VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA STROJNÍHO INŽENÝRSTVÍ

FACULTY OF MECHANICAL ENGINEERING

ÚSTAV VÝROBNÍCH STROJŮ, SYSTÉMŮ A ROBOTIKY

INSTITUTE OF PRODUCTION MACHINES, SYSTEMS AND ROBOTICS

INFORMAČNÍ BEZPEČNOST VE STROJÍRENSTVÍ

INFORMATION SECURITY IN ENGINEERING

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

AUTOR PRÁCE — Tomáš Fialík

AUTHOR

VEDOUCÍ PRÁCE — Ing. Jana Rozehnalová, M.Sc.

SUPERVISOR

BRNO 2020

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ FAKULTA STROJNÍHO INŽENÝRSTVÍ

Zadání bakalářské práce

Ústav:	Ústav výrobních strojů, systémů a robotiky
Student:	**Tomáš Fialík**
Studijní program:	Strojírenství
Studijní obor:	Kvalita, spolehlivost a bezpečnost
Vedoucí práce:	**Ing. Jana Rozehnalová, M.Sc.**
Akademický rok:	2019/20

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách a se Studijním a zkušebním řádem VUT v Brně určuje následující téma bakalářské práce:

Informační bezpečnost ve strojírenství

Stručná charakteristika problematiky úkolu:

Informační bezpečnost je důležitým celosvětovým pojmem napříč různými průmyslovými odvětvími. Každý podnik by měl mít zaveden security management zvládání rizik informačních hrozeb (ISMS - Information Security Management System) na základě znalostí nejen legislativních požadavků či doporučení z norem. Práce rešeršního charakteru pojednává o legislativě, normách a relevantních doporučení vázající se k problematice informační bezpečnosti ve strojírenském výrobním podniku.

Cíle bakalářské práce:

Popis současného stavu a trendů v oblasti informační bezpečnosti.
Provedení analýzy současných legislativních požadavků EU a ČR.
Provedení rešerše požadavků relevantních platných norem.
Systémový rozbor řešené problematiky.
Vypracování hodnocení informačních rizik ve výrobě.
Vlastní závěry a/nebo doporučení pro další rozvoj řešené problematiky.

Seznam doporučené literatury:

ČERMÁK, Miroslav. Řízení informačních rizik v praxi. Brno: Tribun EU, 2009. ISBN 978-80-7399-31-1.

ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: Akademické nakladatelství CERM, 2013. ISBN 9788072048724.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2019/20

V Brně, dne

L. S.

doc. Ing. Petr Blecha, Ph.D. ředitel ústavu	doc. Ing. Jaroslav Katolický, Ph.D. děkan fakulty

ABSTRAKT

Bakalářská práce se zabývá problematikou informační bezpečnosti. Příslušnými legislativními požadavky a řadou norem pro informační bezpečnost. Výsledkem práce je aplikování získaných poznatků na společnosti Ferrit s.r.o., kde bylo provedeno zhodnocení a popsání veškerých oblastí informační bezpečnosti a navrhnutí nových poznatků k zlepšení informační bezpečnosti ve společnosti.

ABSTRACT

This bachelor's thesis deals with the issue of information security, relevant legislative requirements and a number of information security standards. The result of the thesis is the application of the acquired knowledge to a company Ferrit. In Ferrit, all areas of information security were evaluated and described. New findings to improve information security in society were proposed.

KLÍČOVÁ SLOVA

informační bezpečnost, přístup k informační bezpečnosti, legislativní požadavky, bezpečnostní normy, zavádění bezpečnostních opatření, rizika a opatření

KEYWORDS

information security, access to information security, legislative requirements, safety standards, introduction of security features, risks and measures

BIBLIOGRAFICKÁ CITACE

FIALÍK, Tomáš. *Informační bezpečnost ve strojírenství* [online]. Brno, 2020 [cit. 2020-06-14]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/125239. Bakalářská práce. Vysoké učení technické v Brně, Fakulta strojního inženýrství, Ústav výrobních strojů, systémů a robotiky. Vedoucí práce Jana Rozehnalová.

PODĚKOVÁNÍ

Rád bych poděkoval mému vedoucímu bakalářské práce Ing. Janě Rozehnalové, M.Sc. za její čas a odborné vedení při zpracování této bakalářské práce. Děkuji také společnosti Ferrit s.r.o. a hlavně IT oddělení, které mi umožnilo realizovat tuhle práci.

ČESTNÉ PROHLÁŠ ENÍ

Prohlašuji, že tato práce je mým původním dílem, zpracoval jsem ji samostatně pod vedením Ing. Jany Rozehnalové, M.Sc. a s použitím literatury uvedené v seznamu.

V Brně dne 25. 6. 2020 ……

Tomáš Fialík

OBSAH

1 ÚVOD

Současný svět a především doba se dá označit za dobu informační. Firmy po celém světě využívají stroje, počítače a další nezbytná zařízení využívající výpočetní technologie a přenosu dat pro dosáhnutí co nejlepšího produktu nebo služby. Právě tahle data jsou mnohdy tím nejdůležitějším a nejcennějším aktivem, jak pro jednotlivce, tak pro firmy. S rostoucím objemem dat přibývá i množství hrozeb, ať už se jedná o útoky, neúmyslné chyby zaměstnanců nebo nepředvídatelnou přírodu. Tyhle aspekty můžou mít až ničivý dopad na životaschopnost společnosti.

Z těchto důvodů nabírá informační bezpečnost čím dál více na důležitosti, jelikož lidé si začali uvědomovat jakou cenu data, know-how a informace mají. Dříve informační bezpečnost byla výsadou hlavně velkých korporací. To už dneska ale neplatí. Informační bezpečnost se rozšířila až k těm nejmenším firmám.

Ve světě je spousta standardů a přístupů k informační bezpečnosti. Nejznámějším standardem (normou) pro Evropu je řada norem ISO/IEC 27000. Celosvětově pak můžeme jmenovat dva základní přístupy k řízení informační bezpečnosti ITIL a COBBIT.

Zavedením rozumné informační bezpečnosti ve firmě se může předejít nejen ztrátě důležitých informací, ale zároveň to může vést k získání nových obchodních partnerů. Daná společnost tím ukazuje stávajícím i budoucím obchodním partnerům, že se jedná o důvěryhodnou společnost.

Cílem této bakalářské práce je pospat aktuální stav a trendy v informační bezpečnosti, popsat legislativní požadavky EU a ČR. Udělat rešerši norem k dané problematice. Provést systematický rozbor a zhodnotit informační bezpečnost v dané firmě a navrhnout vlastní doporučení pro rozvoj informační bezpečnosti v daném podniku.

2 ÚVOD K PROBLEMATICE INFORMAČNÍ BEZPEČNOSTI

Bezpečnost informace jde ruku v ruce s informační bezpečností. Zdálo by se, že se jedná o totéž, ale není tomu tak. Pojem informační bezpečnosti staví na definici bezpečné informace, tedy takové, jejíž důvěrnost, integrita a dostupnost jsou zachovány. Inherence těchto vlastností tvoří základ informace o různé váze její hodnoty, především obsahu pro odesílatele i příjemce. Důvěrnost značí jistotu, že informace jsou přístupné pouze oprávněným osobám, integrita pak garantuje správnost a celistvost neseného obsahu a dostupnost pak vyjadřuje použitelnost informace pro uživatele v okamžiku potřeby.

Evropské i americké pojetí bezpečnosti informací si jsou blízké a posuzování shody s požadavky se stalo součástí nadnárodních akreditačních a certifikačních schémat. Stabilizaci jistě napomáhá také vývoj v oblasti systémů zajištění jakosti. Po přibližně třiceti letech opět vystupuje do popředí myšlenka integrovaného, dříve komplexního, řízení firem. Spojení analogických požadavků a návodů pro oblasti životního prostředí, zajištění kvality, technické bezpečnosti, obecné bezpečnosti, ochrany zdraví a také informační bezpečnosti je na pořadu dne při aktualizaci norem řady ISO 9000. [5]

2.1 Co je bezpečnost a ochrana informací?

Informační bezpečnost je souhrnné označení pro všechny aktivity směřující k ochraně informací. Jejich cílem je zejména zabránění negativním událostem jako je jejich ztráta, odcizení, únik, zneužití, zničení, narušení či změny.

Důležitost bezpečnosti a ochrany informací roste zároveň s jejich důležitostí. Informace mají cenu jen, pokud se dají použít. To platí jak z pohledu firmy, která chce své informace chránit, tak ale i z pohledu útočníka. Informace jsou jeden z klíčových zdrojů organizace. Bezcenná informace ale nikoho nezajímá, bezcennou informaci nemusíme chránit.

Aby mohly být informace využité, musí být k dispozici dostupným způsobem těm správným lidem. Informace jsou chráněny tehdy, pokud je zabráněno jejich ztrátě.

Informace mohou existovat v různé podobě. Nejčastěji jsou v nějaké podobě dat (souborů, obrázků, videa a podobně), ale také informace může být obsah toho, co říkáme jinému člověku, co předáváme ústně. Pokud je to něco důležitého a cenného, chráníme takto sdělovanou informaci stejně důsledně, jako byla někde zapsaná. Pokud o ně přijdeme nebo naše klíčové informace získá konkurence, může to také znamenat konec našeho podnikání nebo fungování. O informace můžeme přijít v místě uložení (na svém počítači, na serveru nebo v šanonu) nebo někde po cestě k nám (na počítačové síti nebo také když někdo nese kus papíru k nám). [6]

2.2 Co se může s informacemi stát? Co znamená o ně přijít? Jaké problémové situace mohou nastat?

S informacemi se nám může přihodit celá řada nepříjemností. Začněme těmi, kterým se dá snadněji předcházet a které jsou způsobeny často jen nepozorností či nedbalostí.

Ztráta informací je nejběžnější. O informace můžeme přijít při celé řadě situací - smažeme si disk, disk přestane fungovat, utopíme svůj telefon, vyhodíme důležitý papír nebo zapomeneme, kam jsme si ho uložili, či zapomeneme své heslo. To znamená, že informaci nemáme my ani nikdo jiný. Prostě přestala existovat. Od takové situace nás zachrání to, že informace existuje na více místech. Jinými slovy existuje její záloha. Ztráta nemusí být úplná, ale může být jen částečná. To znamená, že přijdeme jen o část informace nebo dat (dojde k porušení tzv. celistvosti).

Nedostupnost informací znamená, že k datům nemáme přístup, není nám dostupné místo jejich uložení (např. nefunguje síť, ztratili jsme klíč nebo někdo jiný přístup zamkl). Pomoci nám může více cest ke zdroji informací nebo opět zálohování. To pomůže například i v situaci, když je nedostupnost způsobená vydíráním (tzv. ransomware).

To jsou situace, kde až na výjimku s ransomware o informace přijdeme, ale nemá je nikdo jiný. Tím se dostáváme k situacím, které jsou z pohledu ochrany informací ještě citlivější a jsou způsobeny aktivitami někoho dalšího - útočníka nebo zloděje.

Odcizení dat nebo informací znamená, že data má někdo jiný. V lepším případě, pokud máme data zálohována, nám zůstanou. V horším případě o informace přijdeme, a ještě navíc je má někdo jiný. Otázkou zůstává, zdali zloděj data zneužije a jak.

Ke zneužití dat nebo informací může dojít v případě odcizení nebo aktivního napadení. V takové situaci sice o informace nepřijdeme, ale jejich hodnota se ve chvíli odcizení může zcela ztratit, neboť cennou informaci má někdo jiný. [6]

2.3 Co tedy dělat pro bezpečnost a ochranu informací a dat?

Všechny důležité informace by měly být v rámci firmy ukládány a přenášeny tak, abychom zabránili všem možným negativním událostem a situacím, jako jsou ztráta informací, jejich odcizení, únik, zneužití, zničení, narušení nebo nechtěné změny. Všechny informace ve firmě ale nelze chránit stejným způsobem a ani by to nemělo význam. Abychom odlišili, které informace chránit a jak silně, je možné rozlišovat různé stupně důvěrnosti - od veřejně dostupných až po ty důvěrné. K tomu se v praxi používají různé klasifikace důvěrnosti informací.

Informace, které firma označí jako chráněné či důvěrné pak chrání a ukládá přiměřeně bezpečným způsobem. Tedy tak, aby nemohlo dojít k jejich ztrátě, nedostupnosti, odcizení nebo zneužití. Je jedno, jestli jsou uložené v elektronické podobě, v papírech nebo v hlavách lidí. Rizika úniku či zneužití informací hrozí nejen z okolního prostředí, ale zejména zevnitř organizace samotné. Je tedy třeba myslet i na to, aby v organizaci samotné existovala pravidla, kdo může k jakým datům přistupovat a proč.

Informační bezpečnost pokrývá kompletně všechny oblasti ukládání či přenosu informací, ať jsou v psané, mluvené či v digitální podobě. Tedy včetně ochrany proti odposlechu či dezinformacím. Lidé a metodiky z oblasti řízení bezpečnosti hovoří o ochraně informací a dat jako o zabránění jakéhokoliv porušení celistvosti, důvěrnosti nebo dostupnosti, které může mít pro organizaci nějaké negativní důsledky. [6]

2.4 Ochrana informací na organizační úrovni

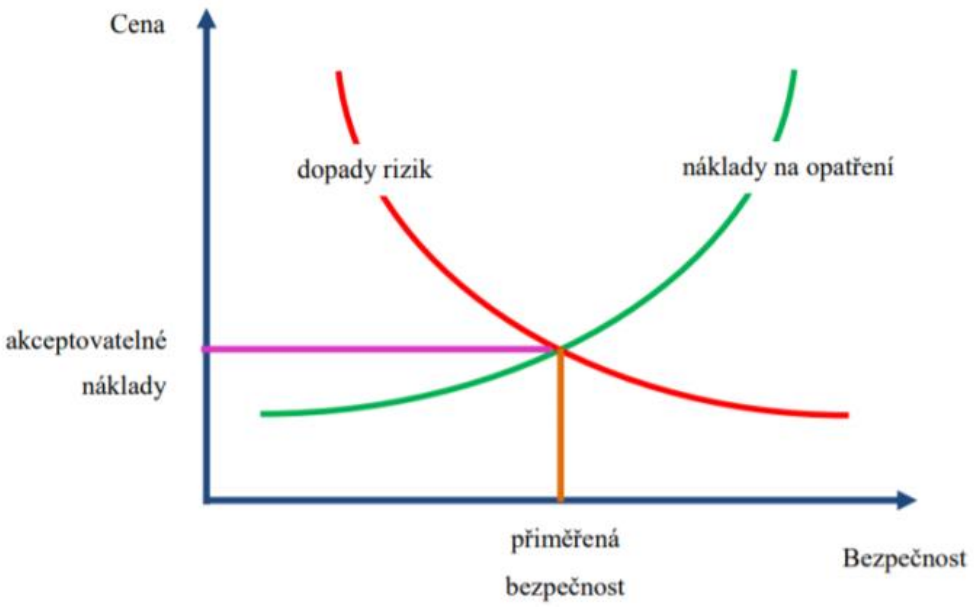
Organizační opatření jsou určitě základem ochrany informací. Je to jednak již zmiňované řízení oprávnění - tedy definice toho, kdo má k čemu přístup a proč. To je součástí pracovních náplní, oprávnění a pravomocí jednotlivých pracovníků. Mezi další organizační opatření patří zavázání mlčenlivosti lidí, kteří důvěrné informace mají, znají nebo s nimi mohou přijít do styku. Mohou to být pracovníci firmy nebo jiní obchodní partneři. Organizační metody spočívají především ve smlouvách - smluvním zavázání mlčenlivosti (např. v pracovní smlouvě, pomocí konkurenční doložky nebo pomocí NDA). Dalším významným nástrojem organizační ochrany dat je vzdělávání. Zvyšování gramotnosti v oblasti bezpečnosti informací lze zabránit mnoha nepříjemným situacím a únikům informací nebo dat, které jsou způsobené prostou neznalostí. [6]

2.5 Ochrana informací na technologické úrovni

Technologicky lze chránit jak důležité informace, které jsou někde ukládány (v počítači nebo ve skříni) ale také například lidskou komunikaci (například sdělování důvěrných informací po telefonu lze technologicky chránit proti odposlechu). V praxi se ochrana informací a dat rozděluje na tzv. fyzickou bezpečnost (ochrana budov a zařízení, zámky ve dveřích, kamerový systém a podobně) a na počítačovou bezpečnost, která má na starosti ochranu informačních technologií a IT infrastruktury. [6]

2.6 Přiměřená bezpečnost

Časová a investiční náročnost projektů na zabezpečení informace musí být pro podnik či instituci přijatelná a musí odpovídat hodnotě chráněných aktiv. Parametry poměrů by měly být stanoveny pomocí bezpečnostní politiky organizace.



Obr. 1) Graf přiměřené bezpečnosti při akceptovatelných nákladech [3]

2.7 ISO/OSI model

V současnosti nejspíš nejpoužívanějším standardem v počítačových sítích. Byl přijat v roce 1979 jako norma standardizační organizace ISO. Tento model se skládá ze sedmi vrstev viz. obrázek. Jednotlivé vrstvy jsou:

Fyzická vrstva

Nejnižší vrstva RM ISO/OSI zprostředkovává fyzický přenos dat v podobě bitů mezi odesílatelem a příjemcem. Řeší se zde především technické parametry, jako jsou elektrické signály definující 0 a 1, typy konektorů, druhy kabelů apod. Nezajímá se o význam jednotlivých bitů, jen je posílá dál. Zabývá se také kódováním, modulací a synchronizací přenosu dat.

Linková vrstva

Tato vrstva bývá také označována jako spojová nebo vrstva datového spoje. Data jsou zde spojována do tzv. rámců o velikosti několik stovek bajtů. Linková vrstva musí poznat začátek a konec rámce, kontroluje jejich správnost pomocí CRC kontrolních součtů.

Další vlastností linkové vrstvy je tzv. řízení toku, kterým se rozumí řízení rychlosti přenosu tak, aby příjemce stíhal rámce zpracovávat.

Linková vrstva zajišťuje přenos pouze u přímého spojení a tudíž i adresy na úrovni linkové vrstvy jsou jednorozměrové bez dalšího logického členění.

Bezpečnost je na úrovni Point-to-Point komunikace, takže mezi dvěma sousedícími účastníky. Využívají se bezpečnostní protokoly jako: CHAP, PAP, PPTP atd.

Síťová vrstva

Využívá tzv. směrování k přenášení dat dále než k sousedním uzlům. Data jsou zde členěna do tzv. packetů. Na rozdíl od rámců složených ze záhlaví, dat a patičky využívajících tzv. MAC adresu odesílatele a příjemce je packet blok dat s hlavičkou na úrovni síťové a vyšší vrstvy a jako adresy jsou zde používány IP adresy obou koncových účastníků a také informace o potvrzování nebo o řízení toku.

Bezpečnostní protokoly: GRE, IPsec, AH, ESP atd.

Transportní vrstva

Zabývá se rozdělením balíku odesílaných dat do packetů, které pak síťová vrstva posílá směrem k příjemci nebo naopak k sestavení došlých packetů opět dohromady. Jedním z jejich úkolů je vyrovnávat rozdíly mezi síťově orientovanými třemi spodními vrstvami a aplikačně orientovanými třemi vyššími. Umí rozpoznávat chyby a někdy je i dokonce opravovat.

Relační vrstva

Tato vrstva se tedy stará o operace během doby, po kterou spolu uzly komunikují, jako je navázání, řízení a rušení spojení, rozhodování o jaké spojení půjde, a také rozhoduje o tom, zda bude použit šifrovaný přenos dat.

Bezpečnost je tu zaměřena na libovolné aplikace pomocí protokolů SSL nebo TLS.

Prezentační vrstva

Překládá data z nejvyšší aplikační vrstvy tak, aby byla srozumitelná všem nižším vrstvám a naopak na straně příjemce je převádí do formátu takového, aby je cílová stanice dovedla rozpoznat a předat dané aplikaci. Zabývá se tedy kompresí a kódováním dat, protože

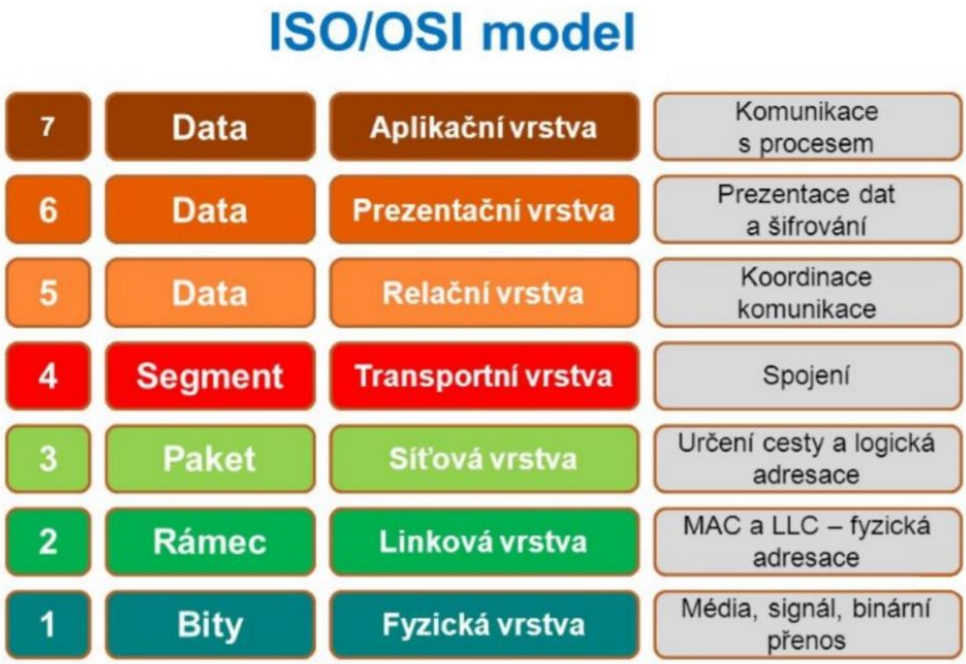
k jedné a téže posloupnosti bitů může jedna aplikace nahlížet jinak než aplikace druhá právě díky např. rozdílnému kódování znaků.

Bezpečnost je tu zaměřena na libovolné aplikace pomocí protokolů SSL nebo TLS.

Aplikační vrstva

Tato nejvyšší vrstva má za úkol poskytování služeb aplikacím. Ze samostatných aplikací jsou zde zahrnuty jen ty součásti, které mají cenu standardizovat. Příkladem služby aplikační vrstvy jsou mechanismy pro přenos elektronické pošty.

Bezpečnost řeší už každá aplikace samostatně. Využívají se bezpečnostní protokoly SSH, SCP, SFTP HTTPS atd. [7]



Obr. 2) Model ISO/OSI [4]

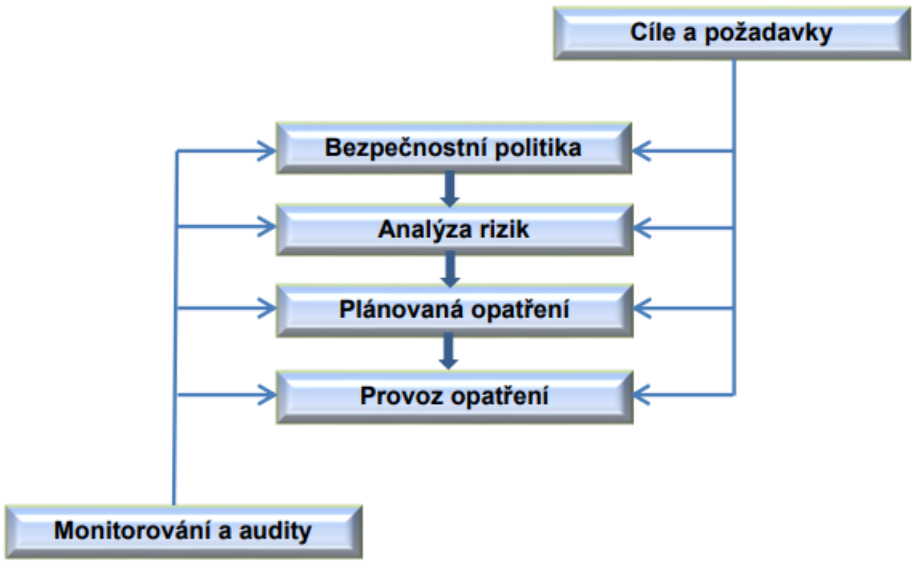
2.8 Mezinárodně uznávané přístupy k řízení informační bezpečnosti

2.8.1 ITIL

Information Technology Infrastructure Library (ITIL) je vymezení přístupů k aplikaci IT služeb na potřebné úrovni při přijatelných nákladech. Jak již vyplývá ze zkratky jedná se o „knihovnu“, která obsahuje souhrn sumarizovaných podkladů IT bezpečnosti. ITIL je šířen formou publikací, CD, školení, konzultací a má rozvinutou sadu osobních kvalifikací a certifikací. ITIL vychází z nejlepších zkušeností (je vlastně souhrnem nejlepších zkušeností), představuje rámec pro zvládnutí řízení IT v organizaci, pojednává komplexně o IT službách a zaměřuje se na neustálé měření a zlepšování kvality dodávaných služeb IT, a to jak z pohledu businessu, tak z pohledu zákazníka. Toto zaměření je hlavní příčinou celosvětového úspěchu ITIL a přispělo k rozšířenému využití a ke klíčovým přínosům získaným u těch organizací, které aplikovaly tyto techniky a procesy ve svých strukturách. [8]

ITIL není norma ani metodika, ITIL obsahuje doporučení a nejlepší praktiky. ITIL obsahuje nebo popisuje:

- definování procesů potřebných pro zajištění ITSM
  - stanovení cílů, vstupů, výstupů a aktiv každého procesu
  - stanovení rolí a jejich odpovědnostní v daném procesu
  - způsob měření kvality poskytovaných IT služeb a účinnosti ITSM procesů
  - vzájemné vazby mezi jednotlivými procesy
- zásady pro implementaci procesů ITSM
  - přínos každého procesu Critical Success Factors, možné problémy a vhodná opatření
  - náklady na implementaci a následné provoz
  - zásady pro řízení podpůrné ICT infrastruktury
  - zásady bezpečnosti ICT infrastruktury [1]



Obr. 3) Základní procesy řízení bezpečnosti informací dle ITIL [1]

2.8.2 COBIT (Control Objectives for Information and related Technology)

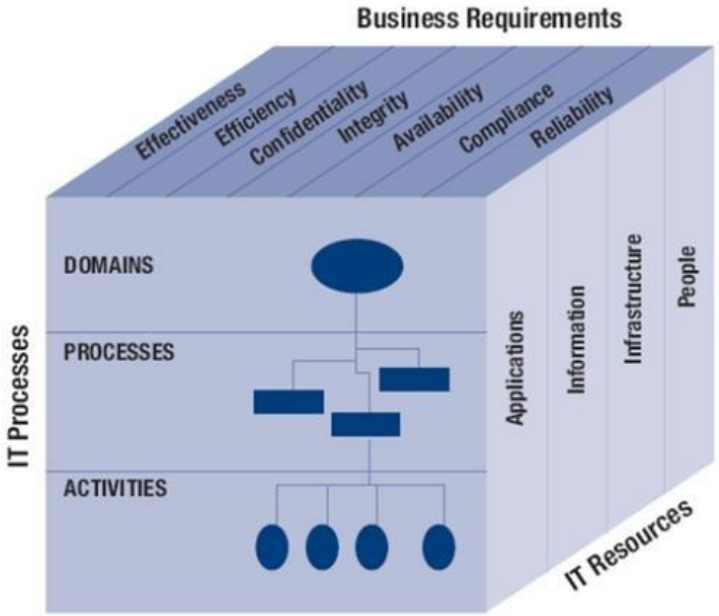
Je rámec nejlepších praktik pro řízení informatiky. Je to soubor nejlepších praktik a postupů, které pomáhají organizaci dosáhnout strategických cílů pomocí efektivního využití dostupných zdrojů a minimalizaci IT rizik. COBIT vzájemně propojuje řízení podniku, řízení a správu informatiky. Toto propojení je realizováno propojením podnikových a IT cílů, definováním metrik a modelů zralosti pro měření cílů a definováním odpovědností vlastníků podniku a IT procesů.

První verze COBIT byla vydána organizací ISACA v roce 1996. První vydání tvořilo rámec, druhé vydání bylo rozšířeno o auditní postupy, sadu implementačních nástrojů a rozpracované procesy kontroly, třetí vydání bylo rozšířeno o manažerské postupy. Třetí vydání COBIT bylo již vydáno institutem ITGI (IT Governance Institute) stejně jako verze COBIT 4.

Aktuální je verze COBIT 5, která konsoliduje a integruje rámce COBIT 4.1, Val IT 2.0 and Risk IT a významně obsahuje rysy modelu BMIS (Business Model for Information Security) a ITAF.

COBIT definuje procesy IT rozdělené do 4 domén:

- plánování a organizace
- akvizice a implementace
- dodávka a podpora
- monitoring a evaluace [9]



Obr. 4) Kostka COBIT [1]

2.9 Základní pojmy

Tato část má za úkol vymezit některé základní pojmy zmiňované v dalších teoretických východiscích práce.

Dostupnost

Zajištění přístupnosti k informaci oprávněnému uživateli v požadovaný okamžik. [1]

Důvěrnost

Zajištění přístupnosti k informaci pouze oprávněnému uživateli. [1]

Integrita

Zajištění správnosti a úplnosti informace. [1]

Aktivum

Je veškerý hmotný a nehmotný majetek. [1]

Hrozba

Je událost ohrožující bezpečnost. [1]

Zranitelnost

Slabé místo aktiva. [1]

Riziko

Je kombinace hrozby a zranitelnosti s dopadem na aktivum. [1]

Dopad

Je vznik škody v důsledku působení hrozby. [1]

Informace

Širší pojem popisující reálné prostředí, jeho stav a procesy v něm probíhající ve formě údajů. Množství informací je rozdíl mezi neurčitosti(entropií) informace (nebo stavu) před a po zprávě. V informatice tvoří informaci kódovaná data (kódováním není myšleno kryptování, ale fyzikální interpretace v úložném zařízení nebo na přenosném disku). [1]

Data

Jsou „plněním“ informace, kterou vytváří. Data je opakovaně interpretovatelná formalizovaná podoba informace vhodná pro komunikaci, vyhodnocování nebo zpracování. [1]

Přenos dat

Přenos dat nebo digitální komunikace je přenos digitálních zpráv nebo digitalizovaného analogového signálu pomocí fyzického dvoubodového nebo vícebodového přenosového prostředí, kterým může být metalický kabel nebo bezdrátový přenos. [1]

Signál

Je fyzikální vyjádření informace ve formě změn fyzikální veličiny v čase. [1]

Informační systém

Přesná definice neexistuje minimálně z důvodu rozmanitosti terminologie. IS lze chápat jako systém vzájemně propojených informací a procesů, které s těmito informacemi pracují. [1]

Bezpečnost informací

Řeší ochranu informací a dostupnost informací. Je ve vzájemném vztahu s pojmy bezpečnost organizace a bezpečnost IS/ICT. [1]

3 SOUČASNÝ STAV A TRENDY V NADCHÁZEJÍCÍCH LETECH V OBLASTI INFORMAČNÍ BEZPEČNOSTI

3.1 Technický a technologický výhled 2020 – 2030

Překotný technický a technologický vývoj způsobuje, že už se tolik nestává, aby se nová technologie udržela na výsluní delší dobu. Ve většině případů se rychle stane běžnou a vytvoří základ pro technologii modernější. Předpovídat proto budoucnost IT není vůbec jednoduché. Nicméně s rokem 2020 vstupujeme do desetiletí, které určitě naplní naše představy o „budoucnosti".

Aby si v tomto roce i v těch následujících, firmy vůbec udržely své místo na trhu, budou muset pomalu začít přemýšlet o digitální transformaci. Dá se předpokládat, že každým rokem podniky s digitální infrastrukturou budou zastupovat čím dál větší procento v globálním HDP.

Pro představu, kam se ubírá vývoj IT, uvedu přehled technologií a směrů s největším potenciálem růstu a rozvoje, které zároveň mají dopad do podnikových IT struktur a jejich zabezpečení.

3.1.1 Internet věcí (IoT)

Dnes připadá na jednoho člověka asi čtyři zařízení internetu věcí. V roce 2030 se předpokládá, že to bude už okolo 15 zařízení. Jedná se například o chytré spotřebiče, čidla, senzory, automobily, regulace, chytré domy. Tato zařízení lze vzájemné propojovat a jednoduše ovládat z jednoho místa (mobil, PC). Jak roste oblíbenost těchto zařízení, roste i hrozba úniku informací. Tyto zařízení mají jeden velký nedostatek – nedostatečné zabezpečení ze stran výrobců.

3.1.2 5G mobilní sítě

Podobně jako revoluční byl pro využívání mobilních dat přechod z 3G na 4G síť, bude přechod na 5G malou revolucí na poli mobilních aplikací a rozvoji „chytrého průmyslu" (Průmysl 4.0). Co tedy sítě 5G přinesou? Měly přinést skokově rapidní zvýšení přenosové rychlosti dat a mnohem nižší odezvu. Ta umožní rozvoj moderních technologií, které jsou limitované právě nízkou přenosovou rychlostí a nedostatečnou odezvou. Na poli průmyslu se očekává rozmach internetu věcí (IoT), umělé inteligence a v neposlední řadě také rozvoj samořiditelných aut.

Negativa 5G sítě – nic není zadarmo a zde to platí mnohonásobně. Budování celé infrastruktury přijde velice draho. Na rozdíl od 4G je signál 5G sítí méně vhodný k přenosu na velké vzdálenosti nebo skrze překážky jako např. zdi budov. To znamená, že síť vysílačů bude muset být mnohem hustší a tedy i nákladnější. Otazník visí také nad tím nejdůležitějším – zabezpečením 5G sítě. Pochybnosti jsou okolo předního výrobce zařízení pro 5G čínské firmy Huawei. Další dva významní výrobci – Nokia a Ericsson nevzbuzují bezpečnostní obavy, ale technicky za firmou Huawei mírně zaostávají.

Velký ekonomický potenciál brzdí obavy z bezpečnosti, která bude rozhodující. Ve chvíli, kdy by 5G měla mít vážné bezpečnostní mezery, může to mít velmi negativní dopady. Hlavně proto, že o tuto technologii by se měla opírat samořiditelná auta, obsáhlé cloudové databáze s citlivými údaji nebo zdravotní technika. Na druhou stranu je zde nezměrný potenciál pro spojení 5G a cloudových aplikací. Tohle spojení by mohlo svět technologií posunout výrazně vpřed.

3.1.3 Cloudová řešení (Cloud computing)

Cloud computing je důležitou technologií pro digitální transformaci firem. Budování vlastních datacenter a infrastruktur je nákladné a hodí se více pro rozsáhlé projekty. Pro střední a malé firmy, živnostníky i jednotlivce je už nějakou dobu cloud computing ideálním řešením. Poskytuje jim podmínky, které by si jinak dovolit nemohli. Výkon i kapacita jsou dnes plně škálovatelné přesně podle požadavků a dají se operativně měnit dle aktuálních potřeb. Navíc poskytovatelé cloudu přebírají odpovědnost za hardwarové a softwarové upgrady, zabezpečení uložených dat, zálohování atd. Cloudové služby jsou privátní i veřejné. Na vzestupu jsou hybridní cloudy umožňující sdílení dat mezi veřejným a privátním cloudem, flexibilnější práci s daty a jejich rozdělení podle citlivosti na zabezpečení. Pro volbu cloudového řešení je důležité nejen poskytovaný prostor, výkon a cena, ale především komplexnost služby a její bezpečnost. Poměrně hodně se rozvíjí i distribuovaný cloud (Distributed cloud) – jde o distribuci (rozložení) veřejných cloudových služeb do různých lokalit, přičemž původní poskytovatel služby je odpovědný za provoz, aktualizace a dohled. Jde o zásadní posun od klasického centralizovaného modelu většiny cloudových služeb, který nastartuje novou éru cloud computingu.

S rozvojem cloudu jde roku v ruce i Saas (software jako služba), kdy si jej pouze pronajímáte od poskytovatele a v cloudu provozujete. Další formy služeb spojených s cloudem jsou PaaS (Platform as a Service) a Iaas (Infrastructure as a Service). U Paas si zákazník pronajímá celou platformu služeb, které využívá včetně např. vlastního software a odpadá mu starost o infrastrukturu. U Iaas se pronajímá celá infrastruktura, kdy se zákazník nechce starat o hardwarovou stránku věci. Je to nákladné a ne tolik úsporné řešení, na druhou stranu má největší kontrolu nad svými daty.

3.1.4 Virtuální asistentky a rozšířená realita

V roce 2019 byly virtuální asistentky/ti na vzestupu. Alexa od Amazonu, Google Home, Siri od Applu a Cortana od Microsoftu všechny posilují, protože se technologie naučily ulehčit každodenní činnosti. A ty samé technologie si nevyhnutelně začnou hledat cestu do firem. Uživatelé začnou v práci očekávat stejnou úroveň technologické podpory v obchodním prostředí jakou mají k dispozici doma. Zejména u poskytovatelů náročných technologií bude tato podpora nejen očekávána, ale vyžadována.

Kontakt se zákazníkem je pro firmy klíčový a vyžaduje spoustu času od zaměstnanců. To je pro firmy nákladné, a proto spousta menších i velkých podniků sahá po chatbotech, jejichž hlavní funkcí je simulovat konverzaci s lidmi. Chatbot není novinkou v oblasti technologií, ale za léta dospěl a s využitím strojového učení je mnohem inteligentnější, zvládne až 85 % komunikace se zákazníkem. Jeho potenciál se přesto dále rozrůstá.

Rozšířená realita (AR, z angl. augmented reality) kombinuje reálný svět s digitálními prvky. Své využití má rozšířená realita např. ve zdravotnictví. S její pomocí se v chirurgii tvoří obrázky mozku a piloti vybaveni přilbami podporujícími AR mají přehled o své nadmořské výšce a rychlosti. Velký potenciál má ve výcviku či vzdělávání. Na rozdíl od AR se VR (virtual reality) tolik nerozšiřuje. Je to dáno především náročností a cenou potřebného hardware.

3.1.5 Blockchain

Přináší potenciál změnit celá odvětví v digitální důvěry, transparentnosti a výměny hodnot. Není jen spjat s Bitcoinem. Bitcoin používá blockchain jako svůj základ. Potenciál blockchainu verifikovat prakticky cokoli hodnotného je téměř neomezený. Je možné sledovat data až k jejich původu, omezit možnost výměny dat za kopie, náhražky či falza. Bude jej možno nasadit, kde je třeba dohledatelnost potravinářství, letecký průmysl, pro dosledování původu náhradních dílů atp. Lze jej též nasadit jako správce identit a integrovat do chytrých dokumentů. Zatím není pro podniková nasazení dostatečně vyspělý, ale jeho potenciál je skoro revoluční.

3.2 Kyberbezpečnost – AI

Jedná se o velké téma dotýkající se téměř každé technologie. Tak jak se vyvíjí a zdokonalují technologie, zdokonalují se i techniky kyberzločinců, kteří budou vyhledávat zranitelnosti jakýchkoliv nových technologií. Musíme očekávat, že se objeví mnohé útoky a odhalí zranitelná místa. Odpovědí musí být předvídavý a aktivní přístup a systematizace procesů, aby byly včas instalovány záplaty a aktualizace.

Všeobecné útoky jsou minulostí. Množí se cílené útoky za pomoci ransomwaru (software blokující počítačový systém, data nebo celou infrastrukturu), který slouží k vydírání oběti – nazývá se cílený ransomware. Moderní útoky budou probíhat sofistikovaněji a mnohdy se budou soustředit na celé infrastruktury. Další nebezpečí bude plynout z pishingových útoků, adware, spamu atd.

Umělá inteligence a strojové učení budou postupně využívány ve stále širší míře a oblastech. Její využití se rozhodně najde i v kybernetické bezpečnosti. Stěžejní role budou ochrana systémů na bázi AI, využívání AI pro zlepšení kybernetické ochrany a obrany a očekávání útoků využívajících AI.

Než však AI dosáhne svého reálného nasazení anebo alespoň použitelnosti, bude suplujícím trendem model „Nulové důvěry“ (Zero trust), který představuje postoj IT „Nikomu nedůvěřuj, vše prověřuj“. Přístupy k systémům bude možné získat pouze explicitním povolením pro jednotlivé uživatele či procesy.

Aktivní vyhledávání hrozeb bude vedle holistických bezpečnostních strategií hrát stále důležitější roli. Standardní přístupy reagují na varování, které je výsledkem detekování potenciálně škodlivé aktivity. Aktivní vyhledávání jde nad tento rámec známých nebezpečí a analyzuje dosud neznámé. Cílem je nalezení nových a neznámých škodlivých softwarů a zranitelností. I když zrovna nenaleznou škodlivý SW, často detekují zranitelnost, které pak generují přísnější pravidla a vedou k omezení prostoru pro nové útoky.

3.2.1 WEB-SECURITY

S příchodem rozhraní WEB 2.0 se změnily i bezpečnostní rizika spojené s obsahem WEB stránek. Sociální sítě a aplikace WEB 2.0 a WEB 3.0 jsou všudypřítomné a do základů mění způsob, jakým na internetu pracujeme. Zároveň jsou novými vstupními body pro hrozby, porušování pravidel a ztrátu dat. Tradiční technologie jako ANTIVIRUS, hodnocení reputace web stránek nebo filtrace URL adres dnes již nedostačují. Proto se bezpečnostní řešení zaměřují na:

- identifikace uživatele – nejen podle IP adres, ale i dalších ID
- kontroly obsahu – přehled nad tokem přicházejících dat – analýza
- filtrování URL – real time bezpečnostní monitoring, kontrola produktivity uživatelů
- ochrana proti malware – antivir k zachycení červů hned na vstupní internetové bráně
- DLP – prevence a kontrola proti úniku citlivých dat
- Remote User Protection – přístup na web pro vzdálené uživatele na ochranu proti útokům s firemním zabezpečením
- Sandbox – služba, která poskytuje detailní forenzní analýzu neznámého malware v bezpečném Sandbox prostředí
- Reporting – přehledný reportovací nástroj

3.3 Trendy v IT bezpečnosti

Obecně platí, že štěstí přeje připraveným. Ať už se bude vývoj IT technologií ubírat jakýmkoliv směrem podstatné pro zabezpečení jakýchkoliv IT procesů bude:

- dostatek relevantních informací
- nasazení adekvátní kombinace HW a SW řešení na ochranu dat a sítového provozu
- udržování veškerých systémů v aktuálním stavu a aplikace všech bezpečnostních záplat
- dodržovaní stanovených bezpečnostních zásad, postupů a jejich pravidelná aktualizace
- předvídavost a prevence.

Jak jsem nastínil již v předešlé kapitole, mezi hlavní trendy v IT bezpečnosti bude patřit model nulové důvěry – Zero tolerance (dále jen ZT), jehož principy jsou popsány tamtéž. Znovu uvedu ty nejdůležitější:

- data a aplikace jsou přístupná pouze autorizovaným a ověřeným uživatelům
- provoz na bázi uživatel, lokalita, aplikace
- vše je prověřováno a plně logováno

K nasazení ZT se využívá nových nástrojů jako je mikrosegmentace, SDN, Network virtualization, Blockchain.

3.3.1 Mikrosegmentace

Segmentace sítě není novinkou. Firmy využívají firewally, virtuální lokální sítě (VLAN) a seznamy řízení přístupu (ACL) pro segmentaci sítě již léta. Při mikrosegmentaci se zásady uplatňují na individuální pracovní zátěže pro zajištění větší odolnosti vůči útokům. VLAN umožňuje hrubozrnnou segmentaci a mikrosegmentace jde hlouběji. Kdekoliv je potřeba, zajistí detailní rozdělení přenosů a oddělí jednotlivé síťové komunikace v nezávislé skupiny.

3.3.2 SDN

Je to přístup k architektuře sítě, který se snaží využít abstrakce k správě síťové funkcionality. Logické topologie – struktury sítě se dosahuje pomocí programování virtuálních komponent. Principem je oddělení rozhodovací části (control plane) síťového prvku od té vykonávající směrovací či přepínací činnost (data plane).

3.3.3 NFV (Network function virtualization)

Podstatou virtualizovaných funkcí sítě je nebýt závislý na specifickém hardwaru, protože ten je drahý. Proto ve své síti chceme opustit fyzická zařízení jako load balancery, firewally, IDSky, IPSky, VPN koncentrátory, atd. a všechno mít jako virtuální stroje v datacentru. S NFV přišli telekomunikační poskytovatelé služeb, u kterých existovalo velké množství různých proprietárních hardwarových boxů. Z dnešního enterprise pohledu je mít vše spíše softwarově běžné.

Aby IT manager nevyhledával v zahlceném internetovém prostředí novinky o hrozbách, začaly fungovat expertní služby poskytující vytřízené informace přesně podle potřeb a odvětví ve které IT technik pracuje. Moderní služby, které slouží za povšimnutí:

Security managemet Center

Služba Security Management Center (SMC) přináší do praxe koncept GRC (Governance, Risk Management and Compliance). Tato koncepce je unikátní tím, že spojuje informace technické bezpečnosti (např. výstupy ze SIEM) a procesní bezpečnosti (např. analýzu rizik) a díky analytickým nástrojům umožňuje správné určení priorit a efektivní zacílení zdrojů. Stav bezpečnosti po zavedení SMC je analyzován a prezentován pomocí kvantitativních finančních metrik. V praxi lze vidět finanční přínosy či ztráty, které stojí za každým bezpečnostním rozhodnutím. SMC dokáže data analyzovat a následně vizualizovat tak, aby výsledkům rozuměli nejen odborníci v oblasti IT či bezpečnosti, ale aby se v nich orientovalo i samotné vedení společnosti. Vysokou přidanou hodnotu a zásadní konkurenční rozdíl tvoří podpora odbornými konzultanty a prvky bezpečnostní heuristiky umožňující provádět správná rozhodnutí i za situace, kdy některé klíčové informace chybí. [11]

ThreatGuard

Vyhledává, analyzuje a monitoruje aktuální bezpečnostní hrozby a identifikuje reálná rizika a jejich kritičnost pro vaše firemní prostředí. Získává se tím včasný a aktuální přehled o nejnovějších kybernetických hrozbách pro vaši IT infrastrukturu včetně doporučení, jak se bránit. Služba nabízí zajímavé benefity v podobě:

- aktivní filtry podle zájmových oblastí
- customizované notifikace
- relevantní informace
- odfiltrovává zbytečný informační šum
- přesně definuje a popíše problém
- identifikuje nápravu
- zpracuje a případně otestuje opatření
- poskytuje individuální konzultace [12]

3.3.4 NETWORK-MONITORING

Sledování počítačové sítě se skládá ze dvou základních částí:

Monitoring provozu – je použití systému který nepřetržitě sleduje počítačovou síť, pomalé nebo selhávající prvky. Správce tak dostává informace o:

- dostupnosti služeb a serverů
- vytíženosti linek, CPU, přepínačů a jiných zařízení

Analýza dat – je použití systému na sběr a následnou analýzu dat za účelem odhalení anomálií, které naznačují možné infiltrace útočníků do vnitřního prostředí.

- využití NetFlow protokolu
- network Behavior Analysis
- filtrování paketů

Nástroje k sledování sítí:

- monitoring v reálném čase (FCM)
- analýza chování sítě (ADS)Monitoring výkonnostních parametrů aplikací (APM)
- nahrávání záznamu datové komunikace (TR)

3.3.5 ENCRYPTION

Je to proces, při kterém se zakóduje zpráva nebo soubor, takovým způsobem, aby si ho mohl přečíst jen daná osoba nebo osoby. K šifrování se používá algoritmus a k dekódování se využije příslušný dekódovací klíč. Věci k zašifrování mohou být:

- soubory uložené na místních pevných discích pracovních stanic
- soubory uložené na výměnných médiích
- celé vyměnitelné jednotky
- celé jednotky pevných disků

3.4 Nejnovější SW a HW produkty nasazované v praxi

3.4.1 Firewal

Nejnovější typy firewallů – Next Generation Firewall (NGFW) změnili pohled na síťový provoz. Tím, že se výrazně změnily možné bezpečnostní rizika, musela se změnit i kontrola síťového provozu. Aplikace dnes již nejsou identifikovatelné jen jako porty. IP adresy nejsou dostačující na identifikaci uživatelů a pakety už nejsou jen obsah dat. Je nutná kontrola jejich obsahu. NGFT detekuje aplikace nejen na základě portů, ale pomocí tzv. signatur, které firewall ke každé aplikaci zná. Neidentifikovatelný obsah paketů při scházejících signaturách řeší podrobnou heuristickou analýzou. Uživatele pak neidentifikuje jen podle IP adresy, ale i podle dalších dostupných uživatelských údajů, jako Active Directory, LDAP, CaptivePortal apod. Kontrola obsahu se zaměřuje na možné úniky dat (DLP) a možné hrozby (malware) a na UR filtr.

3.4.2 IDS/IPS – siťové prvky

Chyby či nedostatky v programech zapříčiňují stále víc útoků. Ty jsou z pohledu tradičního firewallu skryté v legálním provozu. Detekce útoku je však na aplikační vrstvě. IDS (intrusion detection system)- jedná se o pasivní sondy sledující síťový provoz a jsou schopné odhalit podezřelé aktivity, bohužel však až v době jejich průběhu a část paketů vždy dorazí až k cíli.

IPS - Intrusion Prevention System - je aktivní zařízení umístění v síti „in-line“. Dokáže útoky detekovat a okamžitě blokovat už na hranici sítě. Blokované jsou však jen nežádoucí aktivity. Vytváří se tak další vrstva doplňující klasické firewally. NGFW již tato řešení integrují do jednoho celku. Existují scénáře, kdy nasazení samostatného IDS/IPS zařízení dává smysl, a to v místech, kde síťový provoz nesmí procházet firewallem.

3.4.3 DLP (Data Loss Prevention)

Pro zajištění ztráty dat je nutné řešit fyzickou bezpečnost. Je nevyhnutelná a důležitá pro omezení přístupu neoprávněných osob, zálohování dat – pro případ fyzického selhání HW a nebo přírodních katastrof, zabezpečení IT infrastruktury na všech úrovních sítě. Zabezpečení IT infrastruktury představuje:

Gateway:

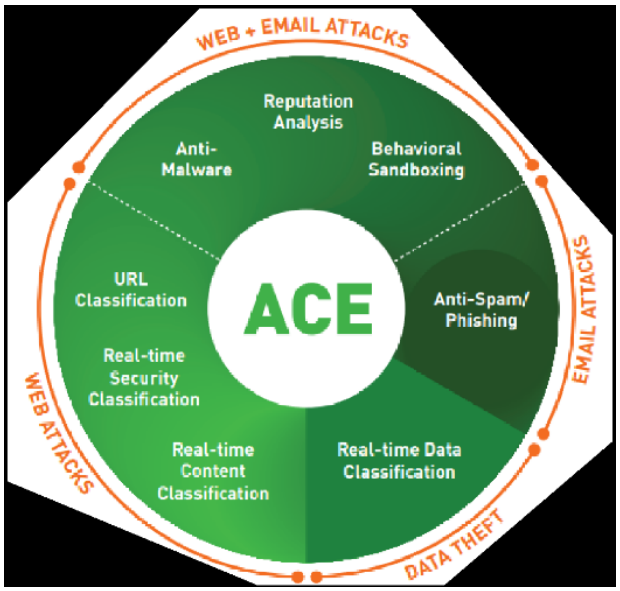
- kontrola všech protokolů přecházejících z internetu do interní sítě a naopak
- kontrola obsahu přecházejícího interní sítě do internetu
- možnost blokování nebo logování.

Network:

- kontrola síťových tiskáren

Endpoint:

- šifrování disků
- kontrola přístupu k portům
- firewall a VPN
- kontrola přístupu k aplikacím a datům [10]



Obr. 5) Model Datta Loss Prevention [10]

3.4.4 DDOS - distributed denial of service

Je typ útoku, který má za úkol převzít kontrolu, nabourat se do sytému a má zahltit server/službu tak, aby vyčerpala svou obslužnou kapacitu a přestala reagovat – odmítla službu. Na ochranu se používá více nástrojů jako:

- IPS prevence narušení systémů
- DoS odmítnutí služby
- NBA ochrana a analýza chování sítě
- reputation services

3.4.5 E-mail Security

Nejčastějšími nástrahami jsou klasické spamové útoky, nevyžádaná pošta s infikovaným obsahem, taktéž phishing prostřednictvím kterého se útočník snaží získat citlivé údaje prostřednictvím falešných WEB stránek atp. Častou metodou je cílená forma phishingu zaměřená na konkrétní osoby s přístupem k cenným informacím za účelem krádeže identity či získání kontroly nad PC, popřípadě napadnutí celofiremní sítě. Útoky DHA (Directory Harvest Attack) slouží k získání emailových adres pomocí masivní vlny emailů s běžnými jmény, které spamerům odhalí funkční a zranitelné maily. Většinou nejslabším článkem jsou právě zaměstnanci, proto je prevence velmi důležitá.

Nasazuje se rozsáhlá kolekce řešení jako: AntiMalware, Antivirus, Antispam, AntiPhishing, AntiSpyware, DLP, mobile DLP, Secure Email Delivery, Email archiving, File Sandboxing, Email Encryption, IM security, Image analyzis, reporting a mnoho funkcionalít.

3.4.6 Vícefaktorová autentizace

K vícefaktorové autentizaci patří smart karty, tokeny, čtečky, Acess managament, Single Sign On, One Time Passwords, PKI a další díky nimž je možné zabezpečit identitu uživatele, citlivé data a služby.

Složení vícefaktorové autentizace:

- něco co vím jen já – např. HESLO, číselná kombinace
- něco co fyzicky mám – např telefon, chytré hodinky
- něco čím jsem – otisk prstu či jiný biometrický znak

Výhody vícefaktorového ověření:

- vysoká bezpečnost a ochrana soukromí uživatele
- automatizace životního cyklu uživatelských identit
- oboustranná autentizace eliminuje nebezpečí pishingu

3.4.7 VPN – Virtual Private Network

Je virtuální soukromá síť zajišťující bezpečnou komunikaci v prostředí veřejné sítě (internet). V rámci kapacity existující infrastruktury je u VPN vyhrazena část kapacity pro komunikaci tak, aby byla fyzicky oddělená. VPN dělíme na intranet a extranet. VPN Remote acces (vzdálený přístup) umožňuje jednotlivým uživatelům se připojit k podnikové síti odkudkoliv a vzdáleně pracovat nebo komunikovat s organizací.

4 LEGISLATIVNÍ POŽADAVKY

4.1 GDPR

V roce 2009 vstoupil v platnost zákon 110/2019 Sb. o zpracování osobních údajů, který je adaptačním zákonem Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), dále jen GDPR (General Data Protection Regulation). Do té doby platila národní úprava - Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

Toto nařízení (zákon) zpřesňuje ochranu osobních údajů a posiluje právo fyzické osoby na kontrolu zpracování osobních údajů. Ty mohou být zachyceny v listinné podobě, ale i v elektronické zejména v různých informačních systémech.
Co všechno jsou osobní údaje podle GDPR:

- jméno, příjmení
- věk a datum narození
- pohlaví
- občanství
- stav
- rodné číslo, nebo jiný identifikátor vydaný státem
- telefonní číslo
- emailová adresa
- IP adresa
- síťový identifikátor

Zvláštní kategorie osobních údajů (osobní údaje zvláště citlivé)

- etnický nebo rasový původ
- zdravotní stav
- náboženské vyznání
- tresty a odsouzení
- sexuální orientace
- politické názory
- členství v odborových organizacích
- osobní údaje dětí
- biometrické a genetické údaje sloužící k identifikaci

Smyslem ochrany dat je učinit taková organizační a technická opatření, která v nejvyšší možné míře omezí možnost nenávratného poškození nebo ztráty dat. Minimalizuje negativní dopady způsobené touto ztrátou či poškozením na další činnost organizace.

Fyzický osoba uděluje odvolatelný souhlas se zpracování svých osobních údajů. Udělený souhlas musí být výslovný, svobodný, konkrétní informovaný.

Každá organizace zpracovávající osobní údaje musí mít ustanoveného pověřence pro ochranu osobních údajů. Pověřenec dohlíží na zpracování osobních údajů a kontroluje dodržování jejich zásad zpracování.

Zásady pro zpracování osobních údajů:

- zákonnost (dodržování zákonné normy pro práci s osobními údaji)
- korektnost a transparentnost (udělený souhlas, ochrana zájmů dotčené osoby, naší a třetích stran)
- účelové omezení (osobní údaje shromažďovány jen pro konkrétní účely se souhlasem)
- minimalizace údajů (data shromažďujeme jen v nezbytném rozsahu)
- přesnost (pouze aktuální údaje odrážející skutečný stav)
- omezení uložení (nedržíme osobní údaje déle, než je nezbytně nutné)
- integrita, důvěrnost (zamezení zničení ztráty, zneužití dat a jejich uchování)
- odpovědnost (jsme schopni doložit plnění předchozích bodů)

Na dodržování tohoto zákona v České republice dohlíží dozorový úřad, kterým je Úřad pro ochranu osobních údajů. Ten má také právo udělovat poměrně vysoké pokuty a sankce za jeho nedodržování.

4.2 Zákon o kybernetické bezpečnosti

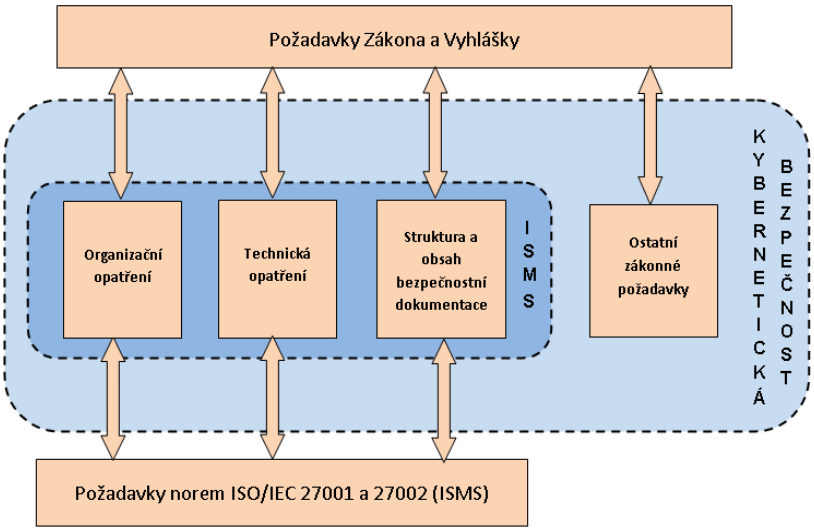
Jedná se o zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Zákon je účinný od 1. 1. 2015.

Zákon řeší zvýšení bezpečnosti kybernetického prostoru a hlavně se snaží ochránit tu část infrastruktury, která je pro fungování státu důležitá a její případné narušení by mohlo vést k poškození nebo ohrožení zájmů České republiky.

Cílem zákona není řešit všechna rizika v kyberprostoru, jako je např. porušování autorských práv, různé podvodné aktivity, úniky elektronických dat či šíření závadného elektronického obsahu.

Pro orgány a osoby, které určuje zákon, přibude řada nových povinností v oblasti zajištění bezpečnosti informačních a komunikačních systémů a komunikace s určenými kontaktními místy.

Zákon stanovuje, jakým způsobem má být kybernetická bezpečnost zajištěna a určuje způsob reakce na kybernetické hrozby nebo řešení nastalého incidentu. [13]



Obr. 6) Vztah mezi ISMS, kybernetické bezpečností, normami a zákonem [13]

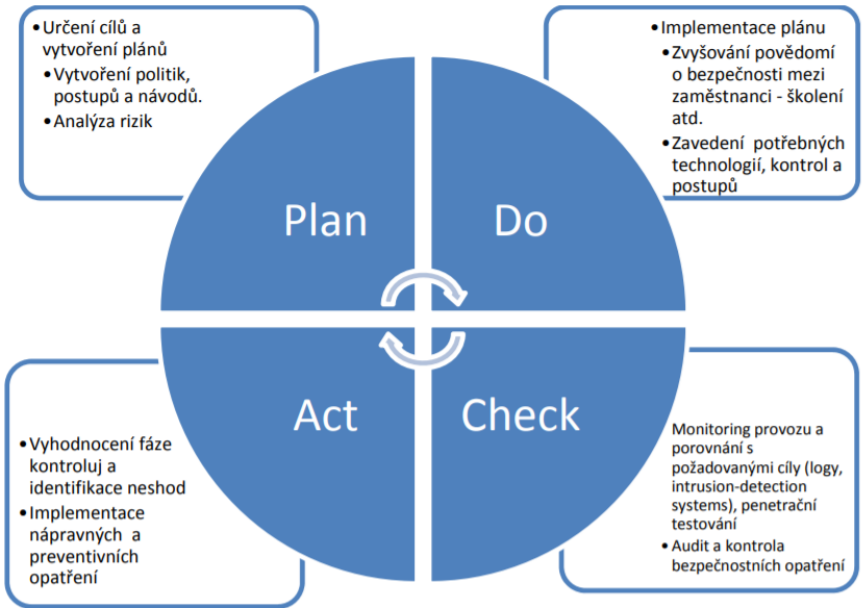
5 PLATNÉ NORMY

5.1 ČSN ISO/IEC 27000

Tato norma poskytuje přehled systémů řízení bezpečnosti informací (ISMS), termíny a definice obecně používané v řadě norem ISMS. Tato mezinárodní norma je použitelná pro všechny typy a velikosti organizací, její nedílnou součástí jsou definice a slovník [1]

5.2 ČSN ISO/IEC 27001

Norma poskytuje doporučení, jak aplikovat vybraná opatření ČSN ISO/IEC 27002 v rámci procesu ustavení, provozu, údržby a zlepšování systému managmentu bezpečnosti informací (ISMS) v organizaci. Norma prosazuje přijetí procesního přístupu k řešení ISMS a zavádí model známý jako Plánuj-Dělej-Kontroluj-Jednej (Paln-Do-Check-Act), který může být aplikován na všechny procesy ISMS tak, jak jsou definovány touto normou. V hlavní části normy jsou specifikovány požadavky na vybudování, zavedení, provoz, monitorování, přezkoumání, udržování, zlepšování a případnou certifikaci zdokumentovaného systému managementu bezpečnosti informací. Jsou zde specifikovány požadavky na výběr a zavedení bezpečnostních opatření uvedenými v ISO/IEC 27002. [1]



Obr. 7) Model Plan-Do-Chech-Act [1]

5.3 ČSN ISO/IEC 27002

Tato norma obsahuje více než 133 strukturovaných oblastí doporučení rozdělených do 11 kapitol, ve kterých je obsaženo více než 5000 přímých a odvozených bezpečnostních opatření, podporující dosahování podnikatelských cílů, přičemž odpovědnost za ně je možné jednoduše přiřadit osobám s odpovídajícími funkcemi. To umožňuje zjistit velmi rychle stav bezpečnosti

informačního systému organizace a zároveň vytvořit východiska pro jeho zlepšení, zejména vymezením oblastí, které nejsou dostatečně zajištěny. [1]

5.4 ČSN ISO/IEC 27003

Tato norma poskytuje doporučení pro ustanovení a implementaci systému řízení bezpečnosti informací v souladu s požadavky normy ISO/IEC 27001. Norma je použitelná pro všechny typy organizací, které zavádějí ISMS. Norma vysvětluje proces návrhu a implementace ISMS. Výsledkem tohoto procesu je finální plán implementace projektu ISMS. Na základě tohoto plánu lze v organizaci realizovat projekt implementace ISMS v pěti etapách:

1. získání souhlasu vedení organizace se zahájením projektu ISMS;
2. definování rozsahu, hranic a politiky ISMS;
3. provedení analýzy požadavků bezpečnosti informací;
4. provedení hodnocení rizik a plánování zvládaní rizik;
5. návrh ISMS.

V přílohách této normy jsou pak uvedeny kontrolní seznamy činností potřebných k ustanovení a implementaci ISMS, popis rolí a odpovědností bezpečnosti informací, informace o interním auditování, struktury politik a informace o monitorování a měření bezpečnosti informací. [1]

5.5 ČSN ISO/IEC 27004

Tato norma poskytuje doporučení pro vývoj a používaní metrik a pro měření účinnosti zavedeného systému řízení bezpečnosti informací a účinnosti opatření nebo skupin opatření, jak je uvedeno v ISO/IEC 27001. Implementace těchto doporučení je předmětem programu měření bezpečnosti informací. Program měření bezpečnosti informací zahrnuje procesy rozvoje metrik a měření, provádění měření, analýzu dat a hlášení výsledků měření a dále proces vyhodnocení a zlepšování programu měření bezpečnosti informací. V příloze normy jsou pak uvedeny příklady konceptů měření pro určitá opatření nebo procesy ISMS. [1]

5.6 ČSN ISO/IEC 27005

Tato norma poskytuje doporučení pro řízení rizik bezpečnosti informací v rámci organizace, podporuje obecný koncept specifikovaný v ISO/IEC 27001 a je strukturována tak, aby dostatečně podporovala implementaci informační bezpečnosti založené na přístupu řízení rizik. Nicméně tato norma nabízí konkrétní metodiku pro řízení rizik bezpečnosti informací. Záleží jen na organizaci, jaký přístup k řízení rizik zvolí. Norma je určena manažerům a pracovníkům, kteří jsou v rámci organizace odpovědní za řízení rizik bezpečnosti informací a tam, kde je to relevantní, také externím subjektům. Je aplikovatelná na všechny typy organizací, které mají v úmyslu řídit rizika, která mohou narušit bezpečnost informací organizace. [1]

5.7 ČSN ISO/IEC 27006

Tato norma specifikuje požadavky doporučení pro orgány provádějící audit a certifikaci systému řízení bezpečnosti informací a doplňuje tak požadavky obsažené v ČSN ISO/IEC 27001. Norma je primárně určena k podpoře procesu akreditace certifikačních orgánů poskytující certifikace ISMS. [1]

5.8 ČSN ISO/IEC 27007

Norma obsahuje doporučení k provádění auditů ISMS podle ČSN ISO/IEC 27001. Obsahově čerpá z ČSN EN ISO/IEC 19011:2002 Směrnice pro auditování systému managmentu a nebo systému enviromentálního managmentu. [1]

5.9 ČSN ISO/IEC 27008

Norma obsahuje doporučení auditorům ISMS a doplňuje ISO 27007. [1]

5.10 ČSN ISO/IEC 27010

Norma poskytuje doporučení pro řízení bezpečnosti informací při interní a mimo firemní komunikaci. [1]

5.11 ČSN ISO/IEC 27017

Mezinárodní norma uvádí pokyny pro kontrolní opatření bezpečnosti informací použitelné na poskytování a používání cloudových služeb poskytnutím dodatečných pokynů k implementaci příslušných kontrolních opatření specifikovaných v ISO/IEC 27002. [14]

5.12 ČSN ISO/IEC 27031

Tato mezinárodní norma popisuje pojmy a principy připravenosti informačních a komunikačních technologií (ICT) pro kontinuitu činnosti organizace a poskytuje rámec metod a postupů k identifikování a specifikování všech aspektů (jako jsou výkonnostní kritéria, návrh a implementace) pro zlepšení připravenosti ICT také umožňuje organizaci měřit parametry výkonnosti, které korelují s její IRBC konzistentním a rozpoznaným způsobem.

Předmět této mezinárodní normy zahrnuje všechny události a incidenty (včetně souvisejících s bezpečností), které mohou mít vliv na ICT infrastrukturu a systémy. To zahrnuje a rozšiřuje postupy řešení a řízení incidentů bezpečnosti informací a služby a plánování připravenosti ICT. [15]

5.13 ČSN ISO/IEC 27032

Tato mezinárodní norma poskytuje doporučení pro zlepšení stavu kybernetické bezpečnosti. Nastiňuje specifické aspekty dané činnosti a jejich závislosti na jiných oblastech bezpečnosti, zejména:

- bezpečnosti informací
- bezpečnosti sítě
- bezpečnosti internetu
- ochraně kritické informační infrastruktury (CIIP)

Pokrývá základní bezpečnostní postupy pro zainteresované strany v kybernetickém prostoru.

Tato mezinárodní norma poskytuje:

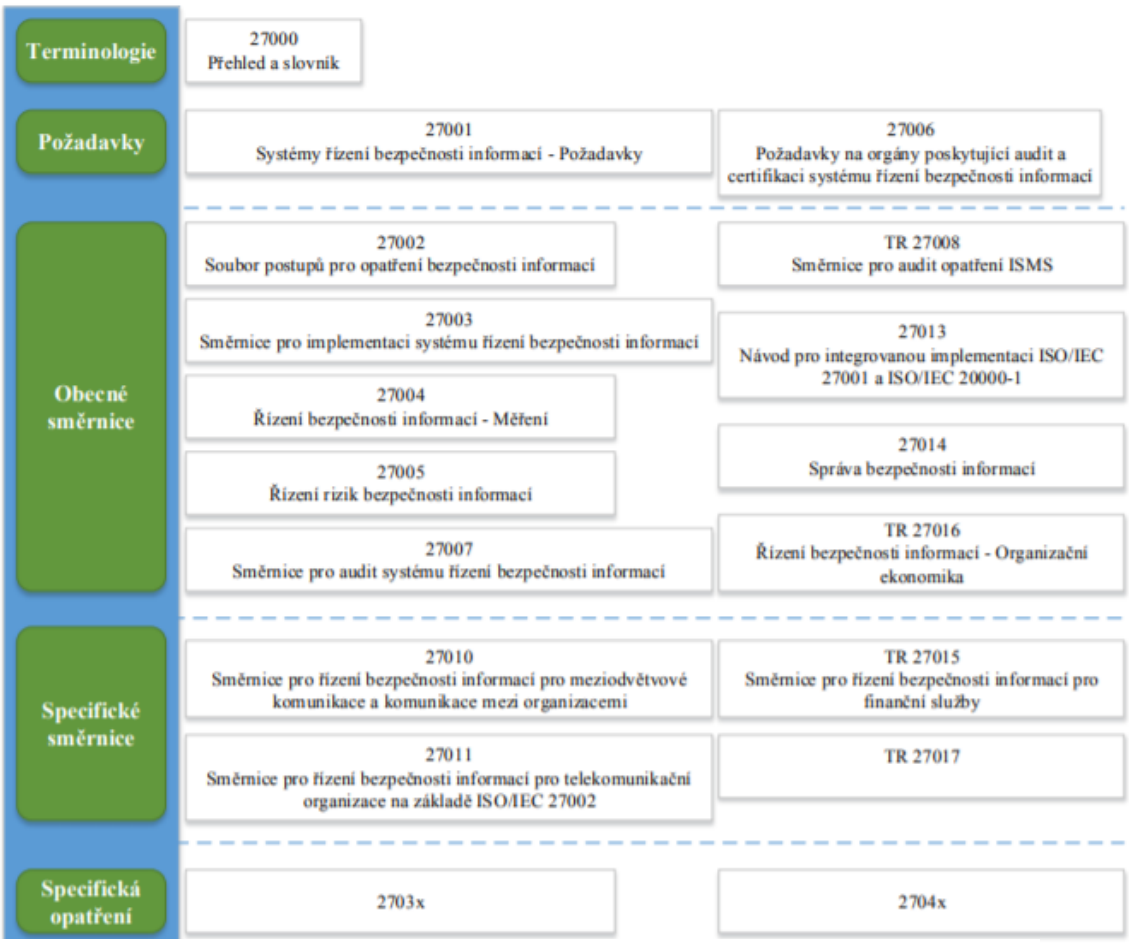
- přehled o kybernetické bezpečnosti
- vysvětlení vztahu mezi kybernetickou bezpečností a jinými typy bezpečnosti
- definici zainteresovaných stran a popis jejich rolí v kybernetické bezpečnosti
- strukturu, která umožňuje zainteresovaným stranám spolupracovat na vyřešení problémů kybernetické bezpečnosti. [16]

5.14 ČSN ISO/IEC 27034

Tato norma poskytuje návod s cílem pomoci organizacím integrovat bezpečnost do procesů používaných pro správu a řízení jejich aplikací. Podává přehled o bezpečnosti aplikací. Zavádí definice, pojmy, principy a procesy související s bezpečností aplikací. Použitelná pro aplikace vyvíjené v organizaci, aplikace získané od třetích stran, a pro aplikace, u kterých je vývoj nebo provoz aplikace zajištěn externě. [17]

5.15 ČSN ISO/IEC 27035

Norma je zaměřena na řízení incidentů bezpečnosti informací. Věnuje se postupům včasné detekce incidentů, jejich hlášení, vyhodnocování závažnosti a následné reakce. Dává doporučení pro identifikaci existujících zranitelností, posouzení jejich závažnosti a přijetí odpovídajících preventivních a nápravných opatření. [1]



Obr. 8) Vztahy mezi normami ISMS

6 FERRIT S.R.O.

Je soukromá česká firma s celosvětovou působností. Jedná se o výrobní společnost s vlastní vývojovou základnou založenou v roce 1993. Řadí se mezi středně veliké podniky s počtem zaměstnanců okolo 220. Je jedna ze tří největších společností v produkci závěsných dopravních systémů. Specializující se na výrobu, výzkum a vývoj, prodej a servis těžebních dopravních a manipulačních strojů a zařízení. Všechny jejich produkty jsou certifikovány pro použití v prostředí s nebezpečím výbuchu plynů a uhelného prachu.

6.1 Produkty

Závěsná dráha

Systém závěsné jednokolejové dopravy je nejefektivnějším a nejlevnějším způsobem dopravy osob, technologického a provozního materiálu v tunelech a důlních chodbách s případným výjezdem na povrch v úklonech do 30 stupňů.

Ozubnicová pozemní dráha

Je určena pro přepravu nákladu a materiálu, popřípadě částí kombajnů, mechanických výztuží a dalších věcí o vysokých hmotností.

Dieselová lokomotiva

Je autonomní trakční prostředek určený k přepravě vlakové soupravy. Máme dva typy dieselové lokomotivy - menší a větší. Menší je určen pro jednokolejové závěsné dráhy. Větší verze je pro pozemní ozubnicovou dráhu.

Akumulátorová lokomotiva

Je trakční prostředek určený pro přepravu vlakové soupravy. Máme dva typy akumulátorové lokomotivy: menší a větší. Menší je určen pro jednokolejové závěsné dráhy. Větší verze je pro pozemní ozubnicovou dráhu.

Trolejové lokomotivy

Jsou určeny pro přepravu materiálu nebo osob v horizontálních důlních dílech bez nebezpečí výbuchu uhelného prachu a plynu. Tahle lokomotiva se pouze vyrábí pro pozemní ozubnicové dráhy.

Manipulátor dieselový

Jedná se o nezávislý diesel-hydraulický agregát ovládaný dálkově nebo manuálně. Využívá se jako tažný prostředek pro přepravu soupravy, nebo pro napájení malé mechanizace (vrtačky, čerpadla, sbíjecího kladiva atd.).

Manipulátor elektrický

Využívá se jako tažný prostředek pro přepravu soupravy. Hydraulický agregát může pohánět vlastní manipulátor, zvedací zařízení, zařízení pro vrtání otvorů pro svorníky nebo jiné prostředky malé mechanizace.

Zvedací zařízení

K manipulaci a transport břemen, technologického materiálu a osob.

Kabiny

Pro přepravu pracovníků, záchranářů, raněných nebo v neposlední řadě kabiny speciální pro vysokorychlostní dopravu.

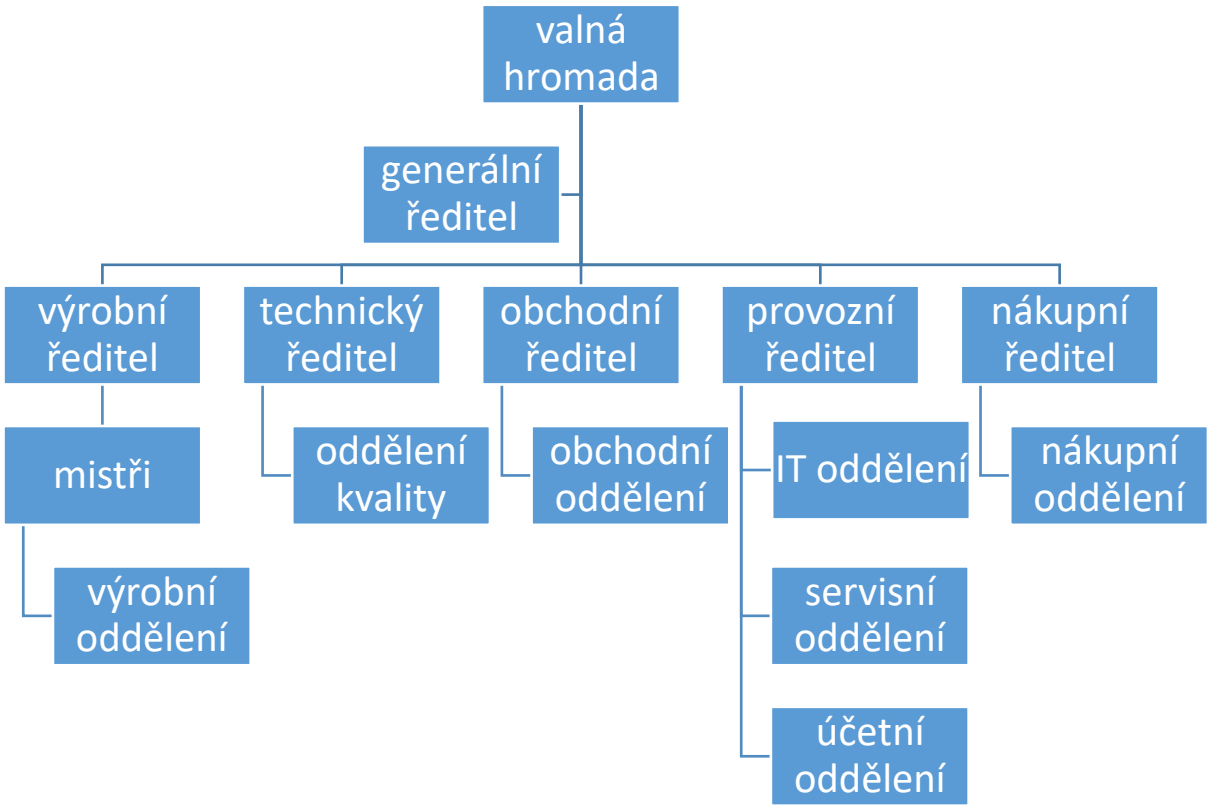
Kontejnery

K přepravě materiálu.

Clever parking (parkovací věž)

Jedná se o novinku, která se bude brzo vyrábět. Jde se o věž s otočným mechanismem, který nezabere moc místa a dokáže uskladnit 8, 12, 14 nebo 16 aut podle velikosti.

6.2 Organizace společnosti



Obr. 9) Model organizace společnosti

6.3 Bezpečnostní politika firmy

Infomační bezpečnost je jedno z nejdůležitějších témat, které společnost řeší. Důvodem je, že veškeré know-how, plány, dokumentace a informace nezbytné k provozu a udržení konkurenceschopnosti ve svém oboru jsou na serverových cloudech nebo ve firemní síti. Jak know-how, tak informace o zákaznících představují aktiva, po kterých by konkurenční firmy nebo útočníci mohli jít. Firma se snaží jít s trendy v oblasti informační bezpečnosti a rozumně investovat do nových ochranných prvků a docílit tak přiměřené bezpečnosti. Tedy stavu bezpečnosti, kdy velikost úsilí a investic do bezpečnosti IS musí odpovídat hodnotě aktiv a míře možných rizik.

Bezpečnost je ve firmě řešena interně kvůli nedůvěře k bezpečnostním společnostem. Ve firmě je vypracována směrnice (viz. příloha 1) k informační bezpečnosti, podle které by se měli zaměstnanci řídit.

6.4 Oblasti informační bezpečnosti

6.4.1 Zabezpečení z venku

Firma využívá FortiGate firewall společnosti FortiNet, který byl vybrán podle potřeb firmy a IT oddělení. Je využíván pro firewall samotný a zároveň jako VPN brána do firemní sítě. Externí forma firewallového řešení byla nahrazena vlastním zařízením z důvodu vyšší bezpečnosti v případě správy vlastní namísto externího subjektu. Kvůli útokům, výpadkům nebo jakýchkoliv dalších problémů má firma dvě internetové konektivity od různých poskytovatelů. Jednu hlavní, která se používá pro běžný provoz a v případě problému se automaticky přepne na druhou záložní. Přístup do sítě je možný jak z firemních počítačů, které jsou zapojené přímo do sítě, tak i přes VPN dálkově.

Každý uživatel má nastavená pravá a omezení, kam všude se mohu dostat podle toho na jaké pozici ve firmě jsou nebo podle toho, co potřebují ke své práci. Je tu přes 100 VPN přístupů. Obrana před vnějšími útoky má několik úrovní zabezpečení. První úroveň je zmíněný firewall, který je na hranici ISP a firemní sítě. Zde jsou definována pravidla pro přístup do firemní sítě nebo do předsazené DMZ, ve které jsou umístěny služby, které komunikují s vnějším světem internetu. V DMZ se nachází například CNC obráběcí stroje, e-mailový a webový server, na kterém běží firemní internet.

V rámci vnitřní sítě je bezpečnost postavena na produktu firmy Eset, konkrétně na uživatelských stanicích Eset Endpoint security a Eset File security na serverech, kde využívají všechny moduly jako například Anti-Phishingová ochrana nebo Anti-Stealth ochrana. Všechna zařízení jsou spravována pomocí ERA serveru, kde na dashboardu mají rychlý a jednoduchý přehled o aktuálním stavu.

6.4.2 Školení uživatelů

Ochrana systému a sítě je tak silná jako nejslabší článek. Nejslabším článkem bývají většinou lidé, neboli uživatelé dané sítě. Nejčastější chyby, které daní uživatelé dělají, jsou používaní slabých hesel, klikání na odkazy a soubory, které by neměli a podobně. Aby se zamezilo, podobným věcem, každého půl roku dostanou vedoucí jednotlivých oddělení firmy instruktáž a materiály s doporučením, kterými by se měli zaměstnanci řídit. Všechna základní práva a povinnosti uživatele výpočetní techniky jsou sepsána v interní směrnici týkající se bezpečnosti IT, se kterou se uživatelé museli seznámit a musí podle ní také jednat. Je v ní

zmíněna mimo jiné politika bezpečnosti hesel, která eliminuje výskyt slabých hesel či četnost jejich povinné změny.

6.4.3 Ukládaní a zálohy dat

Společnost využívá diskové pole jako prostor pro ukládání dat i pro systémové disky virtuálních serverů. File server je také virtuální a díky tomu poskytuje jednodušší správu zálohování. Všechna data uživatelů jsou umístěna v definovaném prostoru, který je zálohován stejně jako všechny servery infrastruktury na jiný záložní server. Tenhle server je umístěn geograficky v jiné lokalitě a je samozřejmě mimo doménu. Tohle eliminuje možnost ztráty zálohy v případě napadení sítě či kompromitování některého z účtů s právy v doménové struktuře. Zálohy probíhají jednou týdně v podobě full backup a denní rozdílové zálohy po dobu dvou týdnů. Odkládají se bokem vždy poslední den v měsíci a firma uchovává tímto způsobem historii dat za kalendářní rok. Mimo tyto zálohy je zapnuta na diskovém prostoru pro uživatelská data funkce shadow copy, která v případě mylného smazání dat uživatelem zjednodušuje jejich obnovu a „šikovnější“ uživatelé ji dokonce provádějí sami.

Mimo klasický file server, společnost využívá pro posílání dat mimo organizaci vlastní cloudové uložiště, které si spravuje také ve své režii a je fyzicky v rámci infrastruktury. Firma zastává postoj, že všechna firemní data zůstávají v jejich režii na vlastních serverech a nechtějí využívat externí společnosti pro správu a ukládání dat.

Každoročně se také odkládají zálohy fyzicky oddělené od systému k datu 31.12, které jsou na discích umístěny v trezoru pro krizové případy, kdyby předchozí systémy nezafungovaly a bylo by potřeba obnovit data.

6.4.4 Fyzická bezpečnost

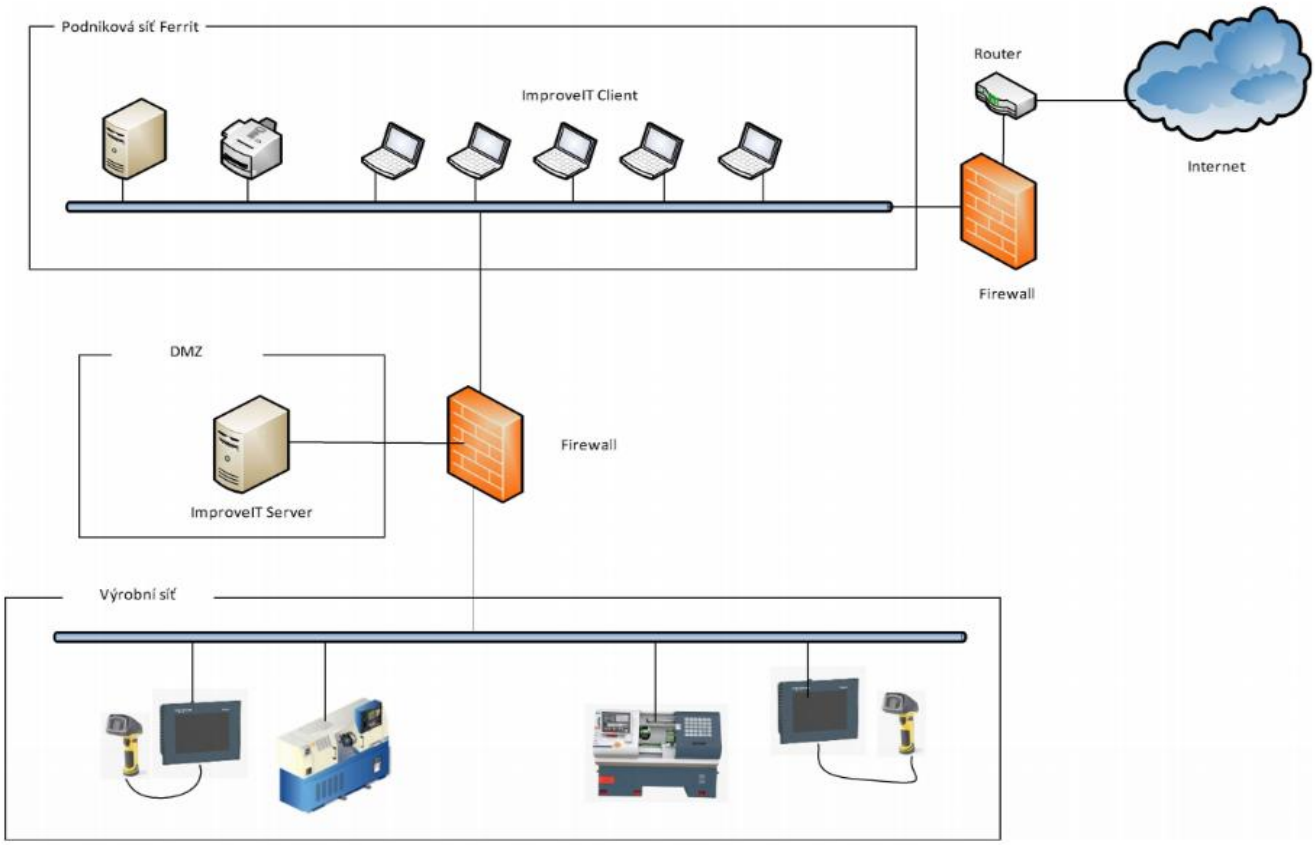
Fyzická bezpečnost má několik prvků. Kamerový systém, který snímá všechny exteriéry a část interiérů, jako jsou hlavní chodby, vstupy do pater, výtah a samozřejmě všechny výrobní prostory a montáže. Všechny vstupní dveře na patra v hlavní budově jsou opatřena elektronickými zámky na čipy, takže pouze oprávněná osoba může vstoupit do určitých pater (každé patro patří různému oddělení). Serverovny jsou opatřeny zabezpečovacím systémem a pro vstup musí oprávněný uživatel zónu odkódovat a následně odemknout dveře, které jsou zvenčí opatřeny koulí namísto kliky.

Hlavní serverovna je vybavena záložním zdrojem, který při výpadku proudu napájí servery samotné a hlavní síťové prvky nutné pro provoz. Tato zařízení dokáže záložní zdroj napájet přibližně 45 minut. V případě komplikací s obnovením dodávky elektřiny, se po patnácti minutách automaticky nastartuje dieselagregát, který začne napájet serverovnu, a všechny důležité rozvaděče v areálu firmy. To zajistí její provozuschopnost i v případě dlouhodobého výpadku elektřiny, aby uživatelé mohli bezpečně dokončit práci a uložit ji.

6.4.5 Kybernetická bezpečnost

V rámci implementace projektu sběru dat ze strojů v Ferrit s.r.o. dochází k připojení strojů do komunikační sítě a propojením s informační sítí podniku. Toto propojení umožňuje výměnu informací mezi výrobou a informačními systémy v podniku v reálném čase. Toto propojení realizuje společnost Ferrit ve své režii.

Z důvodů zabezpečení řídicích systémů strojů před kybernetickými útoky a v souladu s publikací NIST Special Publication 800-82 Guide to Industrial Control Systems (ICS) Security, byla vytvořena taková síťová architektura, která umožní oddělení sítě s výrobními zařízeními (výrobní síť) od podnikové informační sítě. Propojení mezi oběma sítěmi bude realizováno pouze v jediném bodě přes bezpečnostní prvek (firewall), který umožní definovat pravidla při výměně informací mezi sítěmi. [18]



Obr. 10) Struktura podnikové sítě [18]

6.5 Zavádění nových bezpečnostních opatření

Před samotným zaváděním bezpečnostních opatření, je nutné nejdříve provést identifikace a hodnocení aktiv, určení bezpečnostních hrozeb, analýzu rizik, provést jejich vyhodnocení a aplikovat dané bezpečnostní opatření. Poslední částí je sledování a vyhodnocení použitých bezpečnostních prvků. Než se začnou dané kroky provádět, tak hlavní IT manažer musí sepsat dokument, ve kterém informuje představenstvo o daném rozsahu prováděných kroků. Daný dokument musí být musí být odsouhlasen nebo upraven tak, aby s ním představenstvo souhlasilo. Tenhle dokument má pouze informovat představenstvo a není nadále k užitku. Výjimkou je, když se IT managment snaží zavést příslušnou normu z řady norem 27000. Tehdy je dokument nezbytný a je vyžadován auditem, který následně zhodnotí, zda všechny prvky z dané normy jsou aplikované a v pořádku.

6.5.1 Identifikace a hodnocení aktiv

Vše, co má pro organizaci nějakou hodnotu, která může být působením hrozby snížena, můžeme nazývat aktivem. Aktiva dělíme na hmotná (HW, SW atd.) a nehmotná (informace a know-how).

Výstupem této fáze by měl být dokument „Seznam aktiv“. Dokument by měl obsahovat seznam všech aktiv a vazeb mezi nimi, určení jejich vlastníků, stručný popis a jejich hodnotu. K identifikaci aktiv uvnitř hranice analýzy se používá BPA (Business Process Analysis). K ohodnocení aktiv se dá využít metodika CRAMM. [2]

Výsledkem je tabulka s termíny pro kvalitativní hodnocení podle dopadu na společnost. Rizika se dělí na:

- bezvýznamné riziko, žádný dopad na organizaci
- akceptovatelné riziko, zanedbatelný dopad na organizaci
- nízké riziko, potíže či finanční ztráta
- nežádoucí riziko, vážné potíže či podstatné finanční ztráty
- nepřijatelné riziko, existenční potíže [1]

6.5.2 Bezpečnostní hrozby

Hrozby se dělíme na přírodní hrozby (požár, záplavy atd.) a hrozby způsobené lidským faktorem, které jsou buď úmyslné nebo neúmyslné. Úmyslné hrozby jsou cílené útoky, které mají poškodit firmu. Mezi neúmyslné hrozby můžeme zařadit náhodné vymazání dat, poškození zařízení pádem a podobně.

Při určování potencionálních hrozeb byly brány pouze v potaz cílené útoky na společnost. Zbylé hrozby se neuvažovaly, protože byly součástí předešlé identifikace hrozeb a byla už zavedená nezbytná opatření k zabránění jejich vzniku a narušení jakýmkoliv způsobem chodu společnosti. Důvod k zaměření pouze na cílené útoky byla odezva IT oddělení, na pokusy proniknutí do systému přes email zaměstnanců a následné proniknutí přes přístup dodavatelů, kteří také mají omezený přístup do sítě.

Hrozba dalších pokusů o prolomení do sítě je vždy přítomná a příště může ovlivnit integritu a dostupnost dat, které by byly pro firmu vitální.

6.5.3 Analýza rizik

Má za úkol zjistit jakými riziky jsou aktiva ohrožena. Výsledkem je míra rizika.

Rizika máme:

- bezvýznamné, není vyžadováno žádné zvláštní opatření
- akceptovatelné, riziko přijatelné se souhlasem vedení
- mírné, většinou je nutné provést opatření
- nežádoucí, vyžaduje urychlené provedení odpovídajících bezpečnostních opatření
- nepřijatelné, nutnost okamžitého zastavení činnosti [1]

Analýza rizik zde probíhá interním procesem, to znamená, že nejsou využívány externí společnosti pro analýzu rizik, ale vychází ze znalostí a zkušeností IT oddělení, které provádí analýzu rizik ve své režii. Po provedení analýz se stanoví plán a nápravná opatření, která eliminují nebo maximálně sníží riziko. Jedná se o vnější i vnitřní bezpečnost infrastruktury.

6.5.4 Bezpečnostní opatření

Bezpečnostní opatření jsou prevencí na hrozby, které byly zjištěny a vyhodnoceny jako nežádoucí či nepřijatelné.

Před samotou aplikací bezpečnostních opatření IT manažer sepíše dokument, který obsahuje veškeré prvky, které bude zavádět, do jaké míry ovlivní bezpečnost, dobu implementace a odhadovanou cenu nákladů. Další částí dokumentu je vyhodnocení předešlých kroků, které slouží jako podklad a zdůvodnění k zavádění daných bezpečnostních opatření. Daný dokument se předloží vedení, který ho schválí a implementace může začít.

V nynější době společnost nasazuje dvoufaktorové ověřování přístupu na e-mail a VPN pro přístup zvenčí, kdy v případě vyvolání některé z těchto akcí bude mimo klasického zadávání hesla zaměstnanec povinen potvrdit přihlášení buď kódem zaslaným pomocí sms nebo aplikací v telefonu.

Následně je firma ve fázi obměny pokrytí areálu wi-fi signálem z důvodu zastaralého vybavení access pointů a sjednotí pokrytí signálem pod jednu platformu, kde bude využito pro vnitřní síť ověření radius serverem a pro veřejnou síť, která má sloužit vyloženě pro návštěvy společnosti a dostupnost internetu pod jednoduchým heslem, které se bude v měsíčním intervalu měnit. Dále se přepracovávají práva k přístupu do sítě pro jednotlivé dodavatele a zaměstnance. To je z důvodu, kdyby došlo k prolomení hesla nějaké osoby, aby data, ke kterým by si útočník dostal, byla minimální a škody zanedbatelné.

6.6 Zhodnocení informační bezpečnosti a jeho řízení.

Společnost se snaží klást na bezpečnost velký důraz, zejména pak na zajištění bezpečnosti informací o zákaznících a především firemní know-how. Organizace má všechny základní práva a povinnosti uživatele výpočetní techniky sepsána v interní směrnici týkající se bezpečnosti IT.

Hodnocení informační bezpečnosti si podnik zajišťuje interně. Tento přístup je úspornější z hlediska nákladů. Výhodou tohoto přístupu je, že dané IT oddělení dobře zná

prostředí firmy a není potřeba zasvěcovat externí organizaci a odhalovat jí interní a citlivé informace. Nevýhodou je, že dané výsledky nemusí dosahovat tak vysoké úrovně jak od externí společnosti, která se na dané věci specializuje. Další nevýhodou je, že analýzy, zhodnocení a vypracování výsledků trvá spoustu času, během kterého IT oddělení není schopno plnit denní povinnosti.

Hlavním problémem je nedostatek odborníků v IT oddělení. Na celou firmu jsou pouze dva zaměstnanci a jejich manažer. Z toho pouze IT manažer je dostatečně vzdělaný v dané problematice a rozumí všem nezbytným krokům, které k tomu patří. Tohle v budoucnu může vést k nedostatečně objektivním analýzám nebo opomenutí nějakého nedostatku v zabezpečení, které může vést k finančním ztrátám společnosti.

Šíření informačního vědění mezi zaměstnanci probíhá po půl roce. To je adekvátní interval, aby povědomost byla na přiměřené úrovni. Problémem je, že se neklade skoro žádný důraz na ověření, zda zaměstnanci tyhle pokyny dodržují a řídí se danými opatřeními ve směrnici společnosti.

Nová opatření, která zahrnují dvoufaktorové ověřování, přepracování práv zaměstnanců a spolupracujících firem jsou dostatečnými bezpečnostními prvky k zamezení proniknutí a minimalizaci škod budoucích útočníků.

6.7 Doporučení pro zlepšení daného stavu

Nejslabším článkem bezpečnosti firmy, jak už bylo zmíněno, bývají zaměstnanci. Z toho důvodu bych doporučoval zavést ověřování povědomosti zaměstnanců o informační bezpečnosti. Povědomost by se ověřovala v intervalech šesti měsíců pomocí sezení, kde by byli ověřeny znalosti povinností uživatele výpočetní techniky. Dále bych zavedl program, který každé tři měsíce bude vyžadovat změnu hesla a ohlídá, že dané heslo bude obsahovat kombinaci určitého počtu znaků, čísel, velkých, malých písmen a speciálních znaků.

Doporučuji přijmout alespoň jednoho nového IT pracovníka, který by byl schopen vykonávat denní věci, ale zároveň se vyzná v problematice informační bezpečnosti. Tenhle krok vychází z mého osobního pozorování vytíženosti IT oddělení. Navíc další odborník na informační bezpečnost by přispěl k objektivnějšímu hodnocení stavu informační bezpečnosti a vyšší úrovni zabezpečení.

Další návrh se týká využití možnosti zálohy dat na externích cloudových serverech, které by se pronajímaly. Tím dojde k eliminaci nečekaných problémů, které by mohly poškodit serverová uložiště v areálu společnosti.

Zásadním krokem pro aplikaci výše uvedených opatření bude potřeba zlepšení povědomí vedení společnosti o této problematice. Bude na vedoucím IT oddělení předložit a vysvětlit vedení podrobný plán zvýšení financování IT oddělení, tak aby mohly být nasazeny všechny potřebné HW a SW prostředky k zabezpečení informační bezpečnosti podniku.

7 ZÁVĚR

V teoretické časti bakalářské práce rozebírám a popisuji pojem informační bezpečnost. Čím se daná bezpečnost zabývá a proč je nezbytná. Uvádím světové přístupy k řešení dané problematiky jako je ITIL a COBIT. Zároveň se věnuji, jakým směrem se daná problematika bude ubírat a jaké prvky můžeme využít k zamezení, nebo snížení možnosti ztráty dat.

Dále jsem provedl rešerši legislativ a bezpečnostních norem týkající se informační bezpečnosti. U jednotlivých norem jsem vypsal jejich oblast využití. U legislativních požadavků státu jsem pospal hlavní body a oblasti, kterými se GDPR a kybernetická bezpečnost zabývá.

V praktické části bakalářské práce se zaměřuji na společnost Ferrit s.r.o.. Popisuji základní informace o společnosti a produkty, které firma vyrábí. V další části mé bakalářské práce se zabývám bezpečnostní politikou a oblastmi informační bezpečnosti ve společnosti Ferrit s.r.o.. Zde jsem se snažil detailně popsat a analyzovat veškerá zavedená opatření, kterými firma disponuje. A to ve všech oblastech informační bezpečnosti.

V další části této práce věnuji krokům, podle kterých firma Ferit s.r.o. aplikovala principy zavádění bezpečnostních opatření a jejich jednotlivým krokům. Dílčí kroky jsou vypracovány na základě získaných informací a poznatků, které jsem získal při vypracovávání teoretické části bakalářské práce.

Závěrečná část se zaměřuje na navržení vlastních bezpečnostních prvků, opatření a postupů k zlepšení informační bezpečnosti ve společnosti. Ze všech mnou navržených opatření byla doposud realizována pouze jediné. A to dvoufaktorové ověřování přístupu na email a VPN pro přístup zvenčí. V případě vyvolání akce – potřeby autorizovaného přístupu bude mimo klasického zadání hesla zaměstnanec, nebo obchodní partner povinen potvrdit přihlášení buď kódem zaslaným pomocí sms nebo aplikací v telefonu.

8 SEZNAM POUŽITÝCH ZDROJŮ

[1] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: Akademické nakladatelství CERM, 2013. ISBN 9788072048724

[2] ČERMÁK, Miroslav. Řízení informačních rizik v praxi. Brno: Tribun EU, 2009. ISBN 978-80-7399-731-1.

[3] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: Akademické nakladatelství CERM, 2013. ISBN 9788072048724

[4] [online]. [cit. 2020-06-24]. Dostupné z: http://wikipedfie.pedf.cuni.cz/it/doku.php?id=users:jvais:pocitacove_site_ii_okruhy

[5] [online]. [cit. 2020-06-24]. Dostupné z: https://ikaros.cz/bezpecnost-informaci

[6] Bezpečnost a ochrana informací [online]. [cit. 2020-06-24]. Dostupné z: https://managementmania.com/cs/bezpecnost-a-ochrana-informaci

[7] [online]. [cit. 2020-06-24]. Dostupné z: http://ijs.8u.cz/index.php/standardizace-v-pocitacovych-sitich/referencni-model-iso-osi

[8] [online]. [cit. 2020-06-24]. Dostupné z: https://managementmania.com/cs/information-technology-infrastructure-library

[9] [online]. [cit. 2020-06-24]. Dostupné z: https://managementmania.com/cs/cobit-control-objectives-for-information-and-related-technology

[10] [online]. [cit. 2020-06-24]. Dostupné z: https://www.sectec.sk/technologie/forcepoint

[11] [online]. [cit. 2020-06-24]. Dostupné z: https://www.ngss.cz/sluzba/14-security-management-center

[12] Virtuální analytik [online]. [cit. 2020-06-24]. Dostupné z: https://www.threatguard.cz/

[13] Zákon o kybernetické bezpečnosti [online]. [cit. 2020-06-24]. Dostupné z: http://www.tsoft.cz/zakon-o-kyberneticke-bezpecnosti/

[14] 27017 [online]. [cit. 2020-06-24]. Dostupné z: https://csnonline.agentura-cas.cz/Detailnormy.aspx?k=502319

[15] 27031 [online]. [cit. 2020-06-24]. Dostupné z: https://csnonline.agentura-cas.cz/Detailnormy.aspx?k=98676

[16] 27032 [online]. [cit. 2020-06-24]. Dostupné z: https://csnonline.agentura-cas.cz/Detailnormy.aspx?k=93691

[17] 27034 [online]. [cit. 2020-06-24]. Dostupné z: https://csnonline.agentura-cas.cz/Detailnormy.aspx?k=95858

[18] Interní podklady firmy Ferrit s.r.o

9 SEZNAM ZKRATEK, SYMBOLŮ, OBRÁZKŮ A TABULEK

9.1 Seznam obrázků

9.2 SEZNAM POUŽITÝCH ZKRATEK

AD Active Directory
ČSN Česká technická norma
ČR Česká republika
EU Evropská Unie
HW Hardware
ICT Information and Communication Technologies
IEC International Electrotechnical Commission
IS Information System
ISMS Information Security Management System
ISO International Organization for Standardization
IT Information Technology
ITIL Information Technology Infrastructure Library
SW Software
NDA Non-Disclosure Agreement
OSI Open System Interconnection
CD Compact Disc
ITSM IT Service management
BMS Business Model for Information Security
ITAF IT Assurance Framework
HDP Hrubý domácí produkt

PC	Personal Computer
IoT	Internet of Things
Saas	software jako služba
PaaS	Platform as a Service
AR	Augmented Reality
AI	Artificial Intelligence
ID	Identification
DLP	Data Loss Prevention
ZT	Zero Tolerance
URL	Uniform Resource Locator
ACL	Access Control List
VLAN	Virtual LAN
SDN	Software defined networking
VPN	Virtual Private Network
IPS	Intrusion Prevention Systems
DoS	Denial of Service
IM	Instant messaging
IRBC	Readiness for Business Continuity
ISP	Internet Service Provider
DMZ	Demilitarized Zone
ICS	Industrial Control Systems
BPA	Business Process Analysis
Sms	Short message service
Wi-fi	Wireless Fidelity

10 SEZNAM PŘÍLOH

PŘÍLOHY

Příloha č. 1

Obsah