speciální požadavky.

1.4.13 User management

Jde o ucelený soubor opatření pro řízení přístupových oprávnění. Mít přehled o přidělených oprávněních a přístupech je nejen z pohledu bezpečnosti nezbytné, ale v případě zpracovávání osobních údajů i povinné. Vyžaduje to zákon 101/2000sb [2]. Je to zcela pochopitelné. Nejen, že takto lze získat přehled o tom, kdo má v jaké aplikaci a systému oprávnění, ale dovolí nám to provádět pravidelné audity a reagovat neprodleně v kritických situacích. Obzvláště dnes, kdy firmy vyžívají různých externích aplikací poskytovaných v rámci Internetu, má takový dobře vedený user management nezastupitelnou roli. V případě, že některý zaměstnanec nebo externista ukončí smluvní

vztah (nebo mu byl s okamžitou platností ukončen) je tak k dispozici seznam všech jeho přístupů, které lze neprodleně blokovat.

Druhou, neméně významnou rolí user managementu, je schvalovací proces během zakládání uživatelských práv. Obzvláště v rozsáhlých organizacích, kde jsou odpovědnosti za různé aplikace, databáze a jiné prvky s přístupem k datům a informacím rozděleny mezi více správců nebo garantů. A nemusí jít jen o přístup k firemním informacím. V praxi se osvědčuje mít v evidenci i ostatní přístupy. Příkladem může být řízený přístup k internetu.

Poslední, stejně tak důležitou rolí user managementu je odpovědnost za dostatečně škálovatelné odstupňování rolí. Jistě není vhodné, aby všichni zaměstnanci viděli všechna data, nebo měli možnost je editovat. Proto je důležité při výběru a vývoji aplikací pamatovat i na to, aby dokázaly řešit přístupy na různých úrovních. Obzvláště kritické jsou tzv. privilegované účty. Zapomínat se nesmí i na přístupy, které budou vyžadovat auditoři.

1.4.14 Zálohování/archivace

Zálohovat, zálohovat a zálohovat. Základní tři pravidla všech, kteří mají odpovědnost za nějakou část ICT. Profesionálové jsou si důležitosti zálohování dobře vědomi. Běžní uživatelé se obvykle k zálohování uchylují až v době, kdy dojde poprvé ke ztrátě jejich dat. V principu zálohování/archivace plní dvě základní bezpečnostní funkce:

- **Důkazní** - v případě, že někdo neoprávněným způsobem zasáhl do informací, je možné dohledat původní stav a provedenou změnu. Samozřejmě to vyžaduje jistou pravidelnost v zálohování s co nejkratším časovým rozpětím.
- **Záložní/obnovovací** - tato funkce se hodí nejen, když dojde k neoprávněné modifikaci či smazání dat, ale i v případě havárií systémů nebo jen při běžných servisních zákrocích.

Rozdíl mezi archivací a zálohováním je následující.

- **Záloha** - Záznam dat daného IS k určitému datu a v určité situaci na jiné fyzické datové úložiště nebo na externí medium. Tato záloha je uchovávána do doby provedení další zálohy. Cílem je zajistit obnovu systému a aktuálních dat v případě výpadku.

- **Archivace** - Záznam dat daného IS k určitému datu a v určité situaci na jiné fyzické datové úložiště, nebo na externí medium. Jedná se o zálohu historických dat. Tato záloha je uchovávána po stanovenou dobu, bez ohledu na množství dalších provedených záloh či archivací. Data, která byla použita k archivaci, již nemusí být dostupná online.

Aby bylo množství zálohovaných dat udrženo na rozumné velikosti, je nezbytné zálohovat/archivovat jen nutná data. Jelikož by objem uchovávaných dat časem mohl i tak přerůst archivační kapacity, vyvinuly se pro tyto účely speciální SW nástroje a metody. Pro názornost jsou zde uvedeny pouze tři základní.

- **Full backup** - Kompletní záloha celého media, databáze, aplikace či jiného informačního systému. Tato metoda má největší nároky na kapacitu archivačních medii, ale pro obnovení bývá nejspolehlivější a nejrychlejší.
- **Diferencial backup** - Při této metodě dochází k zálohování jen těch dat, která byla změněna od posledního full backup. Metoda poměrně rychlá a úsporná.
- **Incremental backup** - Při této metodě dochází k zálohování jen těch dat, která byla změněna od poslední zálohy. Touto zálohou může být full backup nebo diferenciální backup. Při této metodě dochází k největší úspoře archivačních kapacit, ale narůstá doba potřebná k obnovení. Stejně tak roste riziko, že se nám proces obnovy nepovede.

Zálohování a archivace je problematika natolik obsáhlá, že není možné se ji věnovat dopodrobna v této práci. Proto jsou níže uvedena jen základních pravidla, o kterých se zmiňuje William R. Stanek ve své knize *Windows Server 2003* [12].

- Tím prvním je vybrat spolehlivá media. V privátních případech nám zřejmě budou sloužit flash disky, CD/DVD media, nebo externí disky. V korporátní sféře se pro zálohování a archivaci používají obrovská datová úložiště s disky zapojenými do některého RAID, magnetické pásky LTO, DLT. Ty samozřejmě vyžadují příslušné zapisovací a čtecí mechaniky. Jejich kapacita se dá zvětšovat spojováním do virtuálních knihoven. Media se musí pravidelně kontrolovat na jejich čitelnost.

- Druhou důležitou zásadou je umístění záložních a archivačních medii. Zřejmě by nebyly k ničemu zálohy umístěné na mediích, která shořela i s prostředky ICT, které na nich byly zálohovány, díky tomu, že byly umístěny v jedné místnosti. Také musí být umístěny tak, aby k nim měly přístup pouze odpovědné osoby.
- Třetí důležitou zásadou je jejich pravidelnost. Jde sice o činnosti, které zvyšují nároky na HW, finance i lidské kapacity, ale pouze pravidelné zálohování může přinést požadovanou funkčnost v případě, že nastane situace, kdy bude zapotřebí obnovy dat.

1.4.15 Terminálové služby

Jde o formu zpřístupnění aplikace a dat uživatelům. U těchto řešení se nevyužívá připojení ke službě přes instalovaného klienta v mobilním zařízení ani webového rozhraní, ale uživateli se přenáší pouze grafické rozhraní aplikace, která je spuštěno na terminálovém serveru nebo jeho vzdálená plocha. Uživatel tak pouze pomocí vstupních periferií (klávesnice, myš, touchpad) ovládá aplikaci, která je spuštěna na vzdáleném serveru. V principu jde o to, že je každému uživateli otevřena jeho vlastní session. Toto řešení má dvě výhody. Jednou z nich je možnost zpřístupnění aplikace z různých platforem, a tou druhou samozřejmě bezpečnost. Pro vzdálenou komunikaci jsou otevřeny pouze porty, které jsou nutné pro navázání terminálové služby. Nevýhodou bývá u lepších řešení nutnost zakoupení licencí a potřebná odborná správa. Nejznámějšími službami jsou Windows terminal services, Citrix.

1.4.16 DRP/BCP

Jde o preventivní, dokumentované soubory opatření a postupů, které nám slouží v případě havárie prostředků ICT nebo ztrátě, zničení dat.

DRP - Disaster Recovery Plan. Plán obnovy v případě havárie. Jde o dokument, ve kterém je podrobně popsán postup pro obnovu havarovaného prostředku ICT. Obsahem je instalační manuál, HW/SW požadavky, správná konfigurace, doporučený postup, umístění instalačních medii, závislosti na jiných ICT a jiné nezbytné informace pro zajištění obnovy

poskytovaných služeb v co nejkratším čase. Nezbytnou součástí jsou i kontakty na odpovědné osoby a definování jejich rolí a pravomocí.

BCP – Business Continuity Planning. Jde o strategické plánování zajištění kontinuity podnikání v případě krizových situací. Celé plánování musí vycházet z analýzy rizik a následné impakt analýzy, což je analýza možných dopadů. Cílem je definovat kritická místa a procesy a navrhnout vhodná opatření a strategii obnovy.

1.4.17 DLP

Data Loss Prevention. Jde o softwarová řešení pro identifikaci firemních dat a kontrolu před jejich únikem. Zavedení těchto řešení umožnuje organizacím mít větší kontrolu nad svými daty. Díky možnosti řízení přístupu ke konkrétním typům informací či sledování jejich pohybu a použití. Bez použití těchto nástrojů může v jisté fázi organizace ztratit kontrolu nad tím, kdo k daným datům má přístup. Například, když oprávněný zaměstnanec z některé aplikace vytáhne vzorek dat a uloží je pak na sdílený disk nebo je odešle emailem. DLP software jde v tomto případě o krok dále. Dokáže námi definovaná data označit a toto značení si sebou nese při každém jeho zkopírování nebo použití. Tím může být například odeslání přes email nebo výtisk. Vhodným nastavením upozornění a blokací se získá lepší kontrola nad těmito daty, ale vyžaduje to mít instalované klienty na všech zařízeních, která potencionálně přicházejí v úvahu.

1.4.18 Update/patch/service pack

Tyto instalační balíčky řeší nejen funkční nedostatky a rozšíření informačních systémů, ale i zacelují nalezené bezpečnostní slabiny. Obvykle se objeví informace o jejich výskytu a instalaci spolu s nutností restartovat operační systém v situaci, kdy je to zrovna nejméně vhodné. Naštěstí většina výrobců a dodavatelů má tento proces zautomatizovaný a neklade na uživatele žádné nároky. Je pouze dobré si uvědomit význam těchto servisních balíčků a neblokovat jejich instalaci. V korporátní sféře distribuci těchto balíčků zajištují obvykle správci, kteří předem otestují, zda nebudou mít negativní vliv na chod jimi spravovaných firemních systémů a aplikací.

Jak je vidět, možnosti jsou velké. Ale i tak tento výčet není úplný. Stále vznikají nové technické možnosti. Stejně tak lze za způsob ochrany považovat jakékoliv režimové či

procesní opatření. Každý, kdo je za ochranu firemních dat odpovědný, musí zvážit mnoho faktorů a vybrat sadu těch nejvhodnějších opatření a metod. V případě, že je v daném oboru nováčkem, může využít služeb odborníků na tuto problematiku nebo si pomoci zavedením systému řízení bezpečnosti informací, například ISMS, které vychází z mezinárodní normy ISO 27001 [9], což je mezinárodně platný a uznávaný standard pro řízení informační bezpečnosti. Organizace, které mají zavedena veškerá opatření uvedená v normě ISO 27001, mohou požádat o certifikaci, která je pro jejich obchodní partnery vizitkou důvěryhodnosti. Z toho plynou nejen konkurenční výhody, ale i povinnost každé 3 roky před auditem tuto certifikaci obhájit.

2 POUŽÍVÁNÍ PRIVÁTNÍCH ICT PRO FIREMNÍ ÚČELY

S rozmachem převážně mobilních ICT se dostávají zaměstnavatelé do situace, kdy nemohou dostatečně pružně reagovat na jejich dostupnost a oblíbenost. Do popředí zájmu se tak dostávají úvahy, zda nepovolit zaměstnancům používat jejich osobní, mnohdy modernější mobilní prostředky. Z ekonomického pohledu by to bylo jistě pro firmu jednoznačné plus, ale je nutné si uvědomit, že tyto prostředky nemá zaměstnavatel ve své správě, tudíž z pohledu ochrany informací by se k nim měl chovat jako k nedůvěryhodným. Tyto prostředky mohou být zdrojem potencionálního škodlivého kódu nebo se jejich prostřednictvím může dostat do interní LAN nepovolaná osoba. Ne všichni jejich majitelé jsou uvědomělí a technicky zdatní. Ba naopak. Tím že jsou vlastníky těchto prostředků, používají je převážně ke svým soukromým aktivitám. Připojují je do různých free sítí, navštěvují z pohledu bezpečnosti nedůvěryhodné webové stánky, instalují si SW různé kvality a funkčnosti. Při instalaci nevěnují pozornost podrobným informacím. Z finančních důvodů stahují instalační balíčky z nelegálních úložišť. Vzájemně si tato zařízení půjčují a co je v tomto případě asi nejdůležitější, je skutečnost, že je obvykle nemají vybavena žádným bezpečnostním SW, jako například antivir, antispyware, antiadware, FW, či jiné sofistikované nástroje. Vyjma skutečných IT odborníků, jsou převážnou většinou těchto zařízení z pohledu ICT bezpečnosti naprostí amatéři. Uživatelská přívětivost a jednoduchost ani nenutí majitele těchto zařízení se blíže zabývat odborným nastavováním a konfigurací. Pro tyto účely existují stále propracovanější wizardy, které dovolují jejich uživatelům připojit mobilní zařízení k jakékoliv službě bez hlubších IT znalostí. Obvykle stačí znát správný odkaz, login a heslo, případně mít k dispozici správný certifikát.

A jak tedy těchto soukromých zařízení využít pro firemní účely? Jaké jsou výhody a nevýhody? Jaká z toho vyplývají rizika a jak jim čelit? Toto jsou otázky, na které bude dána odpověď v této kapitole.

Jak pro soukromé tak i firemní prostředky platí stejná pravidla, rizika, hrozby. Rozdíl je pouze v přístupu k těmto možnostem a úrovni jejich odborné péče. Veškerá pravidla a rizika uvedená v kapitole I. Jsou naprosto stejná. Není potřeba je tedy na tomto místě uvádět znovu. U soukromých zařízení je však jejich význam mnohem větší.

2.1 Výhody a nevýhody

Každá mince má svůj rub i líc. Ani u této problematiky tomu není jinak a tak používání privátních zařízení s sebou přináší výhody, ale i nevýhody.

2.1.1 Výhody

Převážně ekonomické hledisko je na první pohled zřejmé, které není nutné blíže rozvádět. Úspora při nákupu drahých zařízení, obzvláště ve velkém množství, je evidentní. Ale jsou tu i další, neméně důležité výhody. Jako další výhodu lze uvést rozmanitost používaných platforem, neboť v korporátní sféře je zvykem z důvodu množství potřebných specialistů se omezovat na jednu vybranou platformu, která je zavedena jako firemní standard. Významnou výhodou je využívání technologických novinek, na které by obvykle došlo ve firmě až s jistým časovým odstupem. I množství takto vybavených uživatelů je významných aspektem. Firma obvykle mobilními prostředky vybavuje jen pracovníky na vybraných pozicích. Tím, že umožní mobilní přístup i řadovým zaměstnancům, zvýší tak jejich produktivitu. Akceschopnost a dostupnost zaměstnanců v mimopracovní době je též vítanou výhodou stejně tak, jako úspory za kancelářské prostory a vybavení v případě trvalého pracovního režimu zvaného Home Office.

2.1.2 Nevýhody

Ty vyplývají hlavně z otázky bezpečnosti. V zásadě jde o to, že nejsou tato zařízení pod odbornou a jednotnou správou. Tudíž je primárním cílem nástrojů na jejich řízení právě eliminace této nevýhody. Jak již bylo řečeno v úvodu této kapitoly, zásadními problémy rizikovosti těchto zařízení jsou jejich neuvědomělí uživatelé, škodlivý software, ale i platformová různorodost. Převážně z tohoto důvodu je nutné poskytovat firemní služby a přístupy tak, aby byly použitelné pro různé platformy. Místo toho aby byly odladěny pro jednu platformu, kumulují se zde slabiny a rizika mnoha platforem, jelikož každá z nich může používat jiné metody zabezpečení nebo například používané porty. Zásadní bezpečnostní slabinou je tzv. rootování/jailbreak. Takováto zařízení jsou náchylná na instalaci malware mnohem více než jejich neodblokovaní bratříčkové.

Rootování – Root, je u OS Android označení pro systémového superuživatele s nejvyššími oprávněními. Běžné aplikace, které uživatel používá nebo instaluje, si vystačí s běžnými user oprávněními. Aby bylo možné získat větší kontrolu nad systémem nebo instalovat aplikace vyžadující přístup k systémovým souborům, je nutné získat oprávnění root. Od názvu tohoto superuživatele pochází pojmenování k odblokování ochrany systému. Tímto se ale vystavují taková zařízení mnohem většímu riziku poškození a to nejen neodborným zásahem do systémových složek a souborů, ale i poskytnutím těchto oprávnění procesům a aplikacím běžícím na pozadí. Těmi mohou být právě různé škodlivé kódy instalované ať už s či bez vědomí uživatelů ICT.

Jailbreak – odemknutí Apple zařízení s operačním systémem iOS. Obdoba rootování. Provedením jailbreak se získá přístup k souborovému systému, možnost provádět různé tweaky a instalovat aplikace, které nebyly schváleny vývojářskými podmínkami Apple. Různé modely iPhone a iPad mají blokované některé funkce z důvodu cenové politiky. Tímto způsobem řeší uživatelé jejich zpřístupnění.

Oba případy znamenají porušení obchodních podmínek, což znamená, že v případě poruchy nebude uznána reklamace. I přesto se těší mezi uživateli velké oblibě, hlavně z důvodu širších možností instalace cracknutých aplikací a personálního nastavení. Nutno také dodat, že bez privilegovaných oprávnění není možné používat některé užitečné a legální programy. Jde především o FW, zálohovací nástroje, antivirové SW, atd.

Přínosy a rizika vyplývající z používání soukromých zařízení v zásadě kopírují popsané výhody a nevýhody. I problematiky neznalému čtenáři tedy bude jasné, že veškerá technická bezpečnostní opatření se musí řešit na straně zaměstnavatele, což znamená na straně jeho serverů a vstupních přístupových bran.

2.2 Licencování

Samostatnou kapitolou této problematiky je licencování použitého SW. Zde neexistuje jednoznačný návod či řešení. Vycházet se musí především z licenčních podmínek jednotlivých SW. Následně je možné rozhodnout, jakou formou bude SW instalován a kdo bude brát na sebe povinnost jeho legalizace. V zásadě existují dvě základní formy

vlastnictví. Firemní a privátní. Z nich lze následně vybrat vhodnou metodu financování, což představuje převzetí veškerých ekonomických nákladů jednou stranou nebo jejich sdílení. Přijatelnou metodou je též pronájem licencí. Takové rozhodnutí vychází převážně z charakteru používaného SW, kdy je nutné zvážit, zda bude využíván jen pro pracovní činnosti nebo jeho možností může vlastník zařízení využít i pro soukromé účely. V případě využití mobilních zařízení pouze jako prostředku zajišťujícího síťovou konektivitu nám tyto starosti odpadají. V tomto případě jsou veškeré firemní aplikace nainstalované na firemním HW, obvykle serveru. Vhodným terminálovým řešením, například Citrix, se pak propagují pro vzdálené použití.

2.3 Právní aspekty

Z pohledu práva je pro organizaci situace obdobná jako v případě firemních zařízení. Právo na ochranu a kontrolu dat a firemních prostředků zůstává organizaci neodepřeno. Horší je to již s prosazením tohoto práva. Tato situace vyplývá s majetnického práva k zařízení, které v tomto případě je na straně uživatele. Veškeré právní možnosti se tedy omezují na soubory vnitřních opatření, které musí majitel mobilního zařízení respektovat a dodržovat, chce-li pro přístup k firemní infrastruktuře využít svého soukromého zařízení. Ve své podstatě jde o model „buď anebo“. To znamená, že majitel zařízení dá jisté možnosti kontroly jeho zařízení nebo mu nebude služba na jeho soukromém zařízení zpřístupněna. Jde tedy o svobodnou vůli majitele rozhodnout se, zda podmínky přijme či nikoliv. Obrovskou výhodou pro majitele zařízení je, že nikdo nesmí přistupovat k jeho privátním informacím na tomto zařízení, ani jeho majiteli v přístupu k nim bránit. Pokud nedodrží firemní podmínky, dojde pouze k odpojení jeho zařízení od poskytované firemní služby.

Z těchto důvodů není vhodné umožnit používat soukromá zařízení pro přístup k zákonem chráněným informacím, jelikož bychom se tak mohli dostat do střetu zájmu se zákonem, který podmínky pro jejich zpracování upravuje. Z pohledu legislativy České republiky se jedná o zákon na ochranu osobních údajů, zákon 101/2000sb [2], a zákon na ochranu utajovaných informací [3].

2.4 Způsoby ochrany firemních dat

Jelikož existuje mnoho důvodů pro i proti použití soukromých zařízení pro firemní účely bude v této kapitole popsáno jak zařídit, aby se tato zařízení mohla používat a přitom eliminovat existující rizika.

Kromě metod uvedených v kapitole I. jsou to softwarově technická řešení vyvinutá speciálně pro tyto účely. Využít se mohou samozřejmě i pro firemní zařízení. Principem těchto řešení je detekce jejich stavu, dostat zařízení alespoň pod částečnou kontrolu a řízený přístup k jednotlivým službám nebo segmentům sítě. V odborném světě se pro tato řešení zavedla a ustálila pojmenování, která vychází z anglických slov.

- BYOD (Bring Your Own Device)
- MDM (Mobile Device Management)

Při zavádění těchto řešení, která také nejsou levná a kromě investic do HW, SW a licencí vyžadují nemalé náklady v podobě lidských zdrojů pro jejich zavedení a správu, je vždy nutné dobře zvážit výhodnost nejen této investice, ale celkově i schválení režimu použití soukromých zařízení. Při analýze se musí brát v úvahu nejen ekonomické dopady, ale i technické možnosti moderních zařízení, výhody pro zaměstnance, jejich produktivitu, hodnotu chráněných aktiv a v neposlední řadě i podmínky legislativní.

2.4.1 MDM

Jde o souhrnné označení produktů, které si kladou za cíl vzdáleně kontrolovat, spravovat a nastavovat mobilní zařízení. Účelem je zajistit bezpečnost jak samotných zařízení, tak bezpečnost dat a aplikací, ke kterým se z těchto zařízení ve firemní infrastruktuře přistupuje. Na trhu existuje mnoho komerčních i free SW, které spadají do kategorie MDM. V případě firemního nasazení si před výběrem správného řešení musí administrátor položit dvě základní otázky:

- Budou se spravovat pouze firemní zařízení nebo i privátní?
- Bude se podporovat pouze jedna mobilní platforma nebo bude vyžadována její nezávislost?

Odpovědi na tyto dvě klíčové otázky pomohou zúžit seznam produktů, mezi kterými lze vybírat to nejvhodnější řešení. Otázka ceny je jistě také důležitá, ale většina produktů existuje ve více licenčních modelech, od free (zdarma, obvykle s omezenými

funkcionalitami), přes subscription (časově omezená licence) až po perpetual (neomezená licence). Často je také možné vybrat si a zaplatit pouze ty moduly pro daný produkt, které jsou pro konkrétní firmu a požadovaný účel zajímavé. Z tohoto důvodu není vhodné brát finanční aspekt jako primární při výběru. Mnohem důležitější budou možnosti správy, nabízené podpory a množství podporovaných platforem. Obzvláště poslední podmínka je velmi důležitá, pokud se firma rozhodne zavést do firemní politiky i podporu soukromých zařízení. V takovém případě se již těžko podaří prosadit jednotnou platformu. Pokud se omezí výběr na některé přední řešení na trhu, kromě jiných funkcionalit zcela jistě bude umět i tyto:

- Detekce jailbreak/rootování
- Provedení automatických úloh na základě zjištěných skutečností, například u detekovaného rootování/jailbreak
- Oddělení osobních a firemních dat a aplikací
- Vzdálené zamknutí zařízení
- Vzdálené smazání zařízení nebo jen selektivních dat
- Management připojených zařízení a uživatelů
- Široké možnosti statistik a reportů
- Vzdálené nastavení poštovních klientů, správa emailových příloh
- Vzdálená správa profilů VPN, WiFi, certifikátů, atd.
- Distribuce aplikací
- V případě porušení bezpečnostních pravidel na mobilním zařízení blokování připojení k firemním službám (pošta, APP, atd.)
- Podpora black/white listu aplikací v zařízení
- Vynucení bezpečnostních pravidel (hesla, odemknutí, atd.)
- Řízení přístupu ke sdíleným dokumentům a souborům, přístup na SharePoint server
- Lokace zařízení
- Podpora integrace s firemní CA

Podporovaných funkcí je skutečně mnoho. A rozhodně se nejedná o úplný seznam. Každý produkt má nějaké to svoje „něco navíc“. Každý produkt přistupuje ke správě z jiného pohledu. Některé z pohledu uživatele, některé z pohledu zařízení. Je pouze na každém správci vybrat si to, které mu bude vyhovovat nejlépe. Vždy však, ale musí mít na paměti, že možnosti vzdálené správy a podpory vycházejí z možností podporovaných

platforem. Proto se může stát, že některé funkcionality budou dostupné pouze pro některé platformy či typy telefonů dle verze jejich OS.

Výhody a nevýhody vyplývající ze zavedení MDM lze shrnout do těchto bodů:

- **Nevýhody**
  - Investice
  - Nutnost instalace klienta na zařízení
- **Výhody**
  - Vzdálená správa nastavení
  - Vzdálená správa aplikací
  - Centrální management
  - Bezpečnost
  - Řízený přístup k dokumentům
  - Reporting a diagnostika

Mezi renomované produkty na trhu se v současné době řadí MobileIron, AirWatch, Blackberry Enterprise Services, a jiné.

2.4.2 BYOD

Toto označení definuje režim, který umožnuje díky firemní politice a strategii používat zaměstnancům svoje vlastní zařízení. Reprezentuje tedy soubor opatření a produktů pro jejich správu, což může být právě i některý produkt z kategorie MDM, ale i produkty a řešení pro řízený přístup do firemní infrastruktury, včetně interních předpisů a jiných opatření. Na rozdíl od MDM, který se orientuje pouze na zajištění určité míry kontroly nad mobilními zařízeními a poskytnutí vybraných firemních služeb obvykle při práci v terénu, jde v případě BYOD o možnost připojení a používání soukromých zařízení a to i při práci uvnitř firmy. To znamená, že se nemusí jednat pouze o mobilní telefony či tablety, ale i o notebooky, desktopová PC či dokonce své vlastní tiskárny nebo WiFi router. Jde o dobový trend a tak informatici ve firemní sféře stojí před nelehkým úkolem, kterým je bezpečnost firemních dat. Pokrok se dá těžko zastavit, a tak pokud má být firma moderní a dynamická, musí zaměstnávat především mladé lidi, kteří jsou převážně iniciátory těchto požadavků na

používání vlastních zařízení, které jim přináší mnoho výhod. A i zde platí, že než plavat proti proudu, vyplatí se využít jeho síly a nést se na jeho vlnách. Proto, pokud to je z pohledu bezpečnosti přijatelné a existují ve firmě vhodné podmínky, je lepší využít výhod, které tento trend přináší než bránit pokroku a raději převzít nad tím kontrolu. To však znamená pro informatiky nové výzvy a přizpůsobení se nejen svým uvažováním, ale i zavedením potřebných opatření.

O MDM již bylo napsáno. Ale toto v mnoha případech nestačí. U BYOD se musí začít od podlahy. To vyžaduje revizi bezpečnostních standardů a změnu filozofie v řízení rizik plynoucích ze správy dat a ochrany zařízení a řídících procesů. Znamená to začít od interních směrnic, přes režimová opatření až po výběr sofistikovaných technických řešení, která minimalizují rizika a umožní bezpečné používání soukromých zařízení a připojení na firemní aplikace a data. Takovými řešeními mohou být například seznamy povolených MAC adres, zavedení terminálových služeb, virtualizovaných řešení jako například VMWare, až po zavedení rozšířených možností sítových prvků jako je Cisco Unified Access nebo Cisco ISE (Cisco Identity Service Engine), který umožňuje self-provisioning zařízení a integraci pravidel s řešením MDM. Tato řešení umožnují soukromá zařízení nejen detekovat a diagnostikovat, ale i dle nastavených pravidel je pouštět do konkrétních segmentů sítě nebo k poskytovaným službám.

- **Výhody**
    - Atraktivita firmy pro nové ale i stávající zaměstnance
    - Vyšší flexibilita a mobilita
    - Vyšší efektivita zaměstnanců
    - Snížení nákladů na nákup a servis prostředků ICT
- **Nevýhody**
    - Náročnější správa bezpečnostní politiky
    - Náročnější podpora uživatelům (vycházející z nehomogenity platforem)
    - Vyšší riziko úniku firemních dat (vycházející z vlastnických práv majitele zařízení)

3 MOŽNOSTI JEDNOTLIVÝCH OS A MOBILNÍCH PLATFOREM

Pro ucelený přehled nad problematikou zajištění bezpečnosti firemních ICT a elektronických dat je nutné si se podívat na bezpečnost i z pohledu nejznámějších operačních systémů dostupných na trhu.

Jak je to s bezpečností jednotlivých operačních systémů? Každý OS má své příznivce i odpůrce. Objektivně lze prohlásit, že žádný OS není 100% bezpečný. Stejně tak jako má každý OS svou uživatelskou přívětivost či nepřívětivost, své technologické možnosti či omezení, tak i co se týče bezpečnosti má své výhody a nevýhody. Vyplývá to z rozdílného přístupu řešení nejen SW architektury a jádra systému, ale i použitým souborovým systémem a co je nejdůležitější, tak filozofickým přístupem k otázce bezpečnosti. Některé systémy jsou uzavřenější a tím pádem i omezenější. Jiné přistupují k této problematice liberálněji a umožnují tak zákazníkovi sice mnohem flexibilnější možnosti, zato ale obvykle s tím, že větší část odpovědnosti za bezpečnost přenáší na samotné uživatele. Který OS je ten správný není možno jednoznačně říct. Ani to není smyslem této práce. Jde především o to, uvést přehled nejpoužívanějších operačních systémů na trhu a podívat se na ně z pohledu bezpečnosti a ochrany dat a informací. Nastínit nejen jejich technické možnosti ale i základní pravidla bezpečného používání a chování jejich uživatelů.

3.1 Desktopové platformy

Mezi uživateli nejznámější a nejpoužívanější operační systémy, jejich verze a distribuce patří:

- **Windows** – XP, Vista, Windows 7, Windows 8
- **OS X** - 10.6 (Snow Leopard), 10.7 (Lion), 10.8 (Mountain Lion), 10.9 (Mavericks)
- **Linux** – na rozdíl od Windows a OS X, existuje několik distribucí jako například Fedora, Red Hat, Debian, SuSe Linux, atd.

Desktopové systémy jsou na tom s bezpečností podstatně lépe, než jejich mobilní verze. Je to dáno nejen historickým vývojem, ale i jejich robustností. U desktopových OS není problém s velikostí RAM, úložného prostoru, obvykle reprezentovaného interním HDD ani

výpočetním výkonem procesoru. Proto je možné implementovat do OS množství bezpečnostních prvků již od jeho výrobce. Ty bývají u nejnovějších verzí již aktivované alespoň v minimálním defaultním nastavení. Následně je na uživateli, jak se k otázce bezpečnosti postaví. Mnoho funkcí je k dispozici v samotném systému, ale nic nebrání uživateli doinstalovat další bezpečnostní prvky, ať již z free edice nebo zakoupit plnohodnotné verze. Většina uživatelů se omezuje pouze na instalaci antivirového programu a nastavení přístupového hesla. Plnohodnotné operační systémy však nabízí mnohem více a jejich uživatelé by se měli naučit je používat a především se bezpečně chovat.

3.1.1 Zásady bezpečnosti

Jelikož bezpečnost moderních desktopových OS je dostatečná a rizika způsobují spíše samotní uživatelé, je zde uvedeno pár základních rad, kterými by se všichni uživatelé měli řídit. V knize *Zabezpečení systému a sítě* [10] je uvedeno 10 obecných pravidel, která jsou zde rozvedena do praktických rad tak, aby byly pochopeny i běžnými uživateli.

- **Operační systém** – vždy se musí používat legální OS a ideálně jeho poslední verze. Jen tak lze dosáhnout toho, že bude k dispozici podpora výrobce a implementovány nejmodernější bezpečnostní technologie.
- **Aktualizace** - zapomínat se také nesmí na pravidelné aktualizace nejen samotného OS, ale všech ostatních součástí, ať již aplikačních tak hardwarových. Ano, i HW používá ke své funkci nějaký SW, který občas jejich výrobci aktualizují. Získají se tak nejen nové možnosti nastavení, ale i zacelení nalezených slabin. Tomuto SW se říká ovladače, anglicky driver.
- **Antivir/Antispyware** – samotný antivir nestačí. Je nutné ho doplnit o antispyware, pokud již není součástí AV distribuce. I zde platí pravidlo, že musí být aktualizovaný a hlavně spuštěný. Ideálně nakonfigurovaný AV hlídá systém na pozadí a kontroluje všechny otevírané a stahované soubory a navštívené stránky. Proto je důležité vybírat takové produkty, které obsahují webové a emailové doplňky.

- **Personal FW** – u moderních OS bývají již součástí distribuce. Chrání PC před nevyžádanou komunikací. Bývá obvykle dobře odladěný již v defaultním nastavení a tak stačí, pokud ho uživatel ponechá zapnutý.
- **Nevypínat bezpečnostní funkce** – každý OS má implementovány nějaké své funkce, které zajišťují nebo zvyšují jeho bezpečnost. Kdo není odborník, neměl by tyto funkce nejen vypínat, ale ani přenastavovat. Příkladem může být nastavení zabezpečení v internetovém prohlížeči nebo User Account Controll.
- **Aplikace** – neinstalovat SW z neznámých zdrojů a používat jen legální SW. Samozřejmě ho pravidelně aktualizovat a v případě že má nějaká bezpečnostní pravidla, řídit se jeho uživatelskou příručkou.
- **Hesla** – nejběžnější autentizační prvek, který může být „bezpečný“ ale i „zbytečný“. Pro maximální využití jeho možností jsou zde uvedena nejdůležitější pravidla při vytváření a používání hesel.
    - **Používat zásadně silná hesla**
        - nepoužívat známé údaje jako jména, data narození. A to nejen údaje vztahující se k osobě uživatele, ale ani osob jeho blízkých, atd.
        - nepoužívat slovníkové výrazy.
        - Nepoužívat slovníková hesla jako: heslo, password, admin, user, atd.
        - nepoužívat po sobě jdoucí znaky abecedy nebo číslice.
        - Síla hesla vychází z množství a typů znaků, které lze použít a délky hesla. Proto se musí volit hesla, která obsahují malá i velká písmena, číslice a další speciální znaky (!+*/@#$%&,....)
        - Minimální délka hesla je dána složitostí hesla a samozřejmě i podmínkami informačního systému, pro který má být použito a dobou jeho používání. Při použití komplexního hesla stačí 8 znaků. Ideálně 14 znaků.
    - **Používat zapamatovatelná hesla** – těžko zapamatovatelná hesla nutí si je poznamenat, neboť při jejich překlepech hrozí zablokování účtu. Proto je vhodné používat krátké fráze a ještě lépe z důvodu slovníkových útoků znaky z nějaké fráze nebo věty. Například heslo „Mb4j+dj2“ je těžko uhodnutelné,

obsahuje 4 druhy znaků a je lehce zapamatovatelné, jelikož vzniklo z věty „Měla babka 4 jabka a dědoušek jenom 2“

- **Pravidelně hesla měnit** – každé heslo je prolomitelné. Limitujícím faktorem je pouze čas. Pravidelnou změnou hesla, která by měla vycházet z jeho složitosti a délky, se zabrání jejich uhádnutí.
- **Nepoužívat stejná hesla** – pro různé služby a aplikace používat rozdílná hesla. Je možné, že user management v některé aplikaci ukládá hesla v čitelné formě. Dojde-li ke kompromitaci hesla v jedné aplikaci, nemůže ho tak útočník využít i pro ostatní aplikace a služby.
- **Nesdělovat hesla** – nikdy a nikomu! Také otázka jejich evidování je sporná. V případě potřeby používání evidence hesel používat pro tento účel vhodný nástroj, který nám ve své šifrované databázi hesla bezpečně uloží. Stále je však nutno mít na paměti, že takto jsou pak všechna hesla chráněna jedním centrálním, které je použito pro přihlášení do této evidence.
- **Pravidlo obezřetnosti při zadávání autentizačních údajů** – dávat pozor při zadávání hesel. Pozor na průmyslové kamery, keylogery, atd.
- **Další faktory** – bezpečnost hesla je dána také formou jeho uložení v informačním systému a politikou jeho použití. Pokud má správce IS nastaveno pravidlo, že po třech pokusech se účet zablokuje, bude heslo mnohem bezpečnější, než když dáme útočníkovi neomezený počet uhodnutí.

- **Privilegované účty** – nepoužívat zvýšená oprávnění pro běžnou práci. Každý OS má svůj superúčet, ale také je možné přidělit zvýšená oprávnění běžnému uživateli. Tato oprávnění se musí používat pouze v oprávněných případech, jinak existuje riziko, že tato oprávnění využije proces běžící na pozadí bez vědomí uživatele.
- **Šifrovat** – není nutné šifrovat celý systém, i když i tady by se našlo zdůvodnění pro jeho prevenci před resetováním admin účtu při bootování ze speciálního CD. Pokud přístup k PC má pouze uživatel, stačí, když bude šifrován obsah privátních složek nebo soubory. Případně mít heslem chráněný BIOS a v něm omezené bootování pouze na HDD.

- **Zálohovat** – zálohovat a archivovat pravidelně důležité soubory. Brát přitom v úvahu životnost použitých medii.
- **Nepřipojovat PC do neznámých sítí** – v podstatě samotný Internet je jedna velká neznámá síť. Ale konektivita s okolním světem je jedním ze základních předpokladů pro používání PC. Je tedy důležité se vyvarovat alespoň různým nedůvěryhodným torentovým sítím a neznámým providerům hlavně u WiFi.
- **Přístup k PC** – zajistit svůj počítač před použitím nepovolanou osobou. Sdílet PC jen s důvěryhodnými osobami a v případě, že je potřeba od někoho zajistit například odborný servis, nenechat ho u PC bez dozoru nebo z PC nenávratně odstranit citlivá data a po jeho vrácení přenastavit všechna hesla a PC zkontrolovat na přítomnost malware. Používat funkce automatického zamykání v případě nečinnosti
- **Pošta** – neotvírat neznámé přílohy nebo přílohy z nevyžádané pošty. Nespouštět odkazy na webové stránky z nevyžádaných emailů a ani na nevyžádanou poštu odpovídat (tím se jen potvrdí platnost emailové adresy, která se tak dostane na spamový list). Ideálně evidentní spam bez otevření rovnou smazat. Pamatovat, že i odesílatel může být podvržený, tudíž nesdělovat přes email žádné citlivé údaje. Může se jednat o tzv. Phishing.
- **Sociální sítě** – mít na paměti, že internet je anonymním místem s anonymními uživateli. Nikdo si nemůže být jist, že ten s kým komunikuje, je skutečně ten, za koho se vydává a kdo všechno odposlouchává komunikaci. Tudíž neuvádět na internetu žádné osobní a citlivé údaje s výjimkou vyplnění formulářů na zabezpečených stránkách, například u bank a státních úřadů.
- **Nenavštěvovat problémové webové stránky** – vyvarovat se stránkám s tématikou porna, násilí, warez, atd. Bývají zdrojem škodlivého kódu.
- **Věnovat pozornost zobrazeným informacím** –informativní hlášky zobrazují důležité informace, které mohou mít dopad na bezpečnost PC. Často jsou však nepozornými uživateli přehlédnuty nebo s nezájmem „odkliknuty“. Čtěte pozorně vše, co se vám na displeji zobrazuje!
- **Nestahovat neznámé soubory** – obzvláště spustitelné soubory (exe, atd.), ale v poslední době je možné šířit škodlivý kód i zabalený uvnitř dokumentů

a multimediálních souborů. Každý stažený soubor nechat prověřit antivirovou/antispyware kontrolou.

- **Zajímat se o bezpečnost** – vědomostí není nikdy dost. Vždyť hackeři zakládají svoje útoky (a mnohdy úspěšně) právě na lidské neznalosti a důvěřivosti.
- **Neznámé a veřejné PC** - (např. internetové kavárny) vyvarovat se jejich používání a není-li to nezbytné, nepoužívat je pro přístup k osobním stránkám, firemním informacím, bankovním účtům. Zadávání osobních nebo autentizačních údajů na těchto strojích je rizikové z důvodu jejich odposlechnutí, například pomocí keylogeru.
- **Přenosná media** – počítač není jen zařízení, na kterém se pracuje, ale vše co je k němu připojeno. Právě cizí zdroje mohou být potencionálním zdrojem zanesení škodlivého kódu. Ani vlastní přenosná zařízení nejsou bezpečná, pokud jsou připojena k jiným PC. Proto se musí dbát i na jejich bezpečnost. Díky jejich rozměrům a přenositelnosti také na bezpečné uložení a pravidelnou antivirovou kontrolu.
- **Funkce „pamatovat heslo“** – tuto funkci, ať je sebevíce užitečná a příjemná, nikdy nepoužívat.
- **Smazané soubory lze obnovit** – málo známá věc mezi běžnými uživateli. Pro mazání používat proto pouze sofistikované nástroje. To platí hlavně v případě, když dochází k výměně datového úložiště nebo se starého PC zbavujete.
- **Elektronický podpis** – používat pro bezpečnou emailovou korespondenci. Používat certifikáty podepsané pouze důvěryhodnými Certifikačními Autoritami a nezapomínat revokovat nepoužívané certifikáty.
- **Používat bezpečné protokoly** – většina používaných protokolů existuje i v jejich zabezpečené verzi. Obvykle se to pozná podle písmene „S“ na konci jejich zkratky. Například, HTTPS, FTPS. Nikdy pří práci v jakékoliv síti nezadávat autentizační, osobní a citlivé údaje na stránkách přístupné z nezabezpečených protokolů!
- **Osobní odpovědnost** – mít na paměti, že žádný technický prvek nezajistí bezpečnost bez odpovědného uživatelského přístupu. Každý si musí uvědomit, že jde o jeho bezpečnost. Počítač se po napadení dá vyléčit, případně přeinstalovat, ale

zcizená data již nikdo nevrátí a mohou tak být způsobeny i materiální škody, například odcizením hotovosti z bankovního účtu.

3.2 Mobilní platformy

Mezi nejznámější výrobce mobilních platforem patří firmy, Apple, Microsoft a Google. Samozřejmě existuje od každého výrobce již mnoho verzí, které sice mohou být ještě hojně rozšířeny, ale z důvodu jejich postupného opouštění a jednoduššího porovnání budou brány v úvahu jen jejich poslední verze. Mezi nejnovější verze mobilních platforem výše uvedených výrobců patří:

- **Windows Phone 8.1** – operační systém od firmy Microsoft
- **iOS (7)** – operační systém od firmy Apple
- **Android (4.4)** – operační systém od firmy Google

U mobilních platforem je bezpečnostní situace o poznání horší. Nejen, že jsou tyto systémy mladší, ale i konstrukce a cena mají nepříznivý vliv na robustnost celého systému. Na konstrukci je v nemalé míře závislý HW výkon a velikost baterie. A protože jsou mobilní zařízení z podstaty věci menší, je logické, že v nich bude menší i baterie, paměť a úložný prostor. Mobilní zařízení je také možné mnohem lépe ztratit či odcizit. Proto již jen z tohoto důvodu jsou náchylnější na možnost, že se k citlivým informacím nebo vzdálenému firemnímu připojení dostane nepovolaná osoba. Právě proto, že jsou snadno ztratitelné, nechtějí běžní uživatelé do nich investovat velké částky peněz. A tak, aby výrobci snížili ceny na minimum, osazují je méně výkonnými komponentami. Toto všechno se samozřejmě musí projevit na velikosti samotného systému, který tak musí být co nejmenší a musí mít co nejnižší energetické nároky. Je-li vzato v úvahu, že výrobci se nechtějí z důvodu konkurenčního boje omezovat na grafickém prostředí, musí se tak sáhnout k některým funkčním omezením. To však běžní uživatelé nevnímají. Pro ně je to přece „jenom telefon“. V každém případě by i při používání těchto mobilních platforem měli ctít stejná pravidla bezpečnosti jako u desktopových verzí a dbát i opatrnosti při jejich nošení.

Naštěstí, hlavně proto, aby výrobci udrželi v rámci konkurenčního boje tato zařízení i v korporátní sféře, musí zajistit určité bezpečnostní minimum. Organizace při používání dbají na určitou bezpečnost přece jenom více, než běžní uživatelé. V následující kapitole

budou popsány jejich bezpečnostní prvky a v závěru kapitoly porovnány jednotlivé platformy.

3.2.1 Bezpečnostní prvky

Níže uvedené bezpečnostní prvky využívají v jisté míře všechny tři mobilní platformy [13].

- **Bezpečný start systému -** neporušenost všech systémových komponent při bootování OS je zajištěna elektronickým podpisem. V paměti ROM je uložen veřejný klíč CA, kterým se ověří pravost komponent.
- **Podepsání zdrojového kódu aplikací -** veškeré aplikace, které lze nainstalovat do těchto zařízení, musí pocházet z centrálního distribučního kanálu, který zajišťuje, že všechny vystavené aplikace jsou podepsány elektronickým podpisem daného vývojáře. Na tomto místě je dobré si připomenout, že právě k obcházení této kontroly se používá rootování/jailbreak.
- **Centrální distribuční kanál -** je místo, odkud je možné stahovat do mobilních zařízení aplikace. Tento obchodně aplikační portál s platební bránou se stará nejen o distribuci a automatické aktualizace, ale díky nastaveným pravidlům a procesům jsou na něm vystavovány jen prověřené aplikace od zaregistrovaných vývojářů. Každá mobilní OS používá svůj. Apple – Apple Store, Android – Google Play, Microsoft – WP store.
- **Izolace aplikací -** aplikace třetích stran mají vyhrazený diskový prostor, API a paměť, které smí při komunikaci s OS využívat. Ostatní části systému jsou znepřístupněny díky spouštění aplikaci s neprivilegovanými oprávněními. I pro obcházení této ochrany se používá rootování/jailbreak. U iOS jsou dokonce od sebe odděleny i jednotlivé aplikace a jejich data. Tomuto principu se říká sandbox (pískoviště).
- **Bezpečnost běžících procesů -** sem patří Address Space Layout Randomization, Execute Never, Data Execution Prevention. Tyto mechanismy se zaměřují na ochranu dat a aplikací uložených v paměti zařízení.

- **Vzdálená správa -** Pro bezpečnost je důležitý rozsah politik, které je možné na jednotlivých platformách vzdáleně nastavit. Ať již přes protokol ActiveSync nebo přes nástroje třetích stran, MDM.
- **Šifrování -** Šifrování uložených dat sice zpomaluje rychlost systému, ale jde o jedno z nejúčinnějších opatření proti neoprávněnému přístupu.
- **Zamykání obrazovky -** Jelikož se jedná převážně o telefony, které musí být stále v pohotovosti, jsou systémy vybaveny možností zamykat obrazovku spuštěného systému. Obvykle jsou vybaveny více možnostmi. Od biometrických senzorů, přes klasické PIN až po gesta. Oblíbená mezi uživateli jsou právě poslední zmíněná gesta, která však patří mezi nejméně bezpečná. Nepovolaná osoba může zjistit potřebný tah ze šmouh na displeji.
- **Další možnosti -** Spočívají převážně z instalace nástrojů třetích stran. Jde především o různé personální FireWall, antiviry, antispyware, antitheft nástroje založené především na lokaci zařízení, případně jeho vzdáleném promazání. Využití těchto bezpečnostních prvků je již volbou uživatele.

3.2.2 Porovnání produktů předních výrobců

V řízení přístupů k jednotlivým aplikacím a jejich datům jednoznačně vede iOS. I když to někdy komplikuje práci se soubory, jde o velmi účinnou ochranu bránící škodlivým kódům dostat se k datům jiných aplikací. I na poli vzdáleného řízení politik má navrch iOS před Androidem [14]. Ten umožňuje více méně jen nastavení politiky hesla, jeho vynucení, uzamykat zařízení nebo ho vzdáleně smazat. iOS umožnuje mnohem více, například blokování fotoaparátu, zakázaní screenshotů, nepovolit instalaci nových aplikací, zakázat vybrané aplikace a další možnosti správy a sledování chování. Co se týče šifrování, tak u iOS a Windows Phone 8 je nastaveno defaultně. Android šifrování podporuje také, ale jeho použití nechává na benevolenci uživatele. Stejně tak umožňuje Android i instalaci z neznámých zdrojů. Toto si musí uživatel v nastavení systému přes GUI povolit. To, že všichni zmiňovaní výrobci mobilních OS podporují výše zmíněné bezpečnostní funkce ještě neznamená, že bezpečnost je u všech mobilních OS stejná. Důvodem nejsou jen drobné rozdíly v jejich implementaci a například v přísnosti kontroly při vystavování aplikací do prodejních portálů, ale například i množství virů a Spyware, které se pro dané

platformy šíří. Statistiky antivirových společností uvádějí, že nejvíce je ohrožena platforma Android. V neposlední řadě je bezpečnost jednotlivých platforem také hodně ovlivněna procentuálním zastoupením dané platformy na světovém trhu. Je logické, že mobilní OS, jež má na světovém trhu 2% podíl, nebude pro „záškodníky" tak lákavý jako ten, který je instalován na 70% zařízení ve světě. To už je úděl popularity, ve které momentálně vítězí Android.

Top Four Operating Systems, Shipments, and Market Share, Q3 2013 (Units in Millions)

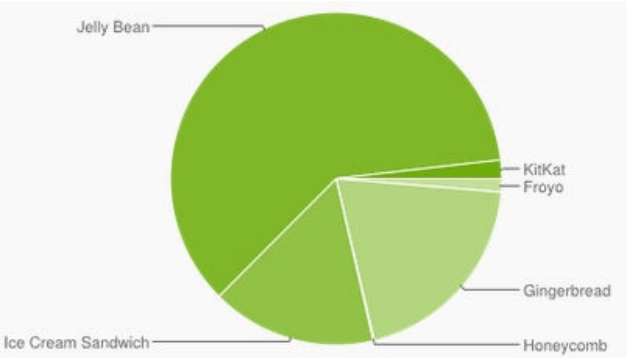
Operating System	3Q13 Shipment Volumes	3Q13 Market Share	3Q12 Shipment Volumes	3Q12 Market Share	Year-Over-Year Change
Android	211.6	81.0%	139.9	74.9%	51.3%
iOS	33.8	12.9%	26.9	14.4%	25.6%
Windows Phone	9.5	3.6%	3.7	2.0%	156.0%
BlackBerry	4.5	1.7%	7.7	4.1%	-41.6%
Others	1.7	0.6%	8.4	4.5%	-80.1%
Total	**261.1**	**100.0%**	**186.7**	**100.0%**	**39.9%**

Obrázek 1. Mobilní platformy, podíl na trhu.

(Zdroj: http://smartmania.cz/clanky/idc-android-prekonal-80-trzni-podil-jak-se-darilo-ostatnim-platformam-6179)

Na základě všech dostupných informací se zdá, že nejbezpečnější platformu pro korporátní používání má v současné době Apple. Největší oblíbenost mezi uživateli ale zase vykazuje Android. Tudíž bude opět na informaticích, aby v případě BYOD nespoléhali pouze na bezpečnost jednotlivých platforem a odpovědnost jejich uživatelů, ale zavedli vhodná opatření pro zajištění bezpečnosti firemních dat. Situaci ještě komplikuje fakt, že mnoho zařízení dnes ještě používá staré verze Android, kterým chybí některé bezpečnostní funkce a nepodporují připojení na MDM.

Version	Codename	API	Distribution
2.2	Froyo	8	1.3%
2.3.3 - 2.3.7	Gingerbread	10	20.0%
3.2	Honeycomb	13	0.1%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	16.1%
4.1.x	Jelly Bean	16	35.5%
4.2.x		17	16.3%
4.3		18	8.9%
4.4	KitKat	19	1.8%



Obrázek 2. Podíl jednotlivých verzí Android na zařízeních

(Zdroj: http://www.androidmarket.cz/ruzne/google-statistika-podilu-verzi-androidu-v-unoru-2014/)

II. PRAKTICKÁ ČÁST

4 NÁVRH INTERNÍCH SMĚRNIC

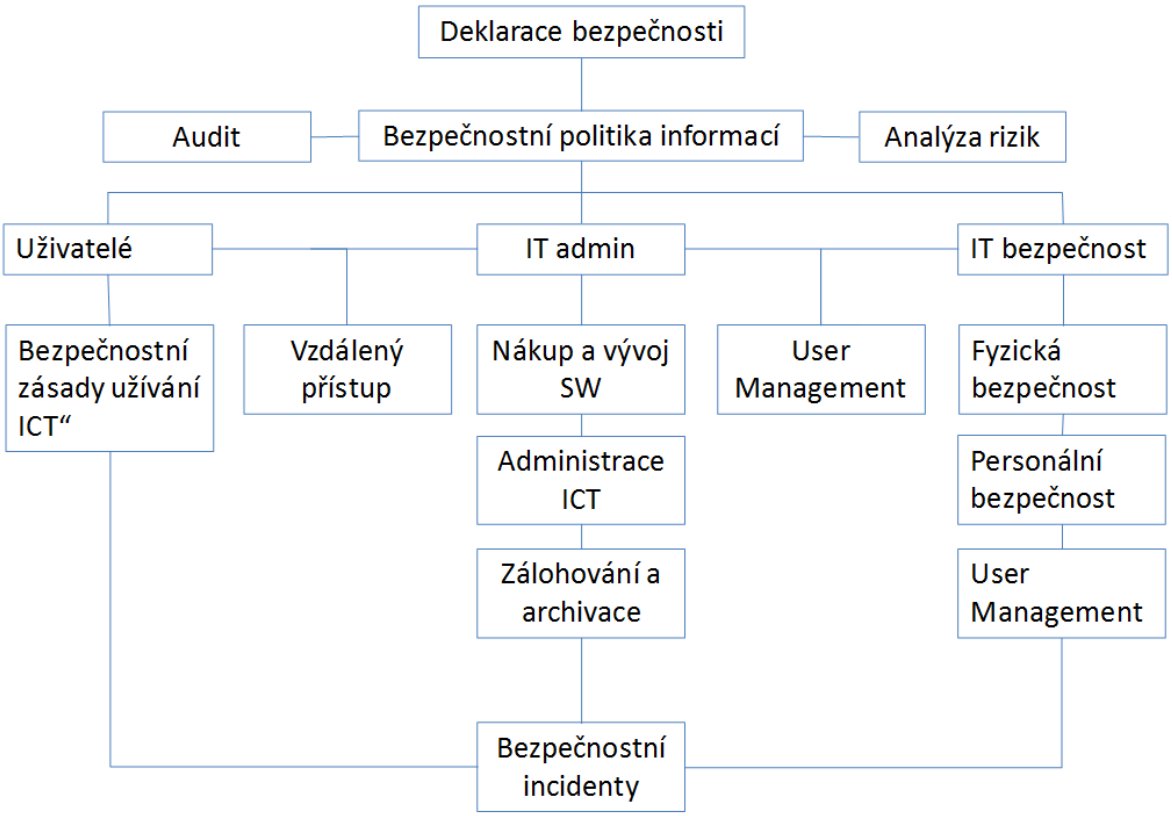
V každé organizaci musí být vypracován soubor interních dokumentů pro zajištění bezpečnosti ICT a informací. Vhodné je vytvořit hierarchii dokumentů na tři úrovně podle toho, pro kterou skupinu zaměstnanců jsou určeny.

- **Vedení/představenstvo – „Deklarace bezpečnosti“**
  Tento dokument je jistým závazkem společnosti, že si přeje a bude podporovat zavedení systému řízení bezpečnosti a vyhradí k tomuto účelu potřebné prostředky
- **Manažer IT bezpečnosti – „Bezpečnostní politika informací“**
  V tomto dokumentu jsou rozpracovány základní oblasti, včetně základních zásad, které musí být v organizaci řešeny s ohledem na bezpečnost ICT a informací.
- **Zaměstnanci - směrnice pro administrátory, uživatele,**
  které rozpracovávají jednotlivé oblasti provozovaných ICT do konkrétních opatření a nařízení. Jsou v nich uvedena všechna potřebná opatření tak, aby bylo v provozu dosaženo souladu s dokumentem „Bezpečnostní politika informací“

V příloze bakalářské práce jsou navrženy texty pro každou úroveň.

- **Příloha 1.** Návrh textu pro dokument „Deklarace bezpečnosti informací“
- **Příloha 2.** Šablona, která může být použita při vytváření dokumentu „Bezpečnostní politika informací“ kterékoliv firmy. Text je navržen tak, aby pokrýval všechny oblasti a opatření uvedené v normě ČSN ISO/IEC 27001 [9] a mohl se tak stát ústředním interním předpisem při řízení bezpečnosti firmy s ohledem na případnou budoucí certifikaci.

  V praxi je nutno vybrat do dokumentu „Bezpečnostní politika informací“ z této univerzální šablony pouze ty body a opatření, které jsou relevantní k charakteru zpracovávaných dat a provozovaných IT služeb. Při jeho vytváření se musí brát v úvahu potřeby organizace, možnosti organizace a výsledný text musí reflektovat legislativní požadavky v době vytvoření a použití.
- **Příloha 3.** Návrh obsahu interní směrnice pro zaměstnance „Bezpečnostní zásady užívání ICT“ (kapitola 4.3)



Obrázek 3. Návrh struktury interních směrnic (zdroj: autor)

Návrhy dokumentů byly vypracovány ze zkušeností autora a byly doplněny z dalších zdrojů [2, 3, 9]

ZÁVĚR

Jak je vidět z obsahu této práce, bezpečnost a ochrana firemním dat je problematika velice rozsáhlá a pro odpovědné osoby velice nelehká. Větší firmy a instituce nebo organizace, které zpracovávají osobní data, jež jsou chráněna zákonem, mají pro tyto účely zřízeny samostatné pracovní pozice nebo dokonce celá oddělení. Jejich úkolem je převážně definovat procesy a interní pravidla a dohlížet na jejich dodržování. Na IT oddělení je, aby při zajištění provozu firemní ICT bralo v úvahu i tato kritéria, podmínky a omezení. Důležité je, aby IT bezpečnost byla součástí celého procesu od výběru, přes konfiguraci, až po bezpečnou likvidaci při ukončení životnosti ICT.

V menších firmách tuto roli obvykle bere na svou odpovědnost samotný administrátor/správce sítě, v ideálním případě s podporou svého zaměstnavatele.

V těch nejmenších firmách, u živnostníků, osob samostatně výdělečně činných, atd., je zvykem, že si svoji techniku spravuje obvykle sám majitel nebo jím pověřená outsourcingová firma. Nemusí to být vždy pravda, ale praxe ukazuje, že s klesající velikostí firmy se snižuje i její odpovědný přístup k ochraně jejich dat. Svým způsobem je to pochopitelné. Každá činnost něco stojí. Nejinak je tomu i u bezpečnosti. Investice do specialistů a technických řešení jsou nemalé a projeví se v ceně produktu nebo poskytovaných služeb.

Ať už se jedná o malou či velkou firmu, vždy je nutné brát v úvahu ekonomické hledisko. Cena za bezpečnost nikdy nesmí převýšit cenu chráněných informací a dat. Proto je důležité najít vhodné kompromisní řešení, které bude na jednu stranu efektivní, na straně druhé splňovat požadavky legislativní a provozní.

Informační a komunikační technologie se staly běžnou součástí soukromého a pracovního života. Rozmach ICT jde ruku v ruce s její klesající cenou a bez sítových služeb a přístupu k Internetu si už dnes ani svůj život nelze představit. S rozmachem mobilních prostředků se ale rozmáhá i další společenský nešvar, a to kyberterorismus. Jeho rozmach a množství forem nám jasně dávají najevo, že bezpečnost a ochrana dat, ať již soukromých či korporátních nabývá na významu a důležitosti.

V této práci se podařilo definovat základní problémy v ochraně firemních dat, které přináší používání soukromých zařízení, stejně tak i používání firemních zařízení pro

soukromé účely. K řešení této problematiky byly uvedeny existující možnosti jak technického tak i režimového a legislativního charakteru. Byla uvedena bezpečnostní opatření, kterými jsou opatřeny operační systémy pro mobilní platformu a sepsána základní pravidla pro bezpečné používání prostředků ICT s ohledem na zachování důvěrnosti, integrity a dostupnosti firemních dat. V praktické části jsou navrženy vzorové texty a šablony pro vytváření interních směrnic.

Na závěr dvě základní a praxí osvědčená pravidla.

1) **Žádné technické opatření nezajistí ochranu a bezpečnost informací a dat bez odpovědného přístupu jejich majitelů a uživatelů.**
2) **Bezpečnost je jako řetěz. Přetrhne se v místě nejslabšího článku.**

SEZNAM POUŽITÉ LITERATURY

[1] MCCLURE, Stuart. Hacking bez tajemství. 3. aktualiz. vyd. Brno: Computer Press, 2003, XXIV, 612 s. ISBN 80-722-6948-8.

[2] Zákon 101/2000 Sb. ze dne 4. dubna 2000, Zákon o ochraně osobních údajů

[3] Zákon 412/2005 Sb. ze dne 21. září 2005, Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti

[4] Zákon č. 262/2006 sb. ze dne 21. dubna 2006, Zákoník práce, Část třináctá: společná ustanovení, Hlava VIII: ochrana majetkových zájmů zaměstnavatele a ochrana osobních práv zaměstnance, § 316

[5] Zákon č. 262/2006 sb. ze dne 21. dubna 2006, Zákoník práce, Část třináctá: společná ustanovení, Hlava II: základní povinnosti zaměstnanců a vedoucích zaměstnanců vyplývající z pracovního poměru nebo dohod o pracích konaných mimo pracovní poměr, jiné povinnosti zaměstnanců, zvláštní povinnosti některých zaměstnanců a výkon jiné výdělečné činnosti, § 301

[6] Zákon č. 262/2006 sb. ze dne 21. dubna 2006, Zákoník práce, Část třináctá: společná ustanovení, Hlava VIII: ochrana majetkových zájmů zaměstnavatele a ochrana osobních práv zaměstnance, § 302

[7] Zákon č. 40/2009 Sb. ze dne 8. ledna 2009, Trestní zákoník, Část druhá: zvláštní část, Hlava V: Trestné činy proti majetku, § 220 Porušení povinnosti při správě cizího majetku

[8] Zákon č. 513/1991 Sb. ze dne 5. listopadu 1991, Obchodní zákoník, Část první: všeobecná ustanovení, Hlava I: základní ustanovení, Díl V: obchodní tajemství, § 17

[9] ČSN ISO 27001:2006. Systémy managementu bezpečnosti informací – Požadavky, Praha: Český normalizační institut, 2006

[10] SMITH, Ben a Brian KOMAR. Zabezpečení systému a sítě Microsoft Windows. 2. vyd. Brno: Computer Press, 2006, 700 s. ISBN 80-251-1260-8.

[11] DOSTÁLEK, Libor, Marta VOHNOUTOVÁ a Miroslav KNOTEK. Velký průvodce infrastrukturou PKI a technologií elektronického podpisu. 2., aktualiz. vyd. Brno: Computer Press, 542 s. ISBN 978-80-251-2619-6.

[12] STANEK, R. Microsoft Windows Server 2003: kapesní rádce administrátora. 1. vyd. Brno: Computer Press, 2003, 535 s. ISBN 80-722-6839-2.

[13] SKÁLA, Zbyněk. Bezpečnost mobilních platforem. In: *SystemOnLine: S přehledem ve světě informačních technologii* [online]. [cit. 2014-03-23]. Dostupné z: http://www.systemonline.cz/it-security/bezpecnost-mobilnich-platforem.htm

[14] Bezpečnost a správa mobilních zařízení. *BusinessIT* [online]. [cit. 2014-03-23]. Dostupné z: http://www.businessit.cz/cz/bezpecnost-sprava-mobilnich-zarizeni-android-apple-mdm.php

[15] PUŽMANOVÁ, Rita. Bezpečnost bezdrátové komunikace: jak zabezpečit wi-fi, bluetooth, GPRS či 3G. Vyd. 1. Brno: Computer Press, 2005, 179 s. ISBN 80-251-0791-4.

[16] JANSA, Lukáš a Petr OTEVŘEL. Softwarové právo: praktický průvodce právní problematikou v IT. Brno: Computer Press, 2011, 340 s. ISBN 978-80-251-3458-

[17] MEDUNA, Martin. Bezpečnost mobilních zařízení s operačním systémem iOS. In: *SystemOnLine: S přehledem ve světě informačních technologii* [online]. [cit. 2014-03-23]. Dostupné z: http://www.systemonline.cz/it-security/bezpecnost-mobilnich-zarizeni-s-ios.htm

[18] Smartmania.cz: IDC: Android překonal 80% tržní podíl, jak se dařilo ostatním platformám?. PODZIMEK, David. [online]. 13.11.2013. [cit. 2014-03-23]. Dostupné z: http://smartmania.cz/clanky/idc-android-prekonal-80-trzni-podil-jak-se-darilo-ostatnim-platformam-6179

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

APP	Aplikace
BCP	Business Continuity Plan
BIOS	Basic Input-Output System
BYOD	Bring Your Own Devices
CA	Certificate Authotrity
ČNB	Česká národní banka
DB	Databáze
DLP	Data Lost Prevention
DRP	Disaster Recovery Plan
EDGE	Enhanced Data Rates for GSM Evolution
FW	FireWall. Jde o bezpečnostní prvek pro řízení sítového provozu.
GB	GigaByte
GPRS	General Packet Radio Service
GUI	Graphical User Interface
HDD	HardDisk
HTTPS	Nástavba sítového protokolu HTTP, pro šifrovanou komunikaci
HW	Hardware
ICT	Informační a komunikační technologie
IPSEC	Bezpečnostní rozšíření IP protokolu
LAN	Local Area Network
LTO	Linear Tape Open
MAC	Jedinečný identifikátor sítového rozhraní
MD5	Hašovací algoritmus, vytvářející otisk o délce 128 bitů
MDM	Mobile Devices Management
OS	Operační systém

ROM	Read Only Memory
S/MIME	Secure/Multipurpose Internet Mail Extensions
SHA2	Šifrovací algoritmus
SIEM	Security Information and Event Management
SIM	Subscriber Identity Module
SMS	Short Message System
SSH	Secure Shell. Náhrada za Telnet.
SSL	Secure Socket Layer
SW	Software
TLS	Transport Layer Security
UMTS	Universal Mobile Telecommunications System
UooU	Úřad na ochranu osobních údajů
VPN	Virtual Private Network
WAN	Wide Area Network
WiFi	Označení několika standardů IEEE 802.11 popisujících bezdrátovou komunikaci

SEZNAM OBRÁZKŮ

SEZNAM PŘÍLOH

Příloha PI:

DEKLARACE BEZPEČNOSTI

Interní dokument

Vedení společnosti XXX deklaruje následující bezpečnostní politiku informací

Společnost XXX přikládá velký význam zabezpečení informací, které jsou jí svěřeny do péče a se kterými zachází. Vnímá ochranu informací svých i informací svých klientů jako ucelenou a řízenou soustavu vyvážených opatření, jejichž cílem je přiměřeně chránit všechna důležitá aktiva. Prioritní je zejména ochrana osobních dat klientů a zákazníků zpracovávaných společností z hlediska zákona na ochranu osobních údajů. Základním úkolem je zajištění dostupnosti, integrity a důvěrnosti dat. Pro ochranu svých i svěřených informací společnost vybudovala, udržuje a rozvíjí systém řízení bezpečnosti informací ve smyslu ČSN ISO/IEC 27001:2006.

Systém řízení bezpečnosti informací vychází z cílů bezpečnosti informací a dále z určených a ohodnocených rizik. Systém dále zahrnuje určení povinností a odpovědností spolu s vytvořením a dodržováním zdokumentovaných bezpečnostních zásad a postupů. Systém současně stanovuje kritéria hodnocení rizik a zahrnuje kontroly dodržování stanovených pravidel, definici zákonných, regulatorních a smluvních požadavků, vzdělávání pracovníků a postupy pro reakci na bezpečnostní incidenty.

Společnost se zavazuje na základě analýzy rizik plnit bezpečnostní opatření a bezpečnostní požadavky v následujících oblastech:

- **Organizační bezpečnost**, která definuje odpovědnosti a rozsah systému řízení bezpečnosti.
- **Klasifikace a řízení aktiv** určující způsob identifikace a ohodnocení aktiv, způsob klasifikace informací a způsob zacházení s nimi. Oblast postihuje i samotnou „Analýzu rizik“, včetně stanovení její struktury a kritéria hodnocení.
- **Bezpečnost lidských zdrojů**, jejímž cílem je, aby se s důvěrnými informacemi seznamoval pouze pracovník k tomu určený.

- **Fyzická bezpečnost a bezpečnost prostředí** předcházející neautorizovanému přístupu, poškození, znehodnocení, zničení či jiným zásahům do informací společnosti a do prostor, ve kterých se nacházejí zařízení společnosti.
- **Řízení komunikací a řízení provozu**, které stanovuje postupy pro řádný a bezpečný provoz prostředků pro zpracování informací a služeb s tím souvisejících.
- **Řízení přístupu**, které definuje ochranu a kontrolu přístupu k informacím, službám a procesům.
- **Akvizice, vývoj a údržba systémů**, které definuje bezpečnostní pravidla vývoje a údržby systémů od fáze návrhu, vývoje, testování až po vlastní provoz a údržbu.
- **Zvládání bezpečnostních událostí**, které stanovuje postupy reakce na poruchy pravidel, bezpečnosti a odolnosti systému řízení bezpečnosti informací.
- **Řízení kontinuity činností organizace**, které stanovují rámec prevence a reakce na krizové situace formou plnění plánů kontinuity.
- **Zajištění souladu s požadavky**, která rozpracovává konkrétní postupy v oblasti zajištění shody přijímaných opatření s legislativou a bezpečnostními nebo technologickými požadavky.

Společnost trvale zajišťuje, že politika bezpečnosti informací:

- odpovídá záměrům společnosti,
- zahrnuje odpovědnost k plnění požadavků a k neustálému zlepšování efektivnosti systému,
- poskytuje rámec pro stanovení a přezkoumání bezpečnostních cílů,
- je sdělována a pochopena ve společnosti při školeních zaměstnanců,
- je pravidelně přezkoumávána z hlediska kontinuity a vhodnosti.

Představenstvo společnosti tímto dává povolení k zavedení a provozu systému řízení bezpečnosti informací ve společnosti XXX.

…….....

Datum a podpis statutárního zástupce

Příloha II:

BEZPEČNOSTNÍ POLITIKA INFORMACÍ

Interní dokument

1. Účel

Účelem tohoto dokumentu je stanovit základní rámec systému řízení bezpečnosti informací (dále jen „ISMS“). Bezpečnostní politika informací vymezuje základní pravomoci, odpovědnosti a definuje zásady systému řízení bezpečnosti informací společnosti XXX.

Bezpečnostní politika informací popisuje konečný cílový stav systému řízení bezpečnosti informací a popisuje jednotlivé cíle bezpečnosti informací v souladu s normami ČSN ISO/IEC 27001 a 27002. Aplikaci jednotlivých bezpečnostních opatření vybraných na základě analýzy rizik jsou povinni zapracovat do příslušné dokumentace odpovědní zaměstnanci.

2. Rozsah působnosti bezpečnostní politiky informací

2.1 Cíl bezpečnosti informací

Pro zachování důvěrnosti je nutné chránit aktiva proti neautorizovanému vyzrazení. Pro zachování integrity je nutné chránit aktiva před neautorizovanou nebo náhodnou modifikací a zajistit jejich správnost a úplnost. Pro zachování dostupnosti je nutné zabezpečit, aby aktiva byla dostupná v souladu s podnikatelskými cíli vždy, když to je potřebné.

Hlavními bezpečnostními cíli jsou:

- Ochrana informačních aktiv.
- Schopnost zvládání nežádoucích událostí včetně zajištění kontinuity činností.
- Ochrana majetku.

- Prosazování odpovědnosti zaměstnanců při zajišťování bezpečnosti.
- Komplexní přístup k prosazování bezpečnosti ve všech oblastech realizace bezpečnosti.

2.2 Strategie bezpečnosti informací

- Strategie bezpečnosti informací vychází z „Deklarace bezpečnosti informací“ společnosti XXX.
- Bezpečnost informací je chápána jako celek složený z jednotlivých opatření organizační bezpečnosti, zajištění ochrany aktiv, personální a fyzické bezpečnosti a bezpečnosti informačních technologií pro zajištění dostupnosti, integrity a důvěrnosti informací. Základem prosazení bezpečnosti informací je realizace a prosazení systému řízení informací ve všech oblastech bezpečnosti.
- Systém řízení bezpečnosti informací je zaveden v souladu s normou ISO/IEC 27001
- Bezpečnost informací je prosazována v souladu s deklarovaným cílem a strategií a odpovídají za ni na všech úrovních vedoucí zaměstnanci.
- Se zavedeným systémem řízení jsou seznámeni všichni zaměstnanci společnosti.
- K údržbě a zlepšování ISMS jsou prováděny oddělením Interní audit pravidelné audity bezpečnosti informací a jsou přijímána nápravná a preventivní opatření (viz kapitola 6 ČSN ISO/IEC 27001).

3. Odpovědnost za bezpečnost informací

- Představenstvo společnosti XXX odpovídá za stav a řízení bezpečnosti informací.
- Za každodenní řešení problematiky bezpečnosti informací a šetření bezpečnostních incidentů je v rámci společnosti odpovědný bezpečnostní manažer.
- Vedoucí zaměstnanci odpovídají za zavedení a dodržování bezpečnostních opatření a spolupráci při šetření bezpečnostních incidentů u jednotlivých součástí.
- Zaměstnanci odpovídají za dodržování bezpečnostních opatření a ohlášení bezpečnostních událostí.
- Společnost XXX stanoví a realizuje bezpečnostní opatření na základě bezpečnostních požadavků vzešlých z analýzy rizik, provádí klasifikaci.

- Výsledky jsou dokumentovány ve zprávě o analýze rizik, která je předkládána představenstvu (min. 1x/rok) – představenstvo rozhodne o akceptaci rizik.

4. Regulatorní a legislativní požadavky na bezpečnost informací

Systém řízení bezpečnosti informací respektuje legislativní a regulatorní požadavky. Jedná se zejména o zákony ČR (zákon č. 101/2000 Sb., o ochraně osobních údajů ve znění pozdějších předpisů, zákon č. 513/1991 Sb., obchodní zákoník ve znění pozdějších předpisů; zákon č. 262/2006 Sb., zákoník práce ve znění pozdějších předpisů, zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským). Při změně relevantních norem je nutné provést revizi ISMS.

5. Kritéria hodnocení rizik

- Bezpečnostní opatření jsou vybrána na základě metodicky prováděné analýzy rizik, požadavků zákonů, zákonných norem a smluvních požadavků.
- Analýza rizik má za cíl odhadnout ztráty, které mohou vzniknout působením hrozeb na aktiva zařazená do ISMS a určit možné hrozby, zranitelnosti a rizika hodnoceného systému.
- K provedení analýzy rizik je využívána metodika zaměřená na následující oblasti:
    - identifikace, ohodnocení a případné seskupení aktiv
    - identifikace hrozeb působících na aktiva a následná identifikace zranitelností
    - zhodnocení důsledků realizace hrozeb, jejich reálné pravděpodobnosti a odhad úrovně rizik pro jednotlivé skupiny aktiv
    - určení akceptovatelné úrovně rizik nebo rozhodnutí o nutnosti snížení jeho úrovně
    - snížení či likvidace rizik prostřednictvím pokrytí hrozeb doporučenými protiopatřeními dle ISO/IEC 27002:2007
- Analýza rizik je aktualizována v periodě dvou let nebo v případě změn v informačních systémech a změn v požadavcích na bezpečnost informací.

6. Organizace bezpečnosti informací

6.1 Interní organizace

Cíl: Řídit bezpečnost informací ve společnosti XXX.

- Je vytvořen normativní rámec pro zahájení a řízení implementace bezpečnosti informací ve společnosti XXX. Představenstvo společnosti XXX schválilo politiku bezpečnosti informací, přiřadilo role v oblasti bezpečnosti informací a koordinuje implementaci bezpečnosti v organizaci.
- V rámci koordinace bezpečnosti je nutné poskytovat podporu vzdělávání v oblasti bezpečnosti dotýkající se celé společnosti XXX, například školení a program zvyšování bezpečnostního povědomí.
- Informace získané z procesu monitorování a přezkoumání bezpečnostních incidentů musí být vyhodnoceny a musí být doporučen vhodný způsob reakce na identifikované bezpečnostní incidenty.

6.2 *Externí subjekty*

Cíl: Zachovat bezpečnost informací organizace a prostředků pro zpracování informací, které jsou přístupné, zpracovávané, sdělované nebo spravované externími subjekty.

- Společnost XXX pokládá za důležité zachovat bezpečnost organizace a prostředků pro zpracování informací, které jsou přístupné, zpracovávané, sdělované nebo spravované externími subjekty.
- Externími subjekty se v tomto smyslu rozumí jak klienti, tak i třetí strany poskytující služby pro činnost společnosti XXX, včetně služeb outsourcingu.
- Při přidělování přístupů k informacím společnosti XXX pro třetí strany se bere do úvahy zejména:
    - hodnota, citlivost a kritičnost příslušných informací
    - opatření nutné k ochraně informací, ke kterým nemají mít externí subjekty přístup
    - způsob, jakým je identifikována organizace nebo personál mající oprávnění k přístupu, jakým způsobem je toto oprávnění ověřeno a jak často znovu potvrzeno

  - postupy a opatření používané externími subjekty při ukládání, komunikování, sdílení a výměně informací
  - jaký může mít dopad nedostupnost informací a prostředků pro zpracování informací externím subjektem
  - dopad, jaký může mít zadání nebo obdržení nepřesných nebo klamných informací externím subjektem
  - zákonné, regulatorní a jiné relevantní smluvní požadavky ve vztahu k externím subjektům, které musí být vzaty v potaz
- Přístup třetích stran k informacím a k prostředkům pro zpracování informací by neměl být umožněn do té doby, než jsou implementována přiměřená bezpečnostní opatření a podepsána dohoda, ve které se vymezí podmínky síťového propojení nebo přístupu třetí strany do prostor společnosti XXX a pracovní podmínky (logický i fyzický přístup k aktivům a informacím).

7. Řízení aktiv

7.1 Odpovědnost za aktiva

Cíl: Nastavit a udržovat přiměřenou ochranu aktiv organizace.

- Evidence aktiv pomáhá zajistit udržování jejich účinné bezpečnostní ochrany. Proces vytvoření seznamu aktiv je důležitý i pro management rizik.
- Organizace musí být schopna identifikovat svá aktiva a jejich relativní hodnotu a důležitost. Na základě těchto informací zajišťuje úroveň ochrany odpovídající hodnotě a důležitosti aktiv.
- Jednotlivá aktiva musí být jasně určena včetně jejich umístění a musí být schválen a zaevidován jejich vlastník a jejich bezpečnostní klasifikace
- Za řádnou evidenci aktiv odpovídá bezpečnostní manažer.
- Aktiva lze použít výhradně k účelům souvisejícím s výkonem pracovní činnosti.
- Aktiva musí být používána v souladu s doporučeními výrobce a technologickými předpisy a pravidly.
- Jakékoli jiné použití aktiv musí být schváleno na úrovni vedení.

- Nedodržení pravidel přípustného použití aktiv je hodnoceno jako porušení pracovní kázně a vede k postihu viníka.

7.2 Klasifikace informací

Cíl: Zajistit, aby informace získaly odpovídající úroveň ochrany.

- Je neefektivní chránit všechny informace stejným způsobem. Proto se zavádí klasifikace informací, která rozdělí informace s ohledem na jejich hodnotu, právní požadavky a citlivost. Pro takto rozdělené informace jsou definována ochranná opatření, která se vztahují pouze na příslušnou kategorii, nebo klasifikační úroveň.
- Klasifikované informace musí být chráněny před neautorizovaným přístupem, změnou nebo znepřístupněním po celou dobu jejich platnosti.

8. Bezpečnost lidských zdrojů

8.1 Před vznikem pracovního vztahu

Cíl: Zajistit, aby zaměstnanci, smluvní a třetí strany byli srozuměni se svými povinnostmi, aby pro jednotlivé role byli vybráni vhodní kandidáti a snížit riziko lidské chyby, krádeže, podvodu nebo zneužití prostředků společnosti XXX.

- Závazky a odpovědnosti zaměstnanců v oblasti bezpečnosti informací jsou stanoveny a zdokumentovány v personální dokumentaci v souladu s touto bezpečnostní politikou. V dokumentech musí být jednoznačně určena odpovědnost zaměstnance za provedené činnosti.
- V rámci přijímacího řízení musí být zájemcům o práci jasně sděleny role a odpovědnosti spojené s místem, o které se ucházejí.

8.2 Během pracovního vztahu

Cíl: Zajistit, aby si zaměstnanci, smluvní a třetí strany byli vědomi bezpečnostních hrozeb a problémů s nimi spojených, svých odpovědností a povinností a aby byli připraveni

podílet se na dodržování politiky bezpečnosti informací během své běžné práce a na snižování rizika lidské chyby.

- Uživatelé musí být pravidelně školeni v bezpečnostních postupech a ve správném používáni prostředků pro zpracování informací, aby byla minimalizována bezpečnostní rizika. Školení v bezpečnostních postupech je vhodné přičlenit k povinně prováděným školením o bezpečnosti práce a o požární ochraně.
- Cílem školení je zajištění, aby si uživatelé uvědomovali bezpečnostní hrozby a problémy s nimi spjaté, aby byli seznámeni se svými povinnostmi a byli připraveni podílet se na dodržování politiky bezpečnosti informací během své běžné práce.
- Před poskytnutím přístupu k systémům IT se musí každý nový uživatel seznámit s relevantními bezpečnostními dokumenty.
- O proškolení musí být vedeny záznamy.
- Za proces a náležitosti spojené s ukončením, nebo změnou pracovního vztahu je odpovědný vedoucí personálního oddělení, který spolupracuje s nadřízeným zaměstnance opouštějícího organizaci tak, aby byly dodrženy veškeré aspekty bezpečnosti a odpovídající postupy.
- V případě změny pracovního vztahu spojené se změnou pracovního zařazení musí být realizovány činnosti navrácení zapůjčených předmětů, které zaměstnanec v novém pracovním zařazení nebude potřebovat. Vždy ale musí být provedena akceptace nebo případně odebrání všech přístupových práv zaměstnance k informačním systémům.

9. Fyzická bezpečnost a bezpečnost prostředí

- Fyzická bezpečnost představuje soubor opatření k zajištění fyzické ochrany prostorů, ve kterých jsou umístěna informační aktiva.

Cílem je zabezpečit ochranu prostorů proti hrozbám:

- neoprávněného vstupu

  - neoprávněné manipulace s aktivy
  - poškození nebo zničení aktiv
  - krádeže aktiv
- Fyzická bezpečnost se doplňuje opatřeními objektové a technické bezpečnosti.
- Za fyzickou bezpečnost jednotlivých pracovišť odpovídají vedoucí příslušných pracovišť (oddělení, divize).
- V rámci periodických bezpečnostních školení zaměstnanců bude prováděno i školení z problematiky fyzické bezpečnosti osob a majetku.

9.1 Zabezpečené oblasti

Cíl: Předcházet neautorizovanému fyzickému přístupu do vymezených prostor, předcházet poškození a zásahům do provozních budov a informací organizace.

- Zabezpečenou oblastí může být uzamykatelná kancelář nebo několik místností uvnitř fyzického bezpečnostního perimetru. Uvnitř bezpečnostního perimetru mohou být mezi oblastmi s rozdílnou úrovní bezpečnosti dodatečné bariéry a perimetry zajišťující kontrolu fyzického přístupu.
- Prostory v objektech jsou členěny tak, aby do prostor, kde není přístup veřejnosti nezbytný, byl omezen volný přístup osob. Vlastníci prostor musí stanovit, které prostory jsou veřejné, a které jsou neveřejné (kam nemá veřejnost přístup).
- Neveřejné oblasti jsou zabezpečeny proti vstupu veřejnosti
- Všichni oprávnění zaměstnanci musí být seznámeni s bezpečnostními pravidly pro práci v zabezpečené oblasti.
- Vstup do zabezpečené oblasti mají pouze oprávnění zaměstnanci, ostatní zaměstnanci nebo návštěvy smějí vstupovat do zabezpečené oblasti pouze v jejich doprovodu. V opodstatněných případech může být za návštěvu považován i personál provádějící úklid nebo servis v zabezpečené oblasti nebo servis zařízení v těchto prostorech umístěných.

9.2 Bezpečnost zařízení

Cíl: Předcházet ztrátě, poškození, krádeži nebo kompromitaci aktiv a přerušení činností organizace.

- Zařízení musí být umístěna a chráněna tak, aby se snížila rizika hrozeb a nebezpečí daná prostředím a aby se omezily příležitosti pro neoprávněný přístup.
- Aktiva, která vyžadují zvláštní ochranu, jsou umístěna do zabezpečených oblastí, aby se zvýšila celková ochrana těchto aktiv.
- Pro elektrická zařízení zajišťující kritické operace jsou použity záložní zdroje UPS, umožňující korektní ukončení nebo pokračování v práci.
- Servis a opravy zařízení jsou prováděny pouze oprávněným personálem. O opravách zařízení se vedou záznamy.
- V případech, kdy údržbu zařízení neprovádí vlastní personál, nebo je zařízení odesíláno do opravy, jsou z něj odstraněny veškeré informace (např. vyjmutí HDD), nebo musí být práce prováděny pod dozorem kompetentního zaměstnance společnosti XXX.
- Všechna zařízení obsahující paměťová média musí být kontrolována tak, aby bylo možné zajistit, že před jejich likvidací nebo opakovaným použitím budou citlivá data a licencované programové vybavení odstraněny nebo bezpečně přepsány.

10. Řízení komunikací a řízení provozu

10.1 Provozní postupy a odpovědnosti

Cíl: Zajistit správný a bezpečný provoz prostředků pro zpracování informací.

- Provozní postupy musí být zdokumentovány a udržovány. Musí být dostupné všem uživatelům a správcům systémů podle jejich pracovního zařazení a role v informačním systému.
- Povinnosti a oblasti odpovědností musí být odděleny tak, aby se snížila možnost neautorizované modifikace nebo zneužití informací či služeb.

10.2 Řízení dodávek služeb třetích stran

Cíl: Zavést a udržovat přiměřenou úroveň bezpečnosti informací a úroveň dodávání služeb ve shodě s uzavřenými dohodami.

- Součástí služeb poskytovaných třetí stranou je realizace smluvně dohodnutých bezpečnostních opatření včetně vymezení služeb a jejich správy.
- Pravidla pro monitorování a přezkoumávání služeb poskytovaných třetími stranami, včetně dodržování bezpečnosti informací, jakož i způsoby řešení vzniklých bezpečnostních incidentů a problémů musí být obsažena v příslušných provozních řádech ve vazbě na příslušný smluvní vztah.

10.3 Plánování a přejímání systémů

Cíl: Minimalizovat riziko selhání informačních systémů

- Oddělení IT musí zajistit, aby požadavky a kritéria pro přejímání nových počítačových systémů byly jednoznačně stanoveny, schváleny, zdokumentovány a otestovány.
- Přechod na nové systémy, instalace aktualizací a zavádění nových verzí musí být formálně schválen.
- Předtím, než je provedeno formální schválení, musí být zváženo následující:
    - požadavky na výpočetní a paměťový výkon
    - postupy pro zotavení se z chyb a restartů systému a havarijní plány
    - příprava a testování rutinních provozních postupů
    - schválená sada nasazených bezpečnostních opatření
    - plán kontinuity činností
    - potvrzení, že instalace nového systému nebude mít nepříznivý vliv na existující systémy
    - zváženy dopady nového systému na celkovou bezpečnost organizace
    - školení v obsluze a použití nového systému
    - snadnost použití, ta může pozitivně ovlivnit výkon uživatelů a zabránit zbytečným chybám

10.4 Ochrana proti škodlivým programům a mobilním kódům

Cíl: Chránit integritu programového vybavení a dat.

- Obecně nejrozšířenějšími hrozbami pro prostředky pro zpracování informací jsou škodlivé programy.
- Škodlivý programový kód (viry, malware, atd.) může být zanesen do systémů prostřednictvím souborů a softwaru zaváděných z vyjímatelných počítačových médií, dále i elektronickou poštou. Škodlivý programový kód může znamenat ohrožení ochranných opatření, neúmyslné prozrazení informací, neúmyslné změny informací, ztrátu integrity systému, zničení informací nebo neoprávněné použití zdrojů systému.
- Uživatelé musí být upozorňováni na nebezpečí, které vzniká použitím neschválených programů nebo působením škodlivých programových kódů. U všech počítačů musí být aplikována opatření pro prevenci a detekování škodlivých programových kódů.

10.5 Zálohování

Cíl: Udržovat integritu a dostupnost informací a prostředků pro jejich zpracování.

- Zálohování informací je důležitým prostředkem pro udržení integrity a dostupnosti informací. Musí být vytvořeny rutinní postupy realizující schválené zásady zálohování a strategii pro vytváření záložních kopií dat, aplikací, případně i prostředí a testování jejich obnovení.
- Proces zálohování musí být řešen už ve fázi projektování, kdy u každého nového projektu musí být řešeno:
    - výběr vhodného zálohovacího systému
    - výběr fyzického umístění zálohovacího systému
    - volba použitých záložních médií a způsob jejich ukládání

10.6 Správa bezpečnosti sítě

Cíl: Zajistit ochranu informací v počítačových sítích a ochranu podpůrné infrastruktury.

- Správci sítí musí realizovat opatření pro zajištění bezpečnosti dat v sítích a ochrany souvisejících služeb před neoprávněným přístupem.
- Zejména při nákupu síťových služeb od třetích stran je nutné identifikovat a smluvně stanovit úroveň poskytovaných služeb a požadavky na správu všech síťových služeb.
- Způsobilost poskytovatele síťových služeb bezpečně zajistit správu dohodnutých síťových služeb musí být prověřena a průběžně monitorována, musí být odsouhlaseno právo provádět audit.

10.7 Bezpečnost při zacházení s médii

Cíl: Předcházet neoprávněnému vyzrazení, modifikaci, ztrátě nebo poškození aktiv a přerušení činností společnosti XXX.

- Správa vyměnitelných počítačových médií používaných k pořizování záloh musí být řádně dokumentována formou záznamů evidence zálohovacích médií.
- Před likvidací nebo znovupoužitím zařízení IT (s důrazem na zálohovací média) se provádí bezpečné smazání těchto informací. Likvidace dat musí být řádně dokumentována formou záznamu o likvidaci dat, tento zápis a vlastní likvidaci dat provádí pouze osoby pověřené vlastníkem aktiva.

10.8 Výměna informací

Cíl: Zajistit bezpečnost informací a programů při jejich výměně v rámci organizace a při jejich výměně s externími subjekty.

- Výměna informací může probíhat s použitím celé řady různých typů komunikačních zařízení zahrnujících elektronickou poštu, hlasová zařízení, fax a video.
- Informace mohou být ohroženy díky nedostatku bezpečnostního povědomí, neznalosti pravidel a postupů používání odpovídající techniky, například zaslechnutí obsahu hovoru vedeného pomocí mobilního telefonu na veřejných místech, zaslechnutí obsahu zprávy na telefonním záznamníku nebo fax zaslaný omylem nesprávné osobě.

- Výměna jiných než veřejných informací s jinou organizací nebo externím subjektem musí být schválena vlastníkem informace, pokud se jedná o elektronickou výměnu, je posouzena bezpečnostním manažerem z hlediska naplnění bezpečnostních požadavků.
- Výměna musí být upravena smlouvou.
- Všichni zaměstnanci společnosti XXX jsou povinni dodržovat stanovená pravidla a způsob užívání. Porušení pravidel užívání je považováno v závažných případech za porušení pracovní kázně, případně třetích stran za nedodržení smluvních závazků.

10.9 Služby elektronického obchodu

Cíl: Zajistit bezpečnost služeb elektronického obchodu a jejich bezpečné použití.

- Informace přenášené ve veřejných sítích v rámci elektronického obchodování musí být chráněny před podvodnými aktivitami, před zpochybňováním smluv, neoprávněným vyzrazením či modifikací.
- Musí být zajištěna ochrana informací přenášených při on-line transakcích tak, aby byl zajištěn úplný přenos informací a zamezilo se chybnému směrování, neoprávněné změně zpráv, neoprávněnému vyzrazení, neoprávněné duplikaci nebo opakování zpráv.
- Programy, data a jiné informace, zpřístupňované na veřejně dostupných systémech a vyžadující vysoký stupeň integrity, musí být chráněny adekvátními mechanizmy, jako například digitálním podpisem.
- Veřejně přístupné systémy musí být předtím, než jsou na ně umístěny informace, testovány na slabiny a možná selhání.

10.10 Monitorování

Cíl: Detekovat neoprávněný přístup k informacím.

- Záznamy, obsahující chybová hlášení včetně bezpečnostně významných událostí, musí být pořizovány a uchovány tak, aby byly využitelné pro budoucí vyhodnocování.

- Zejména jsou použity logy systémů, informace obsažené v nezávislých dohledových systémech a informace o chybách získané jinou cestou (např. HelpDesk)
- Úroveň monitorování jednotlivých informačních systémů je stanovena a je součástí designu systému SIEM.
- Bezpečnostně relevantní události a chyby jsou zaznamenány a analyzovány a provedena opatření k nápravě. Hlášení uživatelů o problémech systému pro zpracování nebo výměnu informací jsou zaznamenávána obvykle v rámci systému HelpDesk.

11. Řízení přístupu

11.1 Požadavky na řízení přístupu

Cíl: Řídit přístup k informacím.

- Zásady řízení přístupu jsou naplňovány následujícími pravidly:
  - je provedena identifikace všech informací vztahujících se k aplikacím a určení rizik, která jsou vůči těmto informacím relevantní
  - uvážení právních a smluvních závazků týkajících se ochrany přístupu k datům nebo službám
  - zavedení standardních uživatelských profilů pro obecné role při zpracování úloh v IT (běžný uživatel, uživatel s právem zápisu)
  - oddělení rolí při řízení přístupů, např. požadavek na zřízení přístupu, schvalování přístupu, administrace přístupu
  - požadavky na formální schválení žádostí o přístup
  - odebírání přístupových práv
- Při specifikaci pravidel pro přístupy jsou vzaty v úvahu následující skutečnosti:
  - rozlišení mezi pravidly, která musí být vždy v platnosti a těmi, která jsou podmíněná nebo volitelná
  - stanovení pravidel založených přednostně na výroku „všechno je obecně zakázáno, pokud není něco výslovně povoleno“ místo slabšího pravidla „všechno je obecně povoleno, pokud není něco výslovně zakázáno“

11.2 Řízení přístupu uživatelů

Cíl: Zajistit oprávněný přístup uživatelů a předcházet neoprávněnému přístupu k informačním systémům.

- Přidělení nebo změna přístupu ke službě nebo zařízení IT je pro uživatele provedena výhradně v souladu s jeho oprávněnými potřebami, v souladu s politikou přidělování práv a na základě schválené žádosti.
- Při postupech pro přidělování přístupů se zvláštním oprávněním (privilegovaná oprávnění) se postupuje podle následujících zásad:
    - zvláštní oprávnění musí být přidělena uživatelům v souladu s politikou pro kontrolu přístupů na základě nutné potřeby a s rozhodnutím případ od případu.
    - musí být podporováno použití systémových procedur, aby se zamezila potřeba vydávat privilegovaná práva uživatelům;
    - musí být podporováno použití takových programů, které nepotřebují vydávání privilegovaných práv;
    - privilegovaná práva musejí být přidělována k jiným uživatelským identifikátorům, než jsou identifikátory pro běžné použití.

11.3 Odpovědnosti uživatelů

Cíl: Předcházet neoprávněnému uživatelskému přístupu, vyzrazení nebo krádeži informací a prostředků pro zpracování informací.

- Uživatelé musí zajistit přiměřenou ochranu nejen obsluhovaných ale i neobsluhovaných zařízení.
- Uživatelé musí postupovat zejména následovně:
    - při krátkodobém přerušení práce ukončit aktivní relace nebo je zajistit vhodným mechanizmem, například spořičem obrazovky s heslem,
    - odhlásit se v případě ukončení práce ze všech používaných relací k serverům nebo informačním systémům a rovněž i od pracovní stanice, ze které byly relace navázány (tj. nevypínat pouze monitor počítače nebo terminál)
    - zajistit přidělené mobilní prostředky proti krádeži
    - chránit své autentizační údaje před neoprávněným použitím

  - zabránit neautorizovanému přístupu k přiděleným prostředkům
- Společnost XXX používá politiku čistého stolu a čisté obrazovky k ochraně informací před neautorizovaným přístupem, ztrátou nebo poškozením.

11.4 Řízení přístupu k síti

Cíl: Předcházet neautorizovanému přístupu k síťovým službám.

- Architektura komunikační infrastruktury a bezpečnostní funkce jejích služeb je volena tak, aby odpovídala charakteru a klasifikaci informací, které jsou v ní uchovávány a zpracovávány.
- Komunikační infrastruktura musí být oddělena od jiných sítí, zejména od veřejných prostředí (Internet apod.).
- Povolené výjimky musí být řádně dokumentovány a ověřovány a musí být schváleny bezpečnostním manažerem. Povolené výjimky musí poskytovat dostatečné záruky a být řešeny tak, že jejich prostřednictvím nedojde k narušení systému řízení přístupu.
- Komunikační infrastruktura musí být budována tak, aby, je-li to technicky možné, selhání jedné bezpečnostní součásti (firewallu, zabezpečení služby, serverového systému apod.) nezpůsobilo vážné ohrožení její bezpečnosti, zejména potom neumožnilo průnik.
- Dále musí obsahovat monitorovací a bezpečnostní prvky umožňující včasnou detekci bezpečnostního nebo provozního selhání nebo chybné funkce její součásti.

11.5 Řízení přístupu k operačnímu systému

Cíl: Předcházet neautorizovanému přístupu k operačním systémům.

- Přístup k operačnímu systému musí být řízen postupy bezpečného přihlášení.
- Všichni uživatelé musí mít pro výhradní osobní použití jedinečný identifikátor (uživatelské ID), musí být také zvolen vhodný způsob autentizace k ověření jejich identity.

- Toto opatření se vztahuje na všechny typy uživatelů (včetně technického personálu, jako jsou operátoři, administrátoři sítě, systémoví programátoři a databázoví administrátoři).
- Uživatelská ID umožňují pozdější vysledování odpovědnosti konkrétních uživatelů za činnosti v systému. Běžné aktivity nesmí být prováděny z privilegovaných účtů určených ke správě systému.
- K uživatelskému ID patří vždy heslo, nebo jiný bezpečný autentizační prvek.

11.6 Řízení přístupu k aplikacím a informacím

Cíl: Předcházet neoprávněnému přístupu k informacím uloženým v počítačových systémech.

- Přístup k programům a informacím musí být omezen jen na oprávněné uživatele.
- Aplikační systémy musí:
    - kontrolovat přístup uživatelů k datům a funkcím aplikačního systému v souladu se stanovenou politikou řízení přístupu
    - poskytovat ochranu před neoprávněným přístupem ke všem nástrojům a systémovým programům, které mohou obejít systémové a aplikační kontrolní mechanizmy
    - logovat přístup a provedené operace
    - nenarušit bezpečnost jiných systémů, se kterými jsou sdíleny informační zdroje

11.7 Mobilní výpočetní zařízení a práce na dálku

Cíl: Zajistit bezpečnost informací při použití mobilní výpočetní techniky a zařízení pro práci na dálku.

- Pro užívání mobilních výpočetních prostředků jsou stanoveny požadavky tak, aby byla zajištěna bezpečnost vnitřního prostředí a jejich bezpečné užívání.
- Vzdálený přístup k prostředkům ICT musí být náležitě řízen

12. Akvizice, vývoj a údržba informačních systémů

12.1 Bezpečnostní požadavky informačních systémů

Cíl: Zajistit, aby se bezpečnost stala neoddělitelnou součástí informačních systémů.

- Požadavky organizace na nové informační systémy nebo na rozšíření existujících systémů musí obsahovat také požadavky na bezpečnostní opatření a musí splňovat minimálně následující požadavky:
    - bezpečnostní požadavky a opatření musí odrážet hodnotu informačních aktiv pro organizaci a možnou škodu, která by mohla být výsledkem nedostatečné bezpečnosti nebo jejího selhání
    - požadavky na bezpečnost informačních systémů a procesy implementace bezpečnosti musí být začleněny do projektu informačního systému již v jeho počáteční fázi,
    - před zprovozněním informačního systému musí vždy proběhnout formální proces testování a zavedení do provozu
    - ve smlouvách s dodavateli musí být specifikovány požadavky na bezpečnost

12.2 Správné zpracování v aplikacích

Cíl: Předcházet chybám, ztrátě, neoprávněné modifikaci nebo zneužití informací v aplikacích.

- Vstupní data aplikací musí být kontrolována z hlediska správnosti a adekvátnosti.
- Kontrolovány jsou transakční vstupy vlastních dat a číselníky.
- Pro detekci jakéhokoliv poškození informací vzniklého chybami při zpracování nebo úmyslnými zásahy musí být začleněny kontroly validace dat do aplikace.
- Pro zajištění, že zpracování uložených informací je správné a odpovídající dané situaci, musí být provedeno ověření platnosti výstupních dat.
- Výstupní kontrola platnosti dat může zahrnovat:
    - prověrku hodnověrnosti, tedy ověření přijatelnosti výstupních dat
    - porovnávací kontrolní součet zajišťující, že byla zpracována všechna data
    - poskytnutí dostatku informací pro následný proces zpracování, pro stanovení správnosti, kompletnosti, přesnosti a klasifikace informací

- postupy pro reakce na výstupní testy platnosti dat
- definice odpovědností všeho personálu účastnícího se výstupního procesu

12.3 Kryptografická opatření

Cíl: Ochránit důvěrnost, autentičnost a integritu informací s pomocí kryptografických prostředků.

- V případě používání kryptografických opatření musí být vypracována příslušná metodika, která bere v úvahu následující požadavky:
  - přístup ke kontrolám kryptografických zařízení a aplikací včetně obecných principů ochrany informací
  - určení úrovně ochrany podle analýzy rizik
  - užití šifrování pro ochranu citlivých informací přenášených mobilními zařízeními, médii a komunikačními linkami

12.4 Bezpečnost systémových souborů

Cíl: Ochránit důvěrnost, autentičnost a integritu systémových souborů

- Instalace programového vybavení do provozního systému musí být řízena a kontrolována.
- Klíčová jsou následující opatření:
  - aktualizace provozního programového vybavení, aplikací a knihoven programů jsou prováděny pouze oprávněným správcem
  - spustitelný kód nesmí být implementován do provozního systému dříve, než je k dispozici doklad o úspěšném testování a převzetí. Testy musí být prováděny na oddělených systémech
  - musí být udržován přehled o instalovaném programovém vybavení a systémová dokumentace
  - programové vybavení použité v provozních systémech musí být udržováno způsobem, který podporuje dodavatel
  - každé rozhodnutí o povýšení verze musí brát v úvahu její bezpečnost
  - fyzický nebo logický přístup musí být umožněn dodavatelům pouze na základě platných servisních smluv

- Zdrojové kódy programů je nutné umístit do kontrolovaného centrálního úložiště, nejlépe v knihovnách zdrojových kódů.

12.5 Bezpečnost procesů vývoje a podpory

Cíl: Udržovat bezpečnost programového vybavení a informací aplikačních systémů.

- Kontrolní procedury pro změnové řízení musí být nastaveny tak, aby se minimalizovala možnost poškození informačních systémů. Procedury pro změnové řízení musí splňovat následující požadavky:
  - požadavky na změny musí být schváleny vlastníkem aktiva
  - aktualizace dokumentace
  - auditní záznamy všech žádostí o změny
  - zajištění vhodné volby doby implementace, aby nebyl narušen provoz
- V rámci změnového řízení jsou požadavky na IT rozčleněny do následujících skupin:
  - požadavek na změnu funkčnosti
  - požadavek na opravu chybné funkce systému
  - požadavek na datovou manipulaci
  - požadavek na provozní zásah
- Po provedení změn operačního systému je nutné provést správcem IS přezkoumání a testování aplikačních systémů se zahrnutím následujících požadavků:
  - přezkoumání kontrolních opatření a postupů zajišťujících integritu, aby bylo zajištěno, že zůstanou účinné i po změně operačního systému
  - zajištění případných změn v plánech kontinuity činností
- Když je vyvíjeno programové vybavení externím dodavatelem, měly by být zváženy následující body:
  - licenční ujednání, vlastnictví kódu a práv duševního vlastnictví
  - osvědčení kvality a správnosti provedených prací
  - právo přístupu k vývoji pro audit kvality a správnosti provedené práce
  - smluvní podmínky na kvalitu a zabezpečení kódu
  - testování na odhalení trojských koní a škodlivých kódů před instalací

12.6 Řízení technických zranitelností

Cíl: Snížit rizika vyplývající z využívání zveřejněných technických zranitelností.

- Rizika zneužití publikovaných technických zranitelností jsou omezena prostřednictvím opatření, která zahrnuje správa technických zranitelností podle následujících doporučení. Tato opatření jsou vzhledem k technickým problémům v této oblasti plně v kompetenci oddělení IT:
    - definice rolí a zodpovědností, včetně monitorování zranitelností, posouzení rizik, instalace oprav, sledování aktiv a koordinace činností
    - zdroje informací o zranitelnostech a jejich aktualizace
    - časové limity reakce na upozornění o zranitelnostech
    - systémy s vysokým rizikem musí být řešeny přednostně. Požadavek předkládá vlastník dotčeného aktiva

13. Zvládání bezpečnostních incidentů

13.1 Hlášení bezpečnostních událostí a slabin

Cíl: Zajistit nahlášení bezpečnostních událostí a slabin informačního systému způsobem, který umožní včasné zahájení kroků vedoucích k nápravě.

- Bezpečnostní události musí být co nejrychleji hlášeny příslušnými řídícími kanály.
- V případě výskytu bezpečnostního incidentu (slabiny) se musí reagovat přiměřeným způsobem.
- Každý zaměstnanec je povinen v případě, že byl účastníkem nebo svědkem bezpečnostního události, toto neprodleně nahlásit příslušnému zaměstnanci pověřeného výkonem bezpečnostních rolí (bezpečnostnímu manažerovi), který iniciuje další činnosti. O incidentu zároveň informuje svého nadřízeného pracovníka.
- Každý bezpečnostní incident nebo podezření na něj musí být vyšetřen, aby byly zjištěny jeho příčiny, a následně musí být podniknuta nápravná opatření, která zamezí jeho opakování.

13.2 Zvládání bezpečnostních incidentů a kroky k nápravě

Cíl: Zajistit odpovídající a účinný přístup ke zvládání bezpečnostních incidentů.

- Při zvládání bezpečnostního incidentu, pokud je to možné, se musí postupovat tak, aby nedošlo ke zničení stop vedoucích k jeho objasnění. Zvládání bezpečnostního incidentu se zpravidla realizuje v následujících etapách:
  - akce na zastavení negativního působení incidentu a informování dotčených stran
  - akce na obnovu realizace procesů zasažených incidentem
  - vyšetřování bezpečnostního incidentu
  - vyhodnocení bezpečnostního incidentu a návrh nápravných doporučení,
  - schválení nápravných doporučení
  - informování dotčených stran o uzavření incidentu
  - rozhodnutí o případném zahájení disciplinárního řízení vůči potenciálním viníkům
  - implementace nápravných doporučení
- Při vyšetřování bezpečnostního incidentu jsou vlastníci aktiv povinni poskytnout potřebnou součinnost, přístup a veškeré informace potřebné k vyšetření incidentu. Musí být realizovány postupy, které zabrání znehodnocení případného důkazního materiálu.
- Informace získané při vyhodnocení bezpečnostních incidentů musí být využity pro identifikaci opakujících se incidentů nebo incidentů s velkými následky.
- Závěry z vyhodnocení bezpečnostních incidentů mohou také signalizovat potřebu využití dodatečných nebo důkladnějších opatření, která by omezila frekvenci, škody a náklady jejich budoucích výskytů. Kromě toho musí být vzaty v úvahu při revizi bezpečnostní politiky.

14. Řízení kontinuity činností organizace

Cíl: Bránit přerušení provozních činností a chránit kritické procesy společnosti XXX před následky závažných selhání informačních systémů nebo katastrof a zajistit včasnou obnovu činností.

- Je třeba, aby kontinuita činností organizace z pohledu bezpečnosti byla založena na identifikaci událostí (nebo sledu událostí), které mohou být příčinou přerušení procesů, např. chyba zařízení, povodeň, požár.
- Je nezbytné, aby poté následovalo hodnocení rizik k určení pravděpodobnosti a velikosti dopadu těchto druhů přerušení, jak z hlediska rozsahu škod, tak doby jejich obnovení.
- Každý plán musí popisovat přístup k zajištění kontinuity činností, např. zajištění dostupnosti a bezpečnosti informací a informačních systémů. Každý plán kontinuity musí jasně specifikovat podmínky své aktivace, stejně jako osoby s odpovědností za vykonávání každého bodu plánu. Při vzniku nových požadavků na havarijní postupy, jako např. evakuační plány nebo jakékoliv existující dohody o zajištění náhradního provozu, musí být adekvátním způsobem doplněny. Revize postupů musí být začleněna do programu řízení změn, aby se zajistilo, že je problematika kontinuity činností vždy náležitě pokryta.

15. Soulad s požadavky

15.1 Soulad s právními normami

Cíl: Vyvarovat se porušení norem trestního nebo občanského práva, zákonných nebo smluvních povinností a bezpečnostních požadavků.

- V oblasti působnosti bezpečnosti je uplatňováno následné (sestupné) pořadí úrovní platnosti normativů:
  - zákonné a podzákonné normy
  - smluvní závazky
  - interní bezpečnostní normativy
  - ostatní normativy
- Musí být uplatňována zásada, kdy veškerá ustanovení normativů nižší úrovně musí být v souladu s ustanoveními normativů vyšší úrovně.
- Zákonem chráněné programové produkty jsou dodávány na základě licenčních ujednání, která limitují jejich užití a která omezují jejich kopírování pouze na vytvoření záložních kopií. Oddělení IT odpovídá za instalaci chráněných

programových produktů na uživatelské stanice tak, aby nebyl překročen maximální počet uživatelských přístupů k programům.

- Oddělení IT odpovídá za oprávněné pořízení počítačového programu a zabezpečuje vedení jeho evidence. Záznam – evidence programového vybavení je veden elektronicky.
- Neoprávněná instalace autorských programových produktů zaměstnanci je chápána jako hrubé porušení pracovní kázně.
- Ochrana dat a soukromí musí být zajištěna v souladu s odpovídající legislativou, předpisy a pokud je to relevantní, se smlouvami.
- Společnost XXX musí vytvořit a do praxe zavést pravidla na ochranu osobních údajů a soukromí v souladu s požadavky zákona č. 101/2000Sb., o ochraně osobních údajů a o změně některých zákonů v platném znění.
- S pravidly musí být seznámeny všechny osoby, které se nějakým způsobem podílejí na zpracování osobních údajů.

15.2 Soulad s bezpečnostními politikami, normami a technická shoda

Cíl: Zajistit shodu systémů s bezpečnostními politikami organizace a normami.

- Soulad s bezpečnostními politikami a normami musí být zajištěn.
- V případě, že je zjištěn nesoulad, musí vedoucí zaměstnanci:
  - určit příčiny nesouladu
  - vyhodnotit potřebu přijetí opatření k nápravě
  - určit a implementovat nápravná opatření
  - přezkoumat přijatá nápravná opatřeni
- Závěry z přezkoumání a přijatá nápravná opatření jsou zaznamenána a záznamy uchovány.

15.3 Hlediska auditu informačních systémů

Cíl: Maximalizovat účinnost auditu a minimalizovat zásahy do/z informačních systémů.

- Auditní činnost je plánována interním auditorem. V případě interního auditu zpracovává interní auditor plán auditu, v případě externího auditu zpracovává zadání auditu.

- V případě, že auditor potřebuje jiný typ přístupu než pouze pro čtení, vyhotoví provozovatel systému kopie požadovaných souborů a předá je auditorovi. Kopie se po ukončení auditu smažou, případně musí být řádným způsobem chráněny.
- Všechny požadavky, postupy a odpovědnosti auditora musí být dokumentovány.

16. Závěrečná ustanovení

- Za dodržování této bezpečnostní politiky informací odpovídají všichni zaměstnanci společnosti.
- Za správnost a aktualizaci tohoto dokumentu odpovídá vedoucí oddělení IT bezpečnosti.
- Kontrolu plnění povinností vyplývajících z ustanovení bezpečnostní politiky informací zajistí v mezích své působnosti představenstvo a vedoucí zaměstnanci.
- Porušení zásad, postupů a pravidel bezpečnosti informací zaměstnancem je považováno za porušení pracovní kázně a může být důvodem k rozvázání pracovního poměru.

Tento řád nabývá platnosti a účinnosti dnem vydání.

…….....
Datum a podpis statutárního zástupce

Příloha III:

BEZPEČNOSTNÍ ZÁSADY UŽÍVÁNÍ ICT

Interní dokument

Účel

Souhrn doporučených pravidel chování při práci s výpočetní technikou. Slouží jako návod k efektivnímu a bezpečnému využívání prostředků IT. Jejím cílem je minimalizovat rizika průniku nepovolaným osobám do firemní infrastruktury, ztrátě či odcizení dat a v neposlední řadě též k minimalizaci nákladů na provoz výpočetní techniky. Těmito pravidly se musí řídit všichni zaměstnanci bez ohledu na pracovní zařazení. Bezpečnost firemní počítačové sítě a dat není zajištěna pouze složitým a finančně nákladným HW a SW, ale především úrovní vzdělanosti a odpovědnosti zaměstnanců. Tato pravidla jsou obecně platná nejen ve firmě XXX, ale též i ve všech jiných počítačových sítích, stejně tak jako při práci na jakémkoli libovolném počítači.

- **Neměnit HW/SW/BIOS konfiguraci** - také nezasahovat do vnitřních částí HW.
- **Zamezit přístup ke svěřené technice nepovolaným osobám** – včetně rodinných příslušníků.
- **Zabezpečit zařízení proti odcizení** - týká se především přenosných zařízení mimo firmu.
- **Nenechávat HW zbytečně zapnutý**
- **Šetřit tiskové náklady** - ne vše musí být vytištěné a barevné.
- **Neinstalovat nelegální a neschválený SW** – hrozba finančních postihů a trestního stíhání.
- **Nepoužívat firemní prostředky ICT k privátním účelům**
- **Pozor na podezřelé emaily** – obzvláště ty s neznámým odesílatelem a vloženou přílohou. Může jít o SPAM, Phishing nebo Malware. Takové emaily a přílohy vůbec neotvírat.
- **Neposílat emailem větší objemy dat** – k těmto účelům jsou vhodnější jiné metody.

- **Pro firemní účely nepoužívat privátní emailové schránky** – mohli by se tak k citlivým firemním informacím dostat nepovolané osoby.
- **Ke vzdálenému přístupu k firemní prostředkům ICT používat firemní HW** – nepoužívat neznámá PC (internetové kavárny, atd). Mohou v nich být instalovány keylogery a jiný škodlivý kód.
- **Dbát obezřetnosti při připojování k neznámým sítím**
- **Neskenovat síť a nezachytávat síťovou komunikaci**
- **Nezapojovat do firemní infrastruktury soukromá zařízení**
- **Vypínat bezdrátové technologie, když nejsou potřeba** - bluetooth, WiFi, atd. Některé bezdrátové technologie mají větší dosah, než si myslíte. Zabráníte tak pokusům o průnik do vašeho zařízení.
- **Při vzdáleném připojení neopouštět pracovní stanici**
- **Zajistit data proti zcizení** – týká se situace při vynášení dat mimo firmu. K dispozici jsou hesla, šifrování, atd. Informace podá odbor IT.
- **Pravidelně zálohovat** - za lokální data na pracovních stanicích si odpovídá každý uživatel sám.
- **Nesdělovat svoje autentizační údaje –** nikdy a nikomu.
- **Pečlivě číst systémové hlášky** - neodklikávejte automaticky nic, co jste si nepřečetli a o čem přesně nevíte, co se provede za operaci.
- **Hesla –** dodržujte zásady bezpečného hesla.
- **Při zjištění viru nebo jiného napadení stanice** - neprodleně vypnout PC a tuto skutečnost oznámit na odbor IT.

Nedodržování interních předpisů bude řešeno dle zákoníku práce.

Tento řád nabývá platnosti a účinnosti dnem vydání.

…….....

Datum a podpis statutárního zástupce