České vysoké učení technické v Praze
Masarykův ústav vyšších studií
a
Vysoká škola ekonomická v Praze

Podnikání a komerční inženýrství v průmyslu

Bc. Radek Zajíc

Vybraná kybernetická rizika a jejich předcházení

Diplomová práce

Praha, 2016

Vedoucí diplomové práce: Ing. Igor Kukliš

Oponent diplomové práce:

Datum obhajoby:

Hodnocení:

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

ZADÁNÍ DIPLOMOVÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení: Zajíc Jméno: Radek Osobní číslo: 365907000

Fakulta/ústav: Masarykův ústav vyšších studií (MÚVS)

Zadávající katedra/ústav: Katedra managementu, MÚVS

Studijní program: Podnikání a komerční inženýrství v průmyslu

Studijní obor: Podnikání a management v průmyslu

II. ÚDAJE K DIPLOMOVÉ PRÁCI

Název diplomové práce:

Vybraná kybernetická rizika a jejich předcházení

Název diplomové práce anglicky:

Description and Mitigation of Selected Cyber-Risks

Pokyny pro vypracování:

Práce spadá do oblasti řízení rizik (angl. risk management) a zabývá se analýzou vybraných kybernetických rizik, jejich popisem a vysvětlením. Poskytuje přehled nejčastěji se vyskytujících kybernetických rizik a nevynechává ani rizika přicházející společně s nastupujícími technologiemi (IoT - internet věcí, IPv6 - internetový protokol nové generace, využívání technologií v 'cloudu', přístup 'Bring your own device'). Navrhuje opatření pro minimalizaci uvedených rizik.
Rámcová osnova: Rešerše metod práce s riziky, popis druhů rizik, strategie zvládnutí rizik, identifikace a hodnocení rizik. Opatření pro minimalizaci uvedených rizik.

Seznam doporučené literatury:

VEBER, Jaromír. Management. Praha: Management Press, 2009
KRULIŠ, Jiří. Jak vítězit nad riziky. Praha: Linde, 2011
TRIM, Peter R a Yang-Im LEE. Cyber security management. Burlington, VT: Gower, 2014
ULSCH, N. Cyber threat!. Hoboken, New Jersey: Wiley, 2014

Jméno a pracoviště vedoucí(ho) diplomové práce:

Ing. Igor Kukliš, Katedra managementu MÚVS

Jméno a pracoviště konzultanta(ky) diplomové práce:

Datum zadání diplomové práce: Termín odevzdání diplomové práce: 8.5.2016

Platnost zadání diplomové práce: 30.6.2017

Podpis vedoucí(ho) práce | Podpis vedoucí(ho) ústavu/katedry | Podpis děkana(ky)

III. PŘEVZETÍ ZADÁNÍ

20. 4. 2016

Datum převzetí zadání

Podpis studenta(ky)

© ČVUT v Praze, Design: ČVUT v Praze, VIC

Prohlášení

Prohlašuji, že jsem diplomovou práci zpracoval samostatně a že jsem uvedl všechny použité informační zdroje.

V Praze, 18. května 2016

.....

podpis diplomanta

Poděkování

Děkuji své ženě Lucii, která mne podporovala od prvotní ideje studia přes všechny studijní peripetie až po poslední zkoušku studia, a i poté při tvorbě této diplomové práce. Děkuji celé své rodině, která v úspěch mých studií věřila i v okamžicích, kdy jsem já sám takový úspěch považoval za stejně nepravděpodobný, jako výhru v loterii. Děkuji i vedoucímu této práce, Ing. Igoru Kuklišovi, za jeho ochotu, trpělivost a obětavost, se kterou k vedení této práce přistoupil, a za všechny jeho návrhy, rady a komentáře, jak práci vylepšit.

Identifikační záznam

ZAJÍC, Radek. *Vybraná kybernetická rizika a jejich předcházení*. Praha, 2016. 99 stran. Diplomová práce. České vysoké učení technické v Praze, Masarykův ústav vyšších studií a Vysoká škola ekonomická v Praze, Podnikání a komerční inženýrství v průmyslu. Vedoucí práce Ing. Igor Kukliš.

Abstrakt

Práce spadá do oblasti řízení rizik, popisuje řízení rizik obecně a ve vztahu ke kybernetickým rizikům. Zabývá se analýzou vybraných kybernetických rizik, jejich popisem a vysvětlením možných příčin. Poskytuje přehled nejčastěji se vyskytujících kybernetických rizik, incidentů či hrozeb, a nevynechává ani rizika přicházející společně s nastupujícími technologiemi (IoT - internet věcí, IPv6 - internetový protokol nové generace, využívání technologií v 'cloudu', přístup 'Bring your own device'). Navrhuje opatření pro minimalizaci uvedených rizik.

Abstract

This thesis is focused on the topic of risk management. Attempts to describe risk management in general as well as in the context of cyber-risks. Analyses selected cyber-risks, describes them and explains the potential causes of such risks. Presents a list of the most common cyber-risks, incidents, threats and mentions the risks arising from the adoption of emerging technologies (such as the Internet of Things, Internet Protocol version 6, Cloud computing and the “Bring Your Own Device” approach). The thesis also proposes countermeasures to minimise mentioned risks.

Klíčová slova

Řízení rizik, kybernetická rizika, hrozby, zranitelnosti, opatření, průnik, kybernetický prostor.

Keywords

Risk management, cyber-risks, threats, vulnerabilities, measures, intrusion, cyber-space.

Obsah

Seznam obrázků

Předmluva

Žijeme v turbulentní době. Rozvoj sítě Internet v uplynulých dvaceti letech přinesl dříve netušené možnosti. Rychlost přenosu informací mezi koncovými uživateli vzrostla za posledních dvacet let o čtyři řády. Vzájemná komunikace je snazší, než kdy dříve byla. Sdílení informací se postupem času stalo snadnější. Sítí Internet každým okamžikem proudí biliony znaků informací. Největší výměnný bod na světě, AMS-IX, ve špičkách přenese půl bilionu znaků za sekundu[1].

Technologie se posouvají každým dnem mílovými kroky vpřed. Stejně tak se ale každým dnem objevují nové hrozby, nová rizika, která nám inovované technologie přinášejí. Bohužel, na rozdíl od některých technických parametrů, jako jsou například cena, dostupnost, rychlost či uživatelská přívětivost moderních zařízení a technologií, existují úskalí, která zůstávají uživateli skryta. V extrémních případech uživatel ani netuší, že by se měl o bezpečnost zajímat, že jeho data proudí sítí nešifrovaná a kdokoli na cestě si je může přečíst.

Skrytými úskalími jsou například informace o tom, jak kvalitní zabezpečení který produkt poskytuje. Zda se data přenášejí zabezpečenou cestou a jsou tak ochráněna proti odposlechu či neautorizovaným změnám. Jak náročné je pro útočníka zabezpečení prolomit – a zda lze zabezpečení v čase zvýšit, například výměnou programového vybavení (software). Zda je vůbec výměna software možná – a je-li možné opravit alespoň bezpečnostní zranitelnosti, které v produktech mohou existovat. Jak dlouho je produkt podporován jeho autorem či výrobcem. Je-li vůbec bezpečnost na straně výrobce řešena.

Bezpečnost informací, sítí, technologií a produktů je bohužel i v dnešní době dost přehlíženým tématem. Autoři produktů často spoléhají na principy *security through obscurity* (zabráním-li uživateli v pochopení, jak produkt funguje, nebude schopen bezpečnost narušit) a *black box* (produkt je černou skříňkou, do které nikdo nevidí). Podobně jako ve fyzickém světě, i do kybernetického prostoru pronikají technicky zdatní lidé, které zajímá, jak věci fungují, a jak by se případně jejich fungování dalo zlepšit. V angličtině se jim kdysi říkalo ***hackeři*** *[hekři]*, a jednalo se o nejvyšší možné uznání pro podobné osobnosti

[1] Grafy aktuálního vytížení lze sledovat na https://ams-ix.net/technical/statistics

s výjimečnými znalostmi fungování kybernetických systémů. Těm, kteří se pak získané znalosti pokusili zneužít, se říkalo ***crackeři*** *[krekři]*. Právě technicky zdatní lidé často zjišťují, že to s bezpečností produktů není ani v dnešní době nikterak slavné. Ti špatní z nich, ***kybernetičtí nebezpečníci***, pak zjištěné nedostatky, či zranitelnosti (anglicky ***vulnerabilities***), jak se jim také říká, zneužívají ve svůj prospěch.

Ačkoli je ochrana před ***nebezpečníky*** náročná a není zadarmo, měla by být vhodně včleněna do řízení každé organizace. Kybernetická bezpečnostní rizika lze vhodnými postupy identifikovat, analyzovat a následně navrhnout a realizovat protiopatření. Bezpečnost lze správnými prostředky dostatečně zvýšit.

A právě analýzou vybraných kybernetických rizik a návrhem opatření ke snížení pravděpodobnosti výskytu takových rizik se zabývá tato práce.

1. Úvod

Organizace ve dnešním světě zpracovávají a uchovávají čím dál více svých aktiv v digitální podobě. Zároveň se pomocí výpočetních prostředků a datových sítí propojují vzájemně mezi sebou, ale i se zákazníky, v důsledku čehož už nestačí realizovat opatření pro zajištění kybernetické bezpečnosti na fyzickém perimetru organizace. Každá organizace, od nejmenších po ty největší, by měla analyzovat kybernetická rizika, která jí hrozí, a přijmout opatření pro jejich minimalizaci.

Dávno se nejedná pouze o riziko ztráty dat, i když to je stále významné. Rizikem může být například poškození reputace značky, narušení logistického řetězce, finanční ztráty či odstavení infrastruktury nutné pro fungování organizace.

Kybernetická rizika už nejsou pouhým problémem, který vyřeší ***pánové, kteří se starají o servery***. Dotýkají se běžných zaměstnanců, všech úrovní managementu, prostupují celou organizací. Dávno ***opustila datové sály***.

V této práci, která je určená zejména pro střední a vyšší management, případně pro útvary informační bezpečnosti a bezpečnosti informačních technologií, se budu zabývat vybranými kybernetickými riziky, potenciálními incidenty, hrozbami a původci takových hrozeb.

Práce je logicky členěna na několik částí, které jsou dále děleny na podkapitoly. V první části práce se zaměřím na teorii oblasti řízení rizik (risk management). Druhá část seznámí čtenáře s kybernetickým prostředím a nastíní možné přístupy ve vztahu ke kybernetickým rizikům. Třetí část práce pak popíše kontext vybraných kybernetických systémů, pokusí se identifikovat některá rizika a jejich původce, a následně navrhne obecně použitelná protiopatření pro zvýšení kybernetické bezpečnosti.

2. Řízení rizik

Součástí většiny manažerských aktivit, zvláště strategických a takových, kde dochází k významným změnám, je ***riziko*** [srov. 1, s. 597], které může působit pro organizaci pozitivně (ve smyslu zvlášť významného úspěchu) či negativně (vede-li ke ztrátám či jiným, nefinančním, negativním dopadům). ***Řízení (management) rizik*** by tak mělo být, zvlášť v dnešní globalizované době, součástí uvažování každého manažera.

Je-li řízení rizika zahrnuto do běžného manažerského rozhodování a podnikového řízení, dochází k omezování možných negativních důsledků událostí během života organizace a k omezování možných negativních dopadů, které by mohly vést až k samotnému zániku organizace.

V této části práce se proto pokusím uvést čtenáře do oblasti řízení rizik (***risk management***), probrat hodnocení rizik, na které navážu v další části přechodem do oblasti kybernetických rizik. Také popíšu některé přístupy, které je vhodné mít na paměti, a to nejen v případě kybernetických rizik.

2.1 Definice pojmů

Riziko je v teorii managementu všudypřítomný průvodní jev, který působí na firemní výsledky. Existují rizika, která mohou vést k pozitivnímu i negativnímu vývoji v organizaci (například riziko vstupu na nový trh, které může oproti očekávání způsobit ztráty nebo nadprůměrné zisky). Existují ale i rizika, která (dojdou-li uplatnění) jsou pro organizaci vždy negativní. Rizika tohoto druhého typu literatura označuje jako ***čistá rizika*** a právě těmito riziky se budu v dalším textu zabývat.

> ***Čisté riziko je takové riziko, které má pouze negativní stránku [srov. 1, s. 598].***

Potenciální významnost rizika lze měřit na základě pravděpodobnosti výskytu a očekávaného dopadu na firemní aktiva. Právě aktiva jsou tím, co v oblasti managementu zvané řízení rizik je třeba před negativními dopady rizik chránit.

> ***Významnost rizika je vyjádřena pravděpodobností výskytu incidentu a mírou dopadu na aktivum [srov. 5, s. 9] [srov. 1, s. 609].***

Definice pracuje s pojmy ***incident, aktivum, pravděpodobnost a dopad***. Při analýze rizik je bezpodmínečně nutné oddělit spouštěcí událost, která vede k aktivaci samotného rizika, a následek takové události. Událost, která je spouštěčem, se nazývá incident.

> ***Incident je taková událost, která způsobuje škodu nebo snížení hodnoty aktiva [srov. 5, s. 9].***

Slovo incident literatura používá v souvislosti s událostmi, které mají negativní dopady na aktivum. V případě neoprávněného průniku do firemní počítačové sítě se zajisté bude jednat o incident ve vztahu k zabezpečení počítačové sítě. Nedojde-li ale ke zcizení osobních dat z informačních systémů organizace, nejedná se o incident s dopadem na oblast osobních dat. Jeden incident může být zdrojem více než jednoho rizika.

> ***Aktivum je cokoli, co je pro zúčastněného hodnotné [srov. 5, s. 10].***

Hodnota aktiv je vždy relevantní právě k tomuto zúčastněnému, ať už se pod pojmem ***zúčastněný*** skrývá oddělení organizace, celý koncern, nebo fyzická osoba. Vzít v potaz zúčastněného je nutné při každé analýze rizik – na základě individuálních potřeb či aktiv zúčastněného pak mohou mít rizika různou pravděpodobnost výskytu i míru dopadu.

> ***Zúčastněným může být organizace, osoba či skupina osob, pro které je prováděna analýza rizik [srov. 5, s. 10].***

Zúčastněný však často není tatáž entita jako ***stakeholder*** (tedy osoba, skupina či organizace, která má se zúčastněnou organizací nebo její částí co do činění, je jejím fungováním dotčena či má na chod firmy vliv [srov. 1, s. 643]). Provádím-li pro konkrétní organizaci analýzu rizik, pak je tato organizace zúčastněná dle výše uvedené definice. Stakeholdery mohou být například její zaměstnanci, techničtí partneři, kteří mají přístup k datům, či firemní management.

Dalšími důležitými pojmy jsou ***pravděpodobnost*** a ***dopad***. Jejich kombinace se pak označuje jako ***úroveň rizika***.

> ***Pravděpodobnost je úroveň náhody, s jakou k určitému jevu dojde [srov. 5, s. 10].***

Pravděpodobnost lze definovat čistě matematicky na škále od 0 (událost se nestane) po 1 (událost se stane vždy) nebo například počtem výskytů jevu za určitý čas.

> ***Dopad rizika reprezentuje výši škody nebo snížení hodnoty aktiva [srov. 5, s. 11].***

Jelikož v tomto textu pracuji pouze s čistými riziky, nemá dopad rizika pozitivní vliv (zvýšení hodnoty aktiva). V analýze rizik, která mohou mít i pozitivní vliv na chod organizace, by dopad rizika mohl být pozitivní i negativní.

> ***Úroveň rizika pak reprezentuje potenciální výši rizika na základě jeho pravděpodobnosti výskytu a očekávaného dopadu [srov. 5, s. 11].***

S takto definovanou terminologií budu dále pracovat v popisu řízení rizik i v praktické části práce.

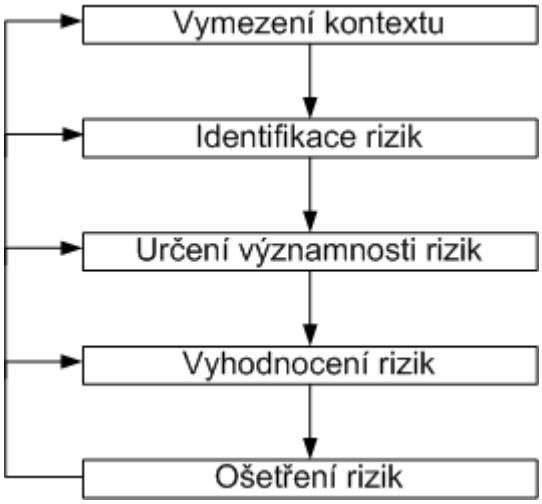
2.2 Řízení rizik

Rizikům je vystavena každá organizace. Řízení rizik obvykle sleduje cíl zajištění přežití organizace (tj. minimalizaci nebezpečí, která by ohrozila existenci firmy), resp. udržení podnikatelské prosperity organizace [srov. 1, s. 605]. Aby s riziky bylo možné pracovat, je nutné stanovit procesy řízení rizik.

> ***Řízení rizik zahrnuje koordinované aktivity řízení organizace ve vztahu k rizikům [srov. 5, s. 12].***

2.3 Proces hodnocení rizik

Proces hodnocení rizik je základním procesem řízení rizik [srov. 5, s. 16].



Obrázek 1 - Proces hodnocení rizik

Mezi jeho základní části patří:

- Vymezení kontextu, ve kterém se rizika řídí
- Identifikace přítomných rizik
- Určení významnosti rizik
- Vyhodnocení rizik
- Ošetření rizik
- Monitorování a prověřování systému řízení rizik

Každou z komponent procesu se budu zabývat dále.

2.3.1 Vymezení kontextu

Ve fázi vymezení kontextu dochází ke specifikaci externího i interního prostředí, ve kterém organizace funguje. Dále dochází ke stanovení objektů řízení rizik v návaznosti na strategii organizace [srov. 1, s. 606].

Mezi součásti kroku vymezení kontextu patří i určení rizikové kapacity firmy a velikosti přijatelného rizika. Riziková kapacita obvykle stanovuje nejvyšší finanční ztrátu, která pro organizaci není smrtící, tj. neovlivní existenci samotné firmy. Její výše je ovlivněna kapitálovou strukturou organizace a jejími schopnostmi získávání finančních prostředků.

Přijatelné (tolerovatelné) riziko představuje výši ztráty, kterou je organizace ochotna pokrýt z rizikové kapacity. Velikost přijatelného rizika je ovlivňována strategickými prioritami organizace a averzí či ochotě managementu k riziku [srov. 1, s. 607].

Objektem řízení rizik jsou takové části systému, které jsou podrobovány hodnocení rizik. Systémem se pak nazývá sada vzájemně závislých entit, které tvoří integrovaný, jasně ohraničený celek [srov. 5, s. 16].

Za systém podle této definice lze v některých případech vnímat například i celou organizaci. Hodnocení rizik pak zahrnuje činnosti, procesy, zaměstnance a další relevantní části organizace.

2.3.2 Identifikace rizik

Aby bylo možné rizika řídit, je třeba je nejprve identifikovat. Identifikace musí proběhnout včas, aby bylo možné postoupit k dalším krokům procesu hodnocení rizik. V této fázi dochází zejména k určení faktorů (v případě kybernetických rizik negativních, u jiných podnikatelských rizik i pozitivních), které mohou ovlivnit dosažení podnikatelských cílů organizace či jejích organizačních jednotek.

Vnitřní rizika organizace pomáhají identifikovat pracovníci (zaměstnanci) organizace; vnější rizika pak vyžadují aktivní sledování podnikatelského okolí [srov. 1, s. 607].

> ***I v boji jde o to, vyhnout se překážkám a pustit se do slabých míst [srov. 11, s. 43].***

Identifikace rizik probíhá ve vztahu k aktivům. Probíhá tedy identifikace potenciálních ***hrozeb*** a ***zranitelností*** a snaha o pochopení, jak mohou hrozby zneužít zranitelností a způsobit ***incidenty***.

> ***Zranitelnost je slabina v návrhu nebo v systému, která může být zneužita hrozbou s cílem způsobit škodu na aktivu. Hrozba je pak událost nebo činnost způsobená zdrojem hrozby a potenciálně vedoucí k incidentu [srov. 5, s. 18].***

Jako příklad zranitelnosti lze uvést například špatně fungující zámek a chybějící alarm, čehož může zneužít zloděj pro vloupání se do objektu. Závažnost zranitelnosti závisí na tom, k jakým hrozbám ji lze zneužít. Ačkoli hrozby mohou vést k incidentům, při analýze rizik je třeba věnovat řádnou péči zejména původcům hrozeb, které jsou v řetězci úplně na začátku a jsou tak přímým zdrojem incidentů.

Původci hrozby mohou (ale nemusí) mít původ v lidech. Podobu pak mají hmotnou i nehmotnou. Mezi původce hrozeb lze zařadit například špatně

školeného operátora (lidský původce hrozby), přírodní katastrofu (přírodní původce hrozby) nebo škodlivý program (nehmotný původce hrozby).

Identifikace hrozeb může probíhat i v kruhu, kdy dochází k přecházení mezi jednotlivými kroky identifikace rizik podle následujícího obrázku [5].

Obrázek 2 - Identifikace hrozeb

Identifikace rizik může využívat různé zdroje informací jako například týmovou diskusi, osobní rozhovory, kontrolní seznamy, historická data či statistická data.

Po identifikaci rizik musí organizace přistoupit ke stanovení významnosti rizik, vyhodnocení rizik a stanovení způsobu řešení rizik.

2.3.3 Určení významnosti a vyhodnocení rizik

Aktivita určení významnosti rizik zahrnuje zpracování výstupů z fáze identifikace rizik a jejich porovnání s hodnotícími kritérii. Cílem je zjistit, proti kterým rizikům je třeba se zajistit (např. v podobě přijetí opatření ke snížení rizika nebo pojištění proti následkům rizika).

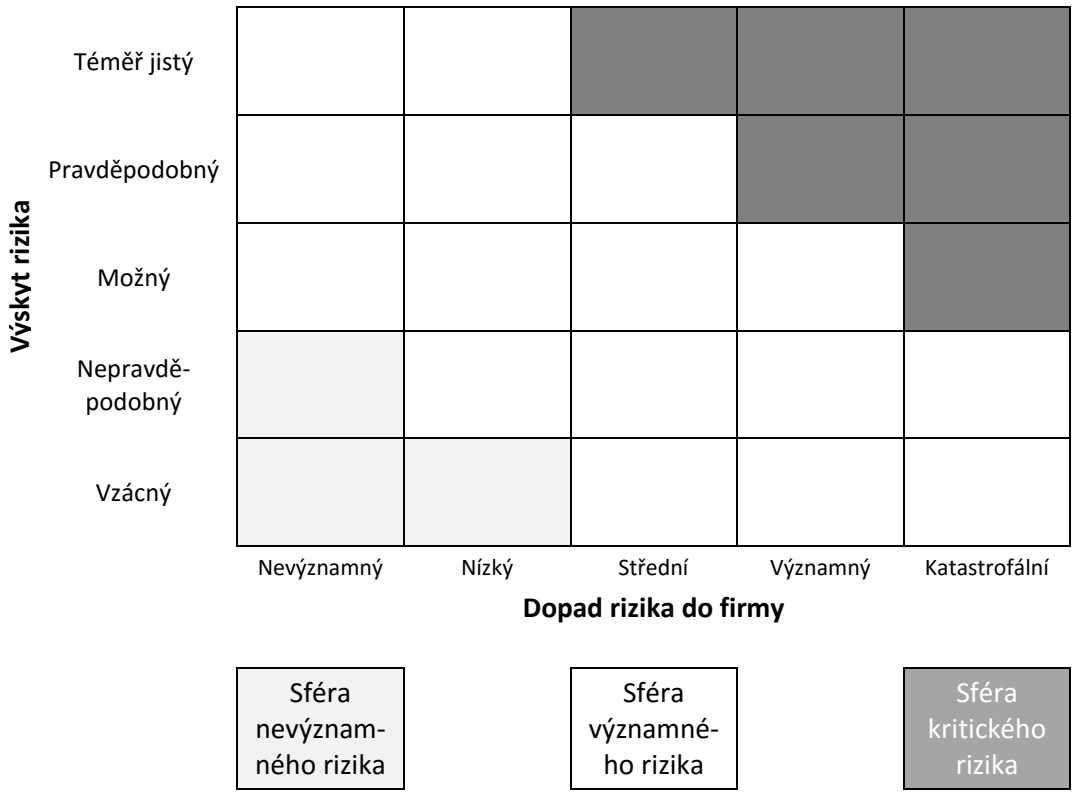
V některých případech lze více různých rizik sloučit pod jedno společné riziko. Tento přístup se hodí zejména tehdy, pokud by rizika samotná nepůsobila výrazné problémy, ale v případě jejich souběhu by byl dopad na organizaci výrazný až katastrofální, případně kdy by více různých rizik mělo dopad na totéž aktivum [srov. 5, s. 21].

Pro krok přijímání opatření ke snížení rizik je dále vhodné rizika seskupit podle společných jmenovatelů. Seskupení je vhodné zejména pro rizika, která sdílejí původce hrozeb či hrozby, mají společné zranitelnosti, nebo působí na

stejná aktiva. Seskupení takových rizik pak může vést k jejich efektivnějšímu ošetření.

Praktickým způsobem určení významnosti rizik je zanesení jejich dopadů a pravděpodobnosti výskytu do matice. Na základě polohy v matici pak lze zhodnotit závažnost rizika.

Následující obrázek zobrazuje možnou podobu matice hodnocení rizik [srov. 1, s. 610].



Obrázek 3 - Možná podoba matice hodnocení významnosti rizik

Dalším krokem po určení významnosti rizik je fáze vyhodnocení rizik. Cílem je posouzení rizik, jejich přijatelnosti a rozhodnutí, proti kterým rizikům budou navržena opatření.

K vyhodnocení rizik je vhodné využít matici pravděpodobností a dopadů rizik, zavedenou během hodnocení významnosti rizik. Každé riziko je vyneseno do této matice a podle toho, do které sféry spadá, je zařazeno do konkrétní úrovně závažnosti rizika.

2.3.3.1 Pravděpodobnost výskytu rizika

Pravděpodobnost výskytu rizika lze vyjádřit na matematické škále od 0 (událost nenastane) do 1 (událost jistá). Rozmezí pravděpodobnostních hodnot ***P*** výskytu rizika pak lze převést na pětistupňovou stupnici **například** takto:

- **Vzácný** – ***P*** v rozmezí 0 až 0,15: riziko se téměř nikdy nevyskytne
- **Nepravděpodobný** – ***P*** v rozmezí 0,15 až 0,35: riziko se vyskytuje pouze za velmi specifických podmínek v organizaci
- **Možný** – ***P*** v rozmezí 0,35 až 0,65: podmínky pro výskyt rizika lze vyvolat v běžném firemním prostředí, ale nevyskytuje se často
- **Pravděpodobný** – ***P*** v rozmezí 0,65 až 0,85: riziko se vyskytuje často, pro jeho výskyt není třeba žádných specifických podmínek
- **Téměř jistý** – ***P*** v rozmezí 0,85 až 1: téměř nikdy nenastane situace, kdy by k riziku nedocházelo

Kalibrace pravděpodobnostních hodnot ***P*** a stupňů pravděpodobnosti je vždy individuální pro každý proces hodnocení rizik a organizace jí musí věnovat náležitou péči.

2.3.3.2 Dopad rizika do firmy

Dopad rizika do firmy, v případě využití navržené matice rizik, lze definovat **například** takto:

- **Nevýznamný** – riziko má pouze mírný interní dopad, neohrožuje významně žádná aktiva, není komplikací pro fungování organizace
- **Nízký** – riziko má pouze interní dopad, může způsobit komplikace při fungování organizace, zpomalit některé procesy, ale neohrožuje organizaci
- **Střední** – riziko má interní i externí dopad, ohrožuje aktiva organizace, může krátkodobě ohrozit fungování organizace a poškodit jméno či značku, ale nevystavuje organizaci rizikům postihu státních orgánů ani neohrožuje existenci organizace
- **Významný** – riziko má významný interní i externí dopad, ohrožuje aktiva organizace, může dlouhodobě ohrozit fungování organizace a poškodit jméno či značku, vystavuje organizaci rizikům postihu státních orgánů, ale neohrožuje existenci organizace
- **Katastrofální** – riziko má významný interní i externí dopad, ohrožuje aktiva organizace, může dlouhodobě ohrozit fungování organizace a poškodit jméno či značku, vystavuje organizaci rizikům postihu státních orgánů, ohrožuje existenci organizace

Podobně jako u stupňů pravděpodobnosti rizika, i v případě stanovení stupňů dopadu rizika do firmy je nutné postupovat s péčí a individuálně v každém procesu hodnocení rizik.

2.3.3.3 Závažnost rizika

V závislosti na umístění rizik v matici hodnocení významu rizik spadá riziko do jedné ze sfér závažnosti rizika.

Podle konkrétní sféry závažnosti rizika pak lze určit, zda je riziko pro organizaci přijatelné, případně jaká opatření mají být provedena.

Pro hodnocení rizika a rozhodování o riziku lze použít následující proces [srov. 1, s. 612]:

Obrázek 4 - Proces rozhodování o riziku

Výsledek procesu vyhodnocení rizika záleží na rizikové toleranci organizace, tj. výši rizika, kterou je firma ochotna akceptovat. Nepřesáhne-li riziko takovou hranici, může organizace riziko přijmout, tzv. ***zadržet***, bez realizace opatření na jeho snížení, a s případnými následky rizika se vypořádat s využitím vlastních zdrojů [srov. 1, s. 611 – 612].

2.3.4 Ošetření rizik

Cílem fáze ošetření rizik je identifikace, výběr a realizace kroků k odstranění příčin či omezení dopadů rizik. V případě špatně zvolených opatření mohou ovšem rizika i vzrůst. Proto je třeba věnovat opatřením pozornost a vyhnout se takovým krokům, které by měly potenciál riziko zesilovat.

Ošetření rizik zahrnuje volbu a aplikaci vhodných opatření ke snížení dopadu rizika [srov. 5, s. 21].

Ačkoli teoreticky lze veškerá rizika označit za nepřijatelná a snažit se je eliminovat, v praxi není takový přístup funkční. Určitá úroveň rizik je vždy přítomna. Koneckonců i podnikání samo je rizikové a tak nikdy nelze eliminovat úplně všechna rizika.

V praxi se tak uplatňují přístupy, kdy probíhá ošetření rizik podle náročnosti (a samozřejmě nákladů) jednotlivých opatření. Existuje-li ekonomicky nenáročné řešení, které eliminuje určité malé riziko, doporučuji toto riziko eliminovat i v případě, že jeho dopady jsou nevýznamné. Podobný princip se uplatňuje u velkých rizik, pokud by náklady na jejich ošetření byly neúnosně vysoké – v takovém případě může existovat i jediná možnost: takové riziko prostě přijmout [srov. 5, s. 22].

Během ošetřování rizik je tak třeba hledat a analyzovat možné způsoby ošetření rizik. Podobně jako v případě identifikace rizik lze využít existující seznamy nástrojů či kroků k ošetření rizik, nebo zvážit skupinovou diskusi nad dostupnými možnostmi ošetření.

Konečný výběr způsobů ošetření rizik tak bude postaven na analýze nákladů a přínosů jednotlivých variant. Během výběru je nutné vzít na vědomí, že některá opatření mohou přinést nová rizika.

Je-li riziko nepřijatelné, přichází v úvahu varianty vyhnutí se riziku a zmírnění rizika. Vyhnutí se riziku je situace, kdy organizace určitou aktivitu nebo projekt odmítne či od jeho realizace ustoupí.

Nelze-li riziko zadržet ani se mu vyhnout, musí organizace přijmout opatření či strategii ke snížení rizika. Mezi taková opatření či strategie patří zejména:

- Odstranění příčin rizika nebo jejich výrazné oslabení
- Snižování negativních dopadů rizika
- Přenos rizika na třetí stranu (např. dodavatele, pojišťovnu)

I po realizaci opatření pro zmírnění rizika však obvykle existuje tzv. ***zbytkové*** (reziduální) riziko.

Aby bylo možné riziko odstranit či oslabit, je třeba omezit pravděpodobnost jeho výskytu, snížit následky incidentů, případně kombinovat obojí. Je třeba zaměřit se na odstranění zdrojů hrozeb, ošetřit zranitelnosti (či alespoň snížit jejich závažnost), nebo jiným způsobem snížit pravděpodobnost výskytu hrozeb.

2.3.5 Monitorování a prověřování rizik

Žádný systém není dokonalý a stejně tak není dokonalé ani sebelepší ošetření rizik. Ani rizika sama o sobě nejsou stálá, v čase přibývají či ubývají. Každá organizace by tak měla hodnocení rizik pravidelně opakovat, revidovat potenciální původce hrozeb, přítomnost zranitelností, sílu rizik a účinnost přijatých opatření. V případě, kdy se změní podmínky prostředí (například se opatření stane neúčinným nebo se objeví nová zranitelnost), je nutné přijmout náležitá opatření.

Organizace by měla vyhodnocovat změny zejména v následujících oblastech [srov. 5, s. 23]:

- Aktiva – pokud v čase dojde k významné změně v množství či struktuře aktiv či ve vnitřním či vnějším kontextu, mohou se objevit nová rizika a jiná naopak zaniknout.
- Hrozby – změny vnitřního či vnějšího prostředí mohou vést ke vzniku nových hrozeb. V některých případech jsou nové hrozby přímo pozorovatelné, v jiných je pro jejich identifikaci třeba provést nové hodnocení rizik.
- Zranitelnosti – vyhodnocování existujících a nově se objevujících zranitelností dokáže zodpovědět otázku, zda jsou na obzoru nové hrozby, které by tyto zranitelnosti využívaly. Nové zranitelnosti pak, vedou-li k novým hrozbám, je nutné vhodným způsobem ošetřit.

Stejně tak je vhodné průběžně vyhodnocovat zbytková rizika, která se v čase mohou proměnit v rizika s mnohem větším dopadem.

3. Kybernetické prostředí

Přístupy k rizikům, jejich hodnocení a ošetřování mohou mít mnoho různých podob. V této práci se dále budu zabývat zejména riziky, která vznikají a existují ve vztahu ke kybernetickým systémům.

3.1 Kybernetický prostor

Literatura [srov. 5, s. 25] definuje kybernetický prostor jako:

> ***Soubor vzájemně propojených sítí výpočetní techniky, včetně služeb, počítačových systémů, jednoúčelových systémů s vestavěnými procesory a řadiči, a informací uloženou na úložištích či putujících sítěmi.***

Za nejznámější kybernetický prostor lze bezpochyby považovat síť Internet, globální počítačovou síť, která je přítomná dnes již v každé zemi – včetně zemí s autoritářskými režimy jako Severní Korea, Kuba, Írán nebo Čína. Internet je nejznámějším kybernetickým prostorem, není ale jediným. Definici kybernetického prostoru splňuje jakýkoli soubor propojených počítačových sítí (internetů s malým „*i*"), které jsou využívané ke komunikaci. Oxfordský slovník definuje heslo cyber-space jako: „Pomyslné prostředí, ve kterém dochází ke komunikaci pomocí počítačových sítí" [srov. 13].

V kontextu organizací je kybernetickým prostorem jakýkoli soubor jedné nebo více vzájemně propojených lokálních počítačových sítí (LAN, Local Area Network). Síti, která propojuje lokální sítě, se pak říká WAN (Wide Area Network, ve významu rozsáhlá síť – český překlad anglického termínu se však v literatuře nepoužívá). Jako příklad kybernetických prostorů, které nejsou připojeny k síti Internet, je možné uvést armádní počítačové sítě, technologické sítě, policejní datové sítě a podobně [srov. 5, s. 25].

3.2 Kybernetický systém

Rizika, která vznikají v souvislosti s existencí kybernetického prostoru (ať už kvůli jeho existenci nebo přímo v něm) mohou mít mnohem dalekosáhlejší dopad. Vzájemnou závislost jakéhokoli systému a kybernetického prostoru je

nutné považovat za zranitelnost. Literatura [srov. 5, s. 26] proto definuje kybernetický systém takto:

> ***Kybernetický systém je systém, který využívá kybernetického prostoru.***

Takový systém zahrnuje výpočetní a informační infrastrukturu, pracovníky a další entity, které mají co do činění s obchodními procesy a chováním systému. Z podstaty věci jsou dnes kybernetické systémy součástí většiny organizací.

Jsou všudypřítomné. Občané, organizace i celé vlády dnes spoléhají na počítačové systémy a síť Internet. Plně využívají těchto prostředků pro různé služby, namátkou uvádím komunikaci se zdravotnickými organizacemi a přístup ke zdravotním datům, obchodní systémy, bankovní instituce a obchodní služby, a tak dále. I některé služby kritické infrastruktury (prvky nebo systémy, jejichž narušení by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu; kritickou infrastrukturu v ČR vymezuje § 2 písm. g) zákona č. 240/2000 Sb., krizový zákon, a nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury), jsou kybernetické systémy.

3.3 Kybernetická bezpečnost

Kybernetická bezpečnost chrání kybernetické systémy před kybernetickými hrozbami. Kybernetická hrozba je hrozba, která těží z existence kybernetického prostoru [srov. 5, s. 29].

Kybernetické hrozby mohou být úmyslné (***malicious***) a neúmyslné (***non-malicious***). Mezi úmyslné hrozby lze zařadit například útoky se záměrem systémy přetížit a zamezit tak jejich fungování (Denial of Service, DoS). Neúmyslné hrozby mohou pramenit z defektů zařízení způsobených například stářím (selhání pevného disku) nebo vlivem chyby v programovém kódu (restart počítačového systému v důsledku neošetřené situace v programu řídících komponent počítačového systému).

V kybernetické bezpečnosti pak lze hovořit zejména o hrozbách, před kterými je třeba aktiva chránit. Kybernetická bezpečnost tak chrání zejména informační nebo infrastrukturní aktiva [srov. 5, s. 30].

3.4 Data, informace, znalosti

Data (nebo také údaje) jsou opakovaně interpretovatelná formalizovaná podoba informace vhodná pro komunikaci, vyhodnocování nebo zpracování nebo taktéž jakékoliv údaje zpracovávané počítačovým programem.

Informace vycházejí ze znalostí. Poskytují například popis či význam dat tak, jak je má chápat člověk. Data se informacemi stávají tehdy, když jsou v kontextu a nesou význam pochopitelný lidmi. Informace lze taktéž popsat jako význam, který je přisouzen datům [8].

Znalosti jsou takové informace, které byly zorganizovány a analyzovány, aby byly srozumitelné a použitelné pro řešení problémů nebo rozhodování a učení [srov. 8, s. 191].

Pochopení a odlišení těchto pojmů má přímý vliv na pochopení významu kybernetických hrozeb pro kybernetickou a informační bezpečnost (vizte dále). V informačních systémech, které jsou součástí kybernetických systémů, lze nalézt mnoho dat, která je třeba chránit. Podobně je tak nutné chránit některé informace (tam, kde kybernetický systém uchovává či reprezentuje data v podobě informací).

V sekci, kde budu popisovat kybernetická rizika a hrozby, s pojmy data, informace a znalosti budu pracovat ve významu definovaném touto podkapitolou.

3.5 Kybernetická versus informační bezpečnost

Informační bezpečnost zajišťuje zejména důvěrnost, integritu a dostupnost informací. Informace může mít různou podobu – elektronickou, fyzickou, dokonce může být reprezentována i jen jako znalost personálu. Pro zajištění informační bezpečnosti musejí být informace ve všech podobách ochráněny před hrozbami a původci hrozeb v jakékoli podobě, včetně fyzických, lidských i technologických hrozeb.

Kybernetická bezpečnost se oproti tomu zabývá ochranou před hrozbami, které využívají kybernetický prostor. Takové hrozby mohou útočit na informační aktiva, proto je informační bezpečnost důležitou součástí kybernetické bezpečnosti. Kybernetická bezpečnost se ale zabývá jen takovými informačními aktivy, ke kterým se dá získat přístup pomocí kybernetického prostoru.

Kybernetická bezpečnost se ale neomezuje na ochranu informačních aktiv. Její starostí je i ochrana infrastruktury a v širším kontextu (tam, kde informační systémy mají dopad na reálný svět) pak i ochrana aktiv v reálném světě (například ochrana života, zdraví, reputace, a tak dále) [srov. 5, s. 30].

Mnoho zdrojů k tématu kybernetické bezpečnosti pak propojuje kybernetickou a informační bezpečnost. Pro správné pochopení principů kybernetické bezpečnosti je ale nutné tyto pojmy nezaměňovat: kybernetická bezpečnost má mnohem širší zásah, neslouží jen k ochraně informačních aktiv a zajištění jejich důvěrnosti, integrity a dostupnosti informací. Podobně informační bezpečnost není rozsahem omezena na hrozby, které vznikají v kybernetickém prostoru.

3.6 Kybernetická bezpečnost a ochrana kritické infrastruktury

Ochrana kritické infrastruktury se zabývá ochranou před narušením, znefunkčněním či neautorizovaným ovládnutím kritické infrastruktury. Ačkoli ochrana kritické infrastruktury zahrnuje i kybernetickou bezpečnost (protože systémy kritické infrastruktury často využívají kybernetické systémy), není na ni omezena [srov. 5, s. 31].

3.7 Řízení kybernetických rizik

Tato kapitola bude popisovat řízení rizik v oblasti kybernetických systémů. Pokusím se zde popsat a zdůraznit odlišnosti kybernetických systémů a kybernetických hrozeb od běžného vnímání řízení rizik. Popíšu kybernetická rizika, jejich podstatu a možnosti, jak je řídit.

3.7.1 Co jsou kybernetická rizika?

Povaha hrozeb a rizik, které se mohou v kybernetickém prostoru objevit, je svým způsobem specifická. Jedním ze specifik kybernetických rizik je to, že se jedná v podstatě vždy o čistá rizika (tedy rizika, která – pokud nastanou – mají vždy negativní dopad na chod organizace).

Stejně tak jsou specifické i metody a techniky, které se pro řízení a hodnocení kybernetických rizik používají. Jedním ze specifik kybernetického prostoru je jeho potenciální dosah – původci hrozeb mohou být kdekoli na světě a přesto

mají potenciál napadnout a hluboce zasáhnout analyzovaný kybernetický systém. Podobně děsivě může působit i fakt, že nemalá část kybernetických hrozeb vzniká s úmyslem uškodit. Protivníci, kteří jsou původem těchto hrozeb, mají své motivy a úmysly – často nečisté. Přesto se běžně vyskytují i neúmyslné hrozby.

Kybernetické riziko lze definovat takto:

> ***Kybernetické riziko je riziko způsobené kybernetickou hrozbou [srov. 5, s. 33].***

Z definice pak lze odvodit, že kybernetické riziko nezahrnuje všechna rizika, kterým může být kybernetický systém vystaven. Například požár místnosti se servery zřejmě není kybernetickým rizikem (požár obvykle není způsoben kybernetickou hrozbou), zatímco nedostupnost dat umístěných na serverech v důsledku úmyslného přetížení datové sítě už kybernetickým rizikem je.

(V dalších kapitolách nicméně budu věnovat menší pozornost i některým rizikům, která mohou ovlivnit kybernetické systémy, ale přitom nejsou kybernetickými riziky.)

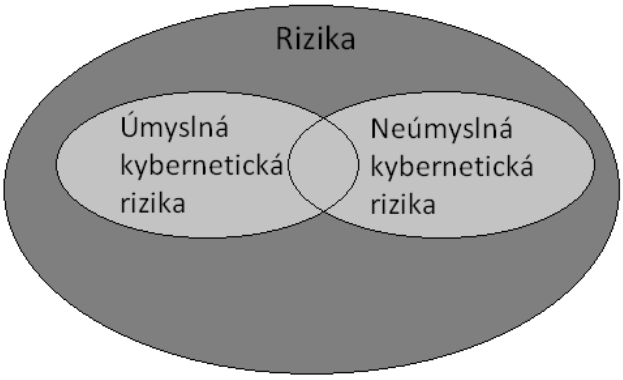
Aby bylo možné lépe pochopit povahu kybernetických rizik a jejich řízení, budu dále rozlišovat mezi ***úmyslnými a neúmyslnými kybernetickými riziky***. Úmyslné kybernetické riziko je takové, které je (alespoň zčásti) způsobeno úmyslnou hrozbou. Ostatní rizika pak označuji za neúmyslná [srov. 5, s. 34].

Některá rizika či hrozby lze v určitých případech klasifikovat jako úmyslná i neúmyslná. Například neautorizovaný přístup k citlivým datům způsobený útočníkem s úmyslem škodit bych zařadil mezi úmyslná kybernetická rizika. Zpřístupnění týchž dat v důsledku nenastavených restrikcí ve vnitrofiremním informačním systému pak bude spadat spíše do kategorie rizik neúmyslných.

K některým incidentům může dojít jen v případě kombinace úmyslných a neúmyslných hrozeb. Příkladem může být úspěšný průnik útočníka do informačního systému (úmyslný akt) v okamžiku technického selhání ochranného mechanismu (například zabezpečovacího prvku). Takovou potenciální situaci doporučuji zařadit mezi úmyslná rizika.

Kybernetická rizika tak lze definovat jako sjednocení úmyslných a neúmyslných kybernetických rizik. Průnik úmyslných a neúmyslných rizik reprezentuje rizika, která mohou být způsobena úmyslně i neúmyslně. Všechna

kybernetická rizika pak jsou jen podmnožinou rizik, kterým mohou být kybernetické systémy vystaveny. Vazbu mezi riziky, kybernetickými riziky, úmyslnými a neúmyslnými riziky ilustruje následující obrázek [srov. 5, s. 34].



Obrázek 5 - Úmyslná a neúmyslná kybernetická rizika

Existence kybernetických systémů způsobuje, že se potenciální útočníci mohou objevit kdekoli. Podobně jakýkoli kybernetický incident, nezávisle na tom, kde ve světě se vyskytne, může mít významný dopad na analyzovaný kybernetický systém.

Takový rozsah potenciálních zdrojů hrozeb, hrozeb či zranitelností vyžaduje důraz na sběr informací a dat pomocí dohledových systémů a pozorování chování systémů [srov. 5, s. 35].

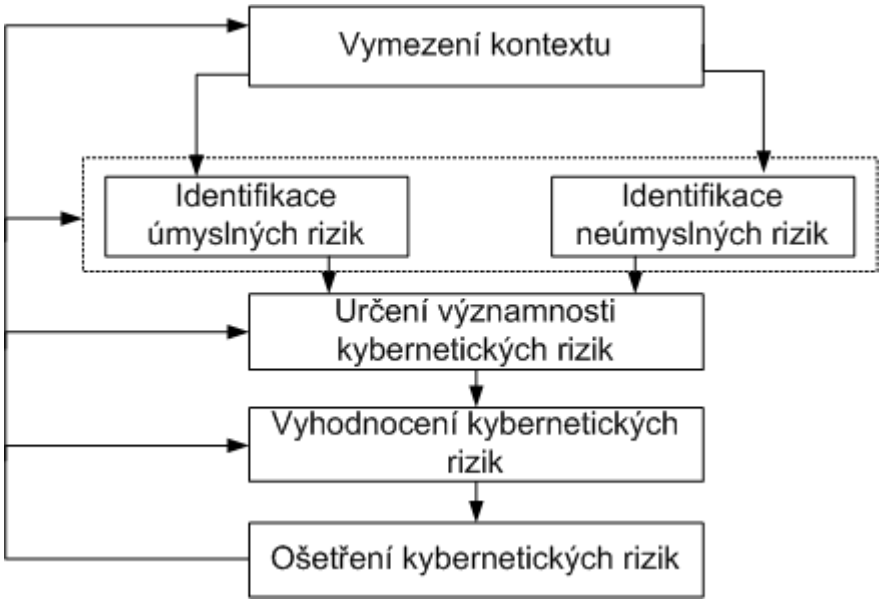
Důležitým prvkem ochrany před kybernetickými riziky jsou jasně definované postupy pro řízení komunikace v případě krizových událostí. Reakcí na incident podobného dopadu nesmí být pouze technické či právní kroky, ale je nutné postupovat podle scénářů pro krizovou komunikaci. Plány pro případ krizové komunikace tak musejí být rozšířeny o reakci na kybernetická rizika, včetně kontaktů na zodpovědné pracovníky pro řízení informační a kybernetické bezpečnosti.

3.8 Hodnocení kybernetických rizik

Od obecného přístupu k rizikům se kybernetická rizika liší zejména v potenciálním dosahu kybernetického prostoru (který může dosahovat až celosvětových rozměrů – a tak i původci hrozeb mohou být odkudkoli ze světa) a dále tím, že je množství možných původců hrozeb a hrozeb samotných obrovské.

Na následujícím obrázku je zpracován proces hodnocení kybernetických rizik [srov. 5, s. 36]. Proces vychází z procesu hodnocení rizik, je však rozšířen

v kroku identifikace rizik tak, aby byl schopen podchytit rizika úmyslná (vycházející z úmyslných hrozeb) a neúmyslná (z neúmyslných hrozeb).



Obrázek 6 - Hodnocení kybernetických rizik

Důvodem rozdělení kroku identifikace rizik je rozdílná povaha rizik, potenciálních hrozeb, původců hrozeb či zranitelností. Přístupy zvolené k jejich identifikaci se pak liší v závislosti na tom, zda se jedná o úmyslné jednání.

V případě úmyslných rizik se setkávají dva subjekty – potenciální útočník (jehož snahou je aktiva společnosti napadnout, poškodit nebo zcizit) a ten, na kterého je útočeno (obvykle společnost vlastnící aktiva, která se je snaží ochránit). Identifikace úmyslných rizik se pak snaží analyzovat možné cesty, které by pro útočníka mohly být zajímavé a je nutné je ošetřit. Zajímavost cest pro útočníka se ovšem odvíjí od jeho znalostí, schopností, dostupných prostředků, ale také od stavu techniky (některé způsoby šifrování dat je s využitím technologií roku 2016 nemožné prolomit; totéž platilo v roce 2000 pro tehdy využívané způsoby šifrování a dostupné technologie, dnes je nicméně možné některé tehdejší technologie úspěšně pokořit).

V případě neúmyslných rizik, mezi která zařazuji třeba nehody či selhání techniky, chybí motiv. Množství hrozeb, které mohou vyvolat neúmyslné riziko, je ale obrovské, téměř až neomezené. V případě neúmyslných rizik je tak vhodné vyjít z existujících aktiv („co se může pokazit?“) a následně identifikovat způsoby, jak může k ohrožení aktiv dojít. Výhodou tohoto přístupu je soustředění zájmu na ta aktiva, která je vhodné ochránit [srov. 5, s. 36].

3.8.1 Vymezení kontextu kybernetických rizik

Mezi specifika kybernetických rizik a vymezení jejich kontextu patří zejména pochopení, jak analyzovaný kybernetický systém funguje a interaguje s kybernetickým a skutečným prostorem. Díky pochopení interakcí je možné pochopit, kde se kybernetická rizika berou. Pochopení fungování systému pomáhá vyjasnit, na která aktiva je třeba se zaměřit.

Kybernetická rizika přicházejí z kybernetického prostoru a je proto třeba znát všechny cesty, kterými se útočník dokáže dostat do kybernetického systému, a kterými mohou kybernetický systém opustit data (která jsou považována za cenná aktiva). Obvykle tak v rámci hodnocení kybernetických rizik dochází k analýze způsobu práce s informacemi, s daty, dále pak k analýze infrastruktury virtuální (používaný software, aplikace, aplikačních rozhraní pro komunikaci mezi systémy) i fyzické (prostředky propojení sítí, zabezpečení zařízení informačních technologií).

Kybernetická rizika ovšem mohou ohrožovat i aktiva mimo kybernetický prostor. Může se jednat například o poškození dobrého jména, obchodní značky. Mohou způsobit výpadek příjmů, ovlivnit podíl na trhu nebo vést k vážným právním důsledkům, pokud neošetřené kybernetické riziko způsobí například únik osobních dat. V extrémních případech může dojít i ke škodě na majetku cizích osob, narušení životního prostředí nebo dokonce k ohrožení života.

Při vyhodnocování kybernetických rizik je proto třeba na takovéto případy pamatovat a neomezovat se pouze na nehmotný aspekt kybernetických systémů [srov. 5, s. 37].

3.8.2 Identifikace úmyslných rizik

> ***Válečné umění nespočívá v tom, spoléhat, že nepřítel nepřijde, jeho základem je být na něj připraven. Nespočívá v odhadu, že útok je nepravděpodobný, ale v dokonalém zabezpečení vlastní pozice [11, s. 55].***

Problém identifikace úmyslných rizik lze demonstrovat na příkladu nikdy nekončící šachové hry, ve které proti sobě hrají útočník (původce hrozby) a obránce kybernetického prostoru. Zatímco obránce je na straně organizace a jejích aktiv, která se snaží chránit, útočník se naopak snaží aktiva poškodit. Tahy, které každá ze stran provádí, jsou založeny na schopnostech a možnostech

obou stran. Ne každý tah je správný a stejně tak, jako může nesprávné ošetření některých rizik usnadnit cestu útočníkovi, může mu jeho tah i uškodit (například tím, že pokus o zneužití zranitelnosti, která je obránci již známa a proti které je systém ošetřen, vyvolá na straně obránce poplach).

Znáš-li protivníka i sám sebe, máš jisté vítězství [11, s. 73].

Identifikace úmyslných rizik se snaží předvídat tahy útočníků a včas navrhovat jejich ošetření. Schopnosti útočníků jsou velmi rozmanité – od primitivních pokusů o narušení integrity systému s využitím na Internetu volně dostupných, předpřipravených nástrojů (takoví útočníci mají v rukou předpřipravené nástroje k pronikání do kybernetických systémů, ale sami netuší, jak tyto fungují) až po velmi sofistikované tahy s využitím znalostí o vnitřním prostředí organizace, používáním pokročilých technologií za statisíce dolarů či schopností analyzovat velmi specifické, dosud nezdokumentované slabiny a zranitelnosti systémů. Jen a pouze znalost či odhad schopností a možností útočníků dokáže naznačit odpověď na otázku, jak sofistikované mohou protivníkovy tahy být.

Během fáze identifikace úmyslných rizik je tak vhodné prozkoumat potenciální původce hrozeb, potenciální útočníky a jejich schopnosti a možnosti. Na základě těchto informací je pak možné určit, do jaké míry a jakým způsobem mohou původci ohrozit chráněná aktiva [srov. 5, s. 38].

Aby bylo možné identifikovat relevantní zdroje hrozeb, je nutné se vžít do rolí potenciálních původců hrozeb – kdo by to mohl být, jakou by mohl mít motivaci a cíle, které nástroje má k dispozici, jak samotné útoky dokáže provést.

Ačkoli ve většině případů jsou původci hrozeb lidé, existují i případy, kdy se jedná o faktor neživý – například o počítačový virus. I za neživými faktory pak často bývá úmysl a účel (například poškození dat či jejich zašifrování a vydírání organizace). Za původce hrozby nakonec teoreticky vždy lze označit člověka, který za škodlivým programem stojí. Původci hrozeb mohou dále stát mimo kybernetický systém, který řízení rizik chrání, či být jeho součástí.

V dalším kroku je třeba pracovat s jednotlivými úmyslnými hrozbami a potenciálními zranitelnostmi, které mohou být zneužity. Dochází k identifikaci ***vektoru útoku*** (způsobu, jakým dochází ke zneužití) a možného způsobu interakce hrozby a kybernetického prostoru. Pro nejlepší možné pochopení je v této části identifikace rizik nutné zapojit osoby, které jsou ochraňovaným

aktivům nejblíže, od kterých lze informace získat například formou osobních rozhovorů či pracovních a diskusních setkání ve větším kolektivu.

Na základě znalostí potenciálních hrozeb je nutné zaměřit se na rozbor existujících zranitelností či identifikovaných vektorů útoku. Dále je nutné prozkoumat existující, již přijaté postupy pro ochranu aktiv či nástroje, které jsou k ochraně již použity. I v tomto případě je nutná spolupráce s pracovníky organizace a jejich okamžitá zpětná vazba. Využít lze i průzkum na Internetu volně dostupných databází zranitelností (např. databáze MITRE Common Vulnerabilities and Exposures [14], využít lze i OWASP Dependency Check [15]) následovaný průzkumem či výzkumem opatření, která proti zranitelnostem byla provedena. Pro ověření informací získaných od personálu organizace je vhodné provést jejich ověření a to například provedením vlastních penetračních testů či kontrolních testů na ošetření zranitelností.

Výsledky rozboru zranitelností pak naznačí, jak složitá může pro útočníka realizace útoku být. Na základě tohoto rozboru je nutné zjistit, jak konkrétně mohou útoky ohrozit dotčená aktiva (i ve vztahu k vážnosti jednotlivých zranitelností). Informace o tom, zda už došlo k nějakým pokusům o poškození aktiv, či zda už některá aktiva byla poškozena, mohou poskytnout záznamy o aktivitách v jednotlivých aplikacích (***application logs, audit logs***).

Identifikovaná úmyslná rizika je pak nutné zanést do seznamu rizik k jejich následnému posouzení v dalších fázích procesu hodnocení rizik.

3.8.3 Identifikace neúmyslných rizik

V případě úmyslných rizik literatura doporučuje začít s identifikací od potenciálních původců hrozeb. Množství původců hrozeb neúmyslných rizik je ale nesmírně veliké [srov. 5, s. 40] a zároveň není přítomen úmysl. Dává tak smysl postupovat obráceně – začít u identifikovaných aktiv, která má smysl chránit, a ptát se, jak může k jejich ohrožení dojít. Každá taková možnost je zároveň potenciálním incidentem. Dalším krokem je identifikace možností vzniku takového incidentu (tedy hrozeb) a na základě identifikovaných hrozeb pak následuje určení původců jednotlivých hrozeb.

Identifikaci neúmyslných incidentů napomáhá analýza reprezentace kybernetických aktiv a jejich vztahu k cíli hodnocení. Například u informačních aktiv je vhodné posoudit způsob ukládání a zpracování informací v každém

jednotlivém systému, přenášení informací v kybernetickém prostoru, či kdo z uživatelů či systémových aplikací má k datům přístup (a na jaké úrovni – například pouze pro čtení či pro čtení i zápis).

Incidenty a neúmyslné události se také často opakují – proto pro jejich identifikaci je možné použít záznamy o aktivitách v aplikacích, data ze systému sledování dostupnosti systémů či jiná relevantní historická data.

Pro identifikaci zranitelností je třeba identifikovat technické a technologické komponenty systému a dále také zaběhlé zvyky v organizaci, procesy a řízení zpřístupňování jednotlivých systémů, fluktuaci personálu a další netechnické, avšak relevantní faktory.

Mezi časté zranitelnosti lze zařadit například nepřítomné ochranné mechanismy, nekontrolovaný přístup k datům či nezabezpečená rozhraní mezi jednotlivými aplikacemi. Takové zranitelnosti snadno mohou vést k neúmyslným či náhodným událostem ohrožujícím aktiva. Například absentující ochrana proti smazání dat může vést ke ztrátě těchto dat v situaci, kdy si zbrklý pracovník splete pracovní prostor, omylem všechna data označí a smaže.

Zranitelnosti mohou plynout například i ze situací vzniklých nedostatečným proškolením personálu, zaběhlými špatnými zvyky či práce pod tlakem. Seznam typických zranitelností nalezne laskavý čtenář například v normě ISO 27005 [16].

Identifikaci hrozeb napomáhá znalost analyzovaného systému a způsobů, jak funguje. Lze zjistit, jaké události mohou vést k identifikovaným incidentům a jakých zranitelností by mohlo být zneužito. Zároveň je třeba zvážit, zda některé neúmyslné hrozby mohou být způsobeny událostmi mimo analyzovaný kybernetický prostor. Jako příklad lze uvést stav, kdy dojde k selhání vzdáleného úložiště mimo kybernetický prostor organizace, což vyvolá selhání kybernetického systému v organizaci, který je na tomto úložišti závislý.

Příklady identifikace hrozeb uvádí již jednou zmiňovaná norma ISO 27005 či dokument ***NIST risk assessment guide*** [12].

Na základě identifikovaných hrozeb je následně možné identifikovat zdroje jednotlivých hrozeb. Lze například zjistit, kdo je uživatelem systému a jaká neúmyslná rizika může způsobit. Stejně tak lze identifikovat běžné činitele neúmyslného selhání, které nemají původ v lidském činiteli – například

nepředpokládaná selhání technických zařízení, selhání vlivem stáří, přírodní vlivy či vyšší moc. K identifikaci takových činitelů opět pomohou historická data a záznamy, zkušenost pracovníků organizace či veřejně dostupná data o možných nedostatcích použitých zařízení.

Na konci fáze identifikace neúmyslných rizik jsou pak rizika zanesena do seznamu rizik pro další kroky hodnocení rizik.

3.8.4 Určení významnosti kybernetických rizik

Určení významnosti v případě kybernetických rizik má ve srovnání s běžnou analýzou rizik na několik odlišností.

V případě kybernetických rizik, za kterými je lidský úmysl, motiv, může být odhad pravděpodobnosti výskytu náročný a být zatížen velkou statistickou chybou. Kybernetické systémy nicméně obvykle poskytují i mnoho možností zaznamenávání, sledování či testování, které odhady zjednodušují. Nezanedbatelná je i veřejná dostupnost zdrojů, které lze k analýze využít.

Již zmíněná databáze zranitelností MITRE či seznam deseti největších bezpečnostních rizik, sestavovaný organizací OWASP (OWASP Top Ten Project [17]), poskytuje hodnocení závažnosti či obvyklých následků zranitelností a hrozeb a také přehled technického dopadu potenciálních útoků [srov. 5, s. 43].

Nicméně, stejně jako v případě jakýchkoli předpřipravených zdrojů, i tyto dopady je třeba během hodnocení rizik zvážit a významnost přizpůsobit analyzovaným aktivům a organizaci. Přítomnost hrozeb lze například otestovat pomocí nástrojů penetračního testování (snaha o kontrolovaný průnik). Riziko plynoucí z určité zranitelnosti pak může být nízké pro systém, který neuchovává žádná cenná aktiva (např. zkušební systém) a naopak vysoké pro systém, na jehož dostupnosti a funkčnosti je činnost organizace životně závislá.

Správné posouzení závažnosti a významnosti je tak nutnou částí hodnocení kybernetických rizik. V případě odhadů pravděpodobnosti výskytu zranitelností, hrozeb či původců hrozeb lze pak postupovat analogicky jako v případě hodnocení závažnosti.

V případě úmyslných i neúmyslných kybernetických hrozeb je tedy vhodné zjistit pravděpodobnost výskytu a závažnost zranitelností, které mohou být zneužity. Těchto dat lze následně využít pro stanovení závažnosti kybernetických rizik [srov. 5, s. 43].

3.8.5 Vyhodnocení kybernetických rizik

V návaznosti na určení významnosti rizik je třeba provést konečnou fázi hodnocení kybernetických rizik. V této fázi probíhá zejména seskupení různých rizik, jejich slučování, vyhodnocování a konsolidace.

V případech, kdy se riziko objevuje mezi úmyslnými i neúmyslnými riziky, pravděpodobnost jeho výskytu vzrůstá. Výskyty v obou skupinách je tedy třeba brát v potaz. Ve fázi ošetření je nutné přijmout taková opatření, která ochrání oba případy.

Při vyhodnocování jednotlivých rizik je nicméně vhodné ponechat rizika oddělená a tak je i vynést do matice hodnocení rizik (nebo do jiného, podobného nástroje, používaného k vyhodnocení).

Sloučení více samostatných rizik pod jedno společné riziko je možné v případech, kdy se rizika navzájem ovlivňují. Při slučování rizik je nutné věnovat pozornost hodnocení rizik, jelikož sloučené riziko může mít mnohem větší dopad, než kdybychom pracovali s jednotlivými riziky samostatně.

Jako poslední pak zůstává seskupování rizik. V některých případech je možné pro ošetření více rizik použít společné nástroje. Seskupování často proběhne u rizik stejného typu (úmyslná versus neúmyslná): například kontrola neoprávněného průniku do kybernetického systému zpravidla poslouží pro rizika úmyslná, zatímco proti neúmyslným rizikům může zafungovat opatření v podobě proškolení zaměstnanců [srov. 5, s. 44].

3.8.6 Ošetření kybernetických rizik

Vysoce technický charakter kybernetických systémů vede často k tomu, že velká většina opatření pro ošetření kybernetických rizik je zajištěna technickými prostředky. Některá opatření mohou kombinovat technické i netechnické prostředky, například kromě technického zamezení nesprávné práce s osobními daty je vhodné i proškolení zaměstnanců na totéž téma.

Z pohledu ošetření rizik přicházejí v úvahu varianty zadržení rizika, vyhnutí se riziku, odstranění či významné oslabení příčin rizika či přenos rizika na třetí stranu.

Cílem fáze ošetření kybernetických rizik je hledání a nalézání způsobů, jak omezit potenciální zdroje hrozeb a hrozby, odstranit či výrazně snížit stupeň

závažnosti zranitelností, či jiným způsobem snížit pravděpodobnost nebo závažnost možných incidentů.

> ***Dokonale uchráníš jen ta místa, na která nelze zaútočit [11, s. 39].***

V případě úmyslných hrozeb může být snaha o úplné eliminování hrozeb náročná či přímo nemožná – vždyť *„jediný skutečně zabezpečený kybernetický systém je takový systém, který je vypnutý, odpojený od sítě Internet, uzamčený v sejfu a pohřbený hluboko pod zemí. A ani pak si jeho bezpečností nemůžeme být jisti“ [18].* Autorem tohoto – možná až příliš silného – tvrzení je J. Keith Mularski, vedoucí týmu FBI pro potírání kybernetické kriminality (volně přeloženo autorem práce).

K omezení pravděpodobnosti výskytu některých hrozeb či závažnosti zranitelností je možné přijmout opatření na různých místech kybernetického systému či prostoru. Jako opatření proti neúmyslným hrozbám lze například zavést technická opatření, kterými dojde ke snížení rizika. Mezi taková opatření zařazuji například přísnější řízení přístupových oprávnění (jejich přidělování, pravidelný audit, nebo zúžení) tak, aby bylo omezeno riziko úniku citlivých dat.

Mezi netechnická opatření patří obecně například bezpečnostní školení a zvyšování povědomí o bezpečnostních rizicích, propracovanější zásady kybernetické bezpečnosti či úpravy procesů ve vztahu k ochraně kybernetických rizik [srov. 5, s. 44].

Výběr a realizace opatření proti kybernetickým rizikům nicméně zahrnuje i faktor efektivity vynaložených nákladů v porovnání s přínosem takového opatření. Již jednou zmíněná vysoká náročnost opatření pro plnohodnotné ošetření kybernetických rizik se uplatňuje i v tomto případě. Obecně je možné postupovat podle Paretova pravidla, které říká, že osmdesát procent důsledků pramení z dvaceti procent příčin. Ošetření všech původců hrozeb, hrozeb a zranitelností je obvykle tak finančně náročné, že si je mohou dovolit jen vybrané instituce, kde je bezpečnost na prvním místě (banky, armády, bezpečnostní složky státu).

Výběr opatření pro omezení rizik dále obvykle zahrnuje analýzu nákladů na pořízení, zavedení, správy, dohledu nad fungováním a údržby dostupných opatření. Některá opatření sice přinášejí výborné výsledky z pohledu eliminace

kybernetických rizik, nicméně prudce snižují výkon kybernetických systémů nebo uživatelskou přívětivost systému.

Uživatelská přívětivost sice nemusí jít přímo proti bezpečnosti, často se tomu tak ale děje. Jako příklad uvádím zabezpečení systému heslem, které musí splňovat příliš složité požadavky na konstrukci a je nutné je obměňovat v krátkých intervalech. Je-li v organizaci více kybernetických systémů a každý má svá komplikovaná pravidla pro hesla, vede to k situacím, kdy uživatelé často rezignují na bezpečnost. Hesla si pak znamenají na štítky, které ponechávají v blízkosti „zabezpečeného“ zařízení.

Případy, kdy se organizace rozhodne pro zadržení rizika, se neliší od obecného přístupu v řízení rizik. Pokud se pak riziko přemění z hypotetického ve skutečné, je na organizaci, aby vzniklé škody na aktivech dokázala nahradit z vlastních zdrojů.

Vyhnutí se kybernetickému riziku vyžaduje od organizace zodpovědný přístup a je realizovatelné zejména v okamžiku zavádění (nebo obměny) kybernetických systémů. V takových případech je stále otevřená možnost volby více či méně rizikových kybernetických systémů a organizace (nebo projektový tým) může při realizaci vybrat takovou variantu, která konkrétní riziko mít nebude. V pozdějších fázích, kdy jsou v organizaci kybernetické systémy zakořeněny, je jakákoli změna ve stávajícím systému časově, technicky i finančně natolik náročná, že už vyhnutí se riziku nemusí být možné [srov. 5, s. 45].

Varianta přenesení kybernetických rizik na třetí stranu je možná a může nabývat například podob zadání realizace subdodávky třetí straně nebo formy pojištění proti kybernetickým rizikům. Ani jedna z variant však není dokonalá – smlouva s třetí stranou sice může obsahovat klauzuli o povinném řízení kybernetických rizik stejně jako klauzuli o finanční zodpovědnosti v případě, kdy dojde k situaci z rizika vyplývající, to nicméně nemusí být dostatečné opatření. Reputace organizace či obchodní značka tak může utrpět i v okamžicích, kdy po ekonomické stránce bude riziko narušení aktiv zajištěno smluvně (a dojde k plnění ze smlouvy).

Samostatnou kapitolou je pak pojištění kybernetických rizik, které je kombinací majetkového a odpovědnostního pojištění. Ačkoli se jedná o poměrně mladou oblast pojišťovnictví, která se po roce 2000 začala rozvíjet

zejména ve Spojených státech amerických, už i v ČR existují produkty pojištění kybernetických rizik, byť v některých případech jsou vhodné pouze pro residenční zákazníky. V ČR nabízí pojištění kybernetických rizik zatím například pojišťovna AIG (pojištění CyberEdge), AXA Assistance (pojištění Cyber Risk), pojišťovací společnost Satum Czech. Pouze pro koncové zákazníky nabízí pojištění ČSOB Pojišťovna. Jedná se zároveň o rostoucí oblast s velkým potenciálem: poradenská společnost PricewaterhouseCoopers International ve studii *Insurance 2020 & beyond: Reaping the dividends of cyber resilience* [19] uvádí, že by celosvětový trh s pojištěním kybernetických rizik mohl mezi lety 2015 a 2020 vzrůst z dvou a půl miliard dolarů až na trojnásobek (7,5 mld. dolarů). I v případě pojištění ale bohužel platí totéž, co bylo zmíněno v případě přenesení rizik na třetí stranu. Pojištění většinou následky v případě rizikové situace pouze zmírní. Pro některé organizace však pojištění může být vhodným nástrojem, který doplní ostatní opatření pro zajištění proti kybernetickým rizikům.

3.8.7 Monitorování a prověřování kybernetických rizik

Vzhledem ke složitosti dnešních kybernetických systémů je prakticky nemožné jednou projít procesem hodnocení rizik, zavést jednorázová opatření a s těmito opatřeními fungovat až do skonání věků. Jak se kybernetické prostředí mění každým dnem, objevují se nové hrozby, zranitelnosti a také nová rizika.

Kybernetické systémy naštěstí dokáží těžit z přístupů automatizace – existuje nespočet možností, jak vyhodnocovat kybernetická rizika a hrozby, sledovat útočníky a přijímat opatření ke snížení rizik téměř v reálném čase. To je koneckonců nutné – útočníci, na rozdíl od organizací, nečekají a nedávají ostatním čas na dlouhé diskuse nad hrozbami. Útočníci hrozby zneužívají často krátce poté, co dojde k jejich zveřejnění – a v některých případech i dříve (jsou-li hrozby známé útočníkům, avšak nikoli veřejnosti).

Mezi praktické možnosti, jak s kybernetickými hrozbami a útočníky bojovat, tak zařazuji například uchovávání záznamů o aktivitě v aplikacích, sledování přehledů o (pokusech o) šíření nebezpečného kódu (počítačové viry, trojské koně a dalších), případně o nestandardním chování síťového provozu (kde se včas mohou ukázat pokusy útočníků o průnik do kybernetického systému).

Je tak například možné využívat těchto dat a v reálném čase je vyhodnocovat – pokud dojde k překročení předem nastavených mezí, může to indikovat probíhající útok na kybernetickou infrastrukturu organizace.

Organizace může také zavést tzv. Computer Emergency Response Team (CERT, někdy též nazýván Computer Security Incident Response Team, CSIRT), tedy tým, který bude mít na starost zejména řešení kybernetických incidentů. Takový tým musí mít znalosti o kybernetickém prostoru, kybernetických systémech organizace, o přijatých opatřeních pro snížení kybernetických rizik a, objeví-li se významná zranitelnost, musí být schopen reagovat a ošetřit rizika v jednotkách až desítkách minut.

Právě tým CERT může stanovit, které indikátory monitorovat, jak je vyhodnocovat, a při jakých mezích reagovat.

Mezi další dostupná a přijatelná opatření pro monitorování a vyhodnocování kybernetických rizik lze zařadit i tvorbu katalogu kybernetických rizik, možných hrozeb a jejich zdrojů, zranitelností a přijatých opatření. Tento katalog by pak měl být revidován či rozšiřován s každou významnou změnou v kybernetické infrastruktuře organizace. Reprezentace dat v takovém katalogu je pak plně v režii každé organizace, nicméně i zde by se měly uplatnit přístupy řízení rizik a data by měla být zpřístupněna pouze vybraným uživatelům a ve vhodné formě (ta bude bezesporu jiná v případě top managementu organizace a jiná pro architekty systémů) [srov. 5, s. 46].

3.9 Zákonná úprava kybernetické bezpečnosti v ČR

Právní úprava kybernetické bezpečnosti v ČR je definována souborem několika norem:

- zákonem č. 181/2014 Sb., o kybernetické bezpečnosti
- vyhláškou č. 316/2014 Sb., o kybernetické bezpečnosti
- vyhláškou 432/2010 Sb., ve znění z 1. 1. 2015 nebo novějším, o kritériích pro určení prvku kritické infrastruktury

3.9.1 Zákon o kybernetické bezpečnosti

Tento zákon a navázané předpisy v ČR dlouho chyběly. Zatímco soukromé organizace se kybernetickou bezpečností již zabývaly, státní správa zůstávala až

do 1. ledna 2015, kdy zákon a návazné předpisy začaly platit, bez kodifikace předpisů pro kybernetickou bezpečnost.

Zákon definuje zejména kybernetický prostor, kritickou informační infrastrukturu, významné informační systémy a významné sítě elektronických komunikací. Definuje bezpečnostní opatření, mezi která řadí technická a organizační opatření, kybernetickou bezpečnostní událost a kybernetický bezpečnostní incident. Ukládá povinnosti v oblasti evidence kybernetických incidentů, přijatých opatření a varování a ustanovuje institut vládního CERT.

Systémy, které jsou v gesci zákona, definuje příloha k nařízení vlády č. 432/2010 Sb., konkrétně její oddíl VI. (Komunikační a informační systémy), bod G. (oblast kybernetické bezpečnosti). Zákonem se dnes musí řídit jen informační systémy a komunikační infrastruktura pod správou orgánu veřejné moci. ***Nevztahuje se tedy na soukromé organizace.***

Přesto se o obsahu zákona krátce zmíním. Zákon a vyhlášky definují například konkrétní bezpečnostní a technická opatření, která musejí orgány veřejné moci v souvislosti s ochranou proti kybernetickým rizikům zavést.

Jedná se zejména o systém řízení rizik, kybernetickou bezpečnostní politiku, organizační bezpečnost a řízení aktiv. Normy také vyžadují stanovení bezpečnostních požadavků pro dodavatele a bezpečnosti lidských zdrojů, kterými zavádí povinnosti bezpečnostních školení státních zaměstnanců a úředníků (těch, kteří spadají do působnosti zákona).

Vyhláška specifikuje i řízení přístupu a bezpečné chování uživatelů, ukládá povinnosti pro zajištění zvládání kybernetických bezpečnostních událostí a incidentů a řízení kontinuity činností. Organizační opatření končí uložením povinnosti kontroly a auditu kritické informační infrastruktury a významných informačních systémů.

Technická opatření obsluhují zejména fyzickou bezpečnost, kontrolu integrity komunikačních sítí, technické prostředky pro ověřování identity uživatelů a řízení přístupových oprávnění. Zavádějí povinnou implementaci nástroje pro ochranu před škodlivým kódem, zaznamenávání činnosti infrastruktury a informačních systémů (včetně jejich uživatelů). Ukládají povinné používání nástrojů pro detekci, sběr a vyhodnocování kybernetických bezpečnostních událostí, a dále také stanovení pravidel pro šifrování dat.

Norma nezapomíná na ustanovení bezpečnostní dokumentace, definuje typy a kategorie kybernetických bezpečnostních incidentů, formu a náležitosti hlášení kybernetických bezpečnostních incidentů.

Ačkoli se tento zákon přímo nedotýká soukromých organizací, dává jim k dispozici ucelený soubor definic a postupů z oblasti kybernetické bezpečnosti, který lze uplatnit i mimo státní správu a transformovat jej do vnitrofiremních směrnic.

3.9.2 Zákon o ochraně osobních údajů

Dalším významným předpisem, který se kybernetické bezpečnosti dotýká, byť pouze částečně, je zákon č. 101/2000 Sb., o ochraně osobních údajů. Tento zákon se vztahuje na všechny organizace, které zpracovávají osobní údaje, a v § 13 odst. 4 ukládá takovým organizacím povinnosti pro informační systémy, ve kterých dochází k ukládání osobních údajů. Jde o povinnosti řízení uživatelských oprávnění, pořizování aplikačních záznamů pro zjišťování, kdy, kým a v jakém rozsahu byly osobní údaje zpracovávány, a aktivní ochrany a zabránění neoprávněného přístupu k datům a datovým nosičům s takovými daty.

4. Kybernetická rizika a hrozby

V této kapitole se budu věnovat vybraným kybernetickým rizikům, kybernetickým hrozbám a jejich předcházení.

Nejprve vymezím kontext kybernetických systémů. Následně identifikuji úmyslná i neúmyslná rizika, incidenty, hrozby a původce hrozeb.

Dále popíšu postupy, jak původce hrozeb či hrozby eliminovat nebo alespoň omezit na takovou míru, aby došlo k výraznému snížení dopadu uvedených kybernetických rizik.

4.1 Vymezení kontextu

V této části se pokusím objasnit čtenáři kontext běžných kybernetických prostředí. Ačkoli potenciálních možností je nespočet, hlavní prostředí, kterým se budu věnovat, jsou elektronické obchody a webové aplikace, infrastruktura organizace (nezávisle na tom, zda je o organizaci velikostí malou, střední či velkou korporaci), programové vybavení, cloud computing, mobilní zařízení, analyzuji koncept ‚Bring your own device' a Internet věcí. Do kontextu zahrnu i uživatele a teoretický koncept síťového modelu ISO/OSI.

4.1.1 Infrastruktura organizace

Infrastruktura organizace je soubor komponent kybernetických systémů, které společně tvoří funkční kybernetický celek – kybernetický prostor organizace.

Základní komponentou kybernetické infrastruktury organizace v roce 2016 je ***počítačová síť***, která vzájemně propojuje jednotlivé kybernetické systémy. Síť může být realizovaná pomocí kabelových (metalických či optických) vedení nebo využívat principů bezdrátového propojování systémů. Propojování jednotlivých částí sítí řídí ***síťové prvky*** (přepínače, směrovače, brány), jejichž nezanedbatelným účelem je kromě propojení sítí i ochrana jednotlivých částí (segmentů) sítě před neoprávněným průnikem.

Infrastruktura v rámci objektu organizace bývá obvykle vyhrazená (nesdílená s žádnou další organizací) a plně pod kontrolou organizace. Pro propojování

počítačových sítí mezi více fyzickými lokalitami organizace lze využít infrastruktury

- vlastní,
- pronajaté, vyhrazené (nesdílené s jinými subjekty),
- pronajaté a sdílené s jinými subjekty.

Součástí infrastruktury jsou i ***uživatelské terminály***. Mezi nejčastější typy terminálů patří

- kancelářské počítače a přenosné počítače (notebooky),
- mobilní telefony, tablety, nebo jiná mobilní zařízení
- specifická jedno- či víceúčelová zařízení jako například telefony, čtečky vstupních karet, objednávkové terminály, pokladny a tak podobně.

Terminály jsou obvykle ovládané uživateli s různými úrovněmi povědomí o kybernetickém prostředí a kybernetické bezpečnosti obecně. Jejich dostupnost není omezována na vyhrazená pracoviště či místnosti, naopak zejména terminály mobilní lze potkat na mnoha pracovištích bez dohledu jejich vlastníků.

Další nezbytnou součástí kybernetické infrastruktury organizace jsou ***servery***, což jsou (obvykle, v porovnání s uživatelskými terminály) lépe vybavené a specializované počítačové systémy, které poskytují služby výpočetního charakteru nebo služby ukládání dat. Vzhledem k charakteru poskytovaných služeb jsou servery často umisťovány do vyhrazených místností s vyšším zabezpečením a přísnějším řízením přístupu (serverové místnosti, datové sály) a jejich provoz je podpořen znásobením a vzájemnou zastupitelností energetických a datových větví (redundance jednotlivých částí infrastruktury). Podobně je redundance využívána i v samotných serverech, kde se jednotlivé komponenty (zdroje napájení, síťové prvky, výpočetní procesory, paměti či disky pro ukládání dat) vyskytují vícekrát.

Kromě fyzických komponent je součástí kybernetické infrastruktury organizace i ***programové vybavení*** (software). Popis druhů programového vybavení by vydal na samostatnou publikaci, přesto se pokusím popsat to nejdůležitější.

Základním programovým vybavením každého fyzického kybernetického terminálu je ***operační systém***, který řídí a obsluhuje komunikaci mezi hardwarem a uživatelským programovým vybavením. Mezi jeho hlavní

funkcionality patří obsluha vstupních a výstupních zařízení (klávesnice, myši, dotykové panely, zobrazovací jednotky, zařízení pro reprodukci zvuku, tiskárny, atp.), férové řízení a přidělování výpočetního času, paměťových prostředků a dalších zdrojů uživatelským aplikacím, správa úložného prostoru, ochrana a organizace dat na prostředcích určených k ukládání dat (diskové jednotky a úložiště dat). Zpřístupňuje aplikacím prostředky síťové infrastruktury a zajišťuje ochranu dat aplikací před jejich zcizením jinými aplikacemi. Může aplikacím zpřístupňovat i specializovaná připojená zařízení (např. bezpečnostní karty a hardwarové klíče).

Uživatelské aplikace pak využívají prostředků operačního systému pro realizaci vlastních výpočetních úkolů. Načítají, zpracovávají a ukládají uživatelská data, komunikují prostřednictvím síťové infrastruktury organizace s jinými uzly uvnitř i vně kybernetického prostoru organizace. Na základě uživatelských vstupů a výstupů realizují uživatelem zadané úkony, starají se o ověřování uživatelské identity a oprávnění a zaznamenávají údaje o své činnosti.

Mezi operačním systémem a hardware leží specializovaný software (***firmware***), který je nutný pro běh hardwaru. Obvykle je každý firmware pevně svázán s konkrétním hardwarem a takový hardware bez správného a funkčního firmware nemůže pracovat.

Uživatelské aplikace, operační systémy i firmware lze nalézt v různé míře v každém terminálu. V některých případech jsou tyto komponenty pevně vestavěny do terminálu bez možnosti jejich výměny či aktualizace (tento přístup se často uplatňuje u jednoúčelových zařízení), obvykle je ale možné komponenty průběžně aktualizovat a to i samostatně (tj. není nutné aktualizovat všechny části najednou).

Pro přístup do infrastruktury organizace z míst, která nejsou přímou součástí infrastruktury, se používá princip ***virtuální privátní sítě***. Součástí kybernetické infrastruktury organizace je ***koncentrátor*** virtuální privátní sítě, což je uzel síťové infrastruktury, který je přístupný z vnějšího prostředí (mimo kybernetickou infrastrukturu organizace) a umožňuje uživatelům stát se součástí kybernetického prostoru organizace i z míst, ve kterých se kybernetická infrastruktura organizace nenachází. Uživatel, který se pak na takovém místě nachází, tak může pomocí nástrojů virtuální privátní sítě sestavit ***datový kanál*** mezi svým terminálem a koncentrátorem virtuální privátní sítě.

V okamžiku, kdy je datový kanál sestaven, se pak uživatelův terminál nepřímo stává součástí kybernetického prostoru organizace.

4.1.2 Elektronické obchody a webové aplikace

Pro zřízení a provozování internetového obchodu je nutné pochopit, jak je takový obchod provozován z pohledu kybernetického prostoru a kybernetických systémů. Kybernetický prostor běžného internetového obchodu je složen z několika klíčových komponent.

První komponentou je rozhraní systému, které je přístupné pro uživatele. Taková rozhraní mohou být dostupná a ovládaná pomocí prohlížeče internetových stránek, jako nativní aplikace, kterou je třeba nainstalovat do uživatelského terminálu nebo do specializovaného terminálu. Uživatelským terminálem může být například počítač nebo mobilní zařízení (telefon, tablet). Specializovaným zařízením pak může být například pokladna či čtečka dat, která se používá v logistickém procesu pro usnadnění expedice či doručování zásilek.

Další komponentou je báze dat. Ta obsahuje data a informace o zákaznících, produktech, objednávkách či další data, která aplikace vyžadují pro fungování celého aplikačního celku.

Neméně důležitou komponentou jsou kybernetické systémy, které nejsou přímo viditelné pro uživatele, ale orchestrují fungování aplikace, řídí komunikaci mezi jednotlivými komponentami systému, či propojují aplikaci s vnějším prostředím (například se skladovými či objednávkovými systémy dodavatelů nebo zákazníků).

V naprosté většině případů elektronické obchody a webové aplikace trpí nedostatkem zabezpečení. Může se jednat o problém nedostatečného zabezpečení uživatelského rozhraní, o problematické zajištění bezpečnosti datové báze nebo o nebezpečí v orchestračních systémech.

Pro zabezpečení uživatelských rozhraní je třeba prozkoumat bezpečnostní standardy elektronických aplikací. Mezi základní principy zabezpečení takových aplikací patří použití šifrování (a tedy i vhodných šifrovacích algoritmů) pro zabezpečení komunikace mezi aplikací a jejím uživatelem, autentizace uživatelů, vhodné řízení přístupových oprávnění k jednotlivým částem systému, vnitřní zajištění konzistence dat a ochrana vstupů a výstupů.

4.1.3 Mobilní zařízení

Ačkoli ještě dvě dekády zpět mohla být mobilní zařízení jakýmsi módním výstřelkem a ani před jednou dekádou by nikdo nepředpokládal, že počet mobilních zařízení připojených k Internetu předběhne počet počítačů, dnes je situace jiná. ***Mobilní zařízení jsou všudypřítomná***, a proto je třeba k nim přistupovat s náležitým respektem a péčí.

Za mobilní zařízení v této práci považuji ta zařízení, která umožňují přístup k datové síti téměř odkudkoli, kdykoli a za jakýchkoli podmínek. Vyznačují se častou přítomností mimo kybernetický prostor organizace, ale zároveň chtějí prostředků organizace využívat. Často tak využívají virtuálních privátních sítí. Nejčastěji se jedná o přenosné počítače (notebooky), mobilní telefony, tablety, ale i chytrou (nositelnou) elektroniku jako například chytré hodinky.

Mobilní zařízení představují lákadlo pro zloděje. Obvykle má velkou cenu už samotný přístroj. Pokud se ale k přístroji a datům v něm dostane útočník, který cílí na konkrétní organizaci, které přístroj patří, může způsobit nespočitatelné škody. I z tohoto důvodu je třeba mít tato zařízení pod kontrolou, znát jejich slabiny i silné stránky, řídit, kam přistupují a mít připravené plány pro kritické scénáře, jakými je například krádež, ztráta nebo kompromitace.

4.1.4 Koncept ‚Bring Your Own Device'

Tradiční přístupy, kdy pracovníci organizací pracovali s kybernetickými nástroji, plně vlastněnými organizací, pouze v prostředí této organizace, se v posledních letech začíná měnit. S rozšiřující se dostupností přenosných počítačů a chytrých mobilních zařízení si je pořizují pracovníci i ze svých zdrojů.

Nebývá výjimkou ani situace, kdy zařízení vlastněné zaměstnancem má lepší parametry, než zařízení poskytované zaměstnavatelem. Může se jednat o parametry technické (zařízení je rychlejší, větší, déle vydrží pracovat bez elektrické sítě, má k dispozici technologii pro připojování k síti s využitím datových služeb mobilních sítí) nebo ergonomické (s počítačem se lépe pracuje, je lehčí) nebo kombinace obojího (má podsvícenou klávesnici, na které se lépe píše v noci).

V takových situacích pracovníci přicházejí s myšlenkou práce prostřednictvím takových zařízení, která vlastní oni, v kybernetickém prostředí spravovaném organizací. Koncept má anglický název ‚Bring Your Own Device'

(přines si a pracuj na svém zařízení) a zkratkové slovo BYOD. Jakkoli se na první pohled může taková myšlenka zdát nereálná, existují prostředky, jak pracovníkům vyhovět a přitom omezit kybernetická rizika, která z takových situací přirozeně plynou. To vše ovšem pouze za předpokladu, že pracovník bude souhlasit s omezením, že jeho zařízení bude (alespoň částečně) pod kontrolou organizace.

I pro organizaci může mít akceptace přístupu ‚Bring Your Own Device' výhody. V případě, kdy organizace zaměstnancům nemusí nakupovat výpočetní techniku, mobilní zařízení a programové vybavení, může ušetřit na nákladech na zaměstnance.

4.1.5 Cloud computing

Správa vlastní kybernetické infrastruktury vyžaduje od organizace netriviální úroveň znalostí výpočetních technologií, jejich správy, pravidelnou modernizaci a udržování aktuálních verzí programového vybavení.

Oproti tomu cloud computing staví na principech ***přenesení*** (alespoň některých) starostí o kybernetickou infrastrukturu na externí subjekt (třetí stranu).

V cloud computingu obvykle ***externí subjekty*** nabízí služby, které jsou dostupné ze sítě Internet nebo tuto síť využívají pro komunikaci s kybernetickou infrastrukturou organizace.

Jedním z modelů fungování cloud computingu je ***infrastruktura jako služba***. Externí subjekt se v tomto modelu stará o správu hardware (a firmware) zejména výpočetních prostředků (serverů) a síťových komponent. Hojně se využívá virtualizace, kdy jsou nad skutečnou infrastrukturou vystavěny prvky infrastruktury virtuální (ale jinak plnohodnotné a výkonem se blížící fyzické infrastruktuře). Díky virtualizaci je možné lépe škálovat vertikálně (lze snadno posílit nebo ubrat výkon výpočetní jednotky podle potřeby) i horizontálně (je-li třeba více nebo méně výpočetních jednotek, lze je snadno přidávat a ubírat).

Organizace, která chce využívat infrastrukturu jako službu, je pak odstíněna od nutností realizovat investiční akce na pořízení takových prostředků a v průběhu životnosti vynakládat další, provozní náklady. Výhodou je možnost rychlého přidání dalších výpočetních prostředků, jsou-li potřeba, a pokud jimi

externí subjekt disponuje. Nevýhodou je částečná ztráta kontroly nad hardware a síťovou infrastrukturou. Mezi typické poskytovatele infrastruktury zařazuji například Amazon Web Services (AWS) či Microsoft Azure.

Další model cloud computingu je ***platforma jako služba***. V tomto případě poskytuje externí subjekt uživateli či organizaci nástroje pro tvorbu aplikace. Vytvořená aplikace v rámci takové platformy pak sama řeší škálování výpočetních prostředků pro své fungování a organizace nemusí tyto problémy řešit ve vlastní režii. Nevýhodou bývá ***vendor lock-in***, tedy uzamčení zákazníka, při kterém tento nemůže snadno přejít od stávajícího dodavatele služby (angl. ***vendor***) k jinému. Mezi typické představitele patří například Google App Engine (nikoli Google Apps).

Poslední model cloud computingu je ***software jako služba***. V tomto modelu je služba plně vyvíjena a provozována externím subjektem a uživateli pouze zpřístupňována (s omezenou možností konfigurace). V některých případech má uživatel přístup k datům i prostřednictvím standardizovaných rozhraní (aplikačních programovacích rozhraní, ***API***) či standardizovaných protokolů (například pro přístup k elektronické poště). Typickým představitelem služby tohoto typu jsou Google Apps (elektronická pošta, dokumenty, kalendář a další nástroje on-line).

V případě služeb Cloud Computingu je třeba zaměřit se na několik oblastí: co se děje s daty, kde je služba provozována, jak je financována, jaká je dostupnost služby a odpovědnost externího subjektu. Toto vše by mělo být specifikováno ve smluvních podmínkách pro využívání služby.

V případě dat je nutné zjistit, pod jakou jurisdikcí je služba poskytována (nejčastěji podle právního řádu EU nebo USA, v případě největších poskytovatelů je často možné zvolit si umístění podle toho, jakou jurisdikci požadujeme). Dále si poskytovatel může vyhradit právo data organizace poskytnout dalším stranám, začít je používat pro své (často marketingové) účely či prohlásit, že se data, která jsou do služby umístěna, stávají výhradně jeho vlastnictvím a může si s nimi dělat, co uzná za vhodné – všechny tři případy jsou poměrně časté, a přesto organizace takové služby využívají.

Externí subjekt obvykle využívá některé z následujících možností, jak poskytované služby financovat:

- Služba je dotovaná (zřídkakdy)

- Služba je financovaná z reklam, které se uživateli zobrazují (časté)
- Služba je financovaná prodejem osobních údajů nebo dat uživatele (časté)
- Služba je hrazená organizací, která přenesla starosti na třetí subjekt (vybrané služby)

Služba může být hrazená i kombinací výše uvedeného. Pokud už uživatel (organizace) za službu „v cloudu“ platí, ***neobdrží licence*** za poskytnutí programového vybavení do výhradního užívání (jako v případě koupě programového vybavení pro výpočetní prostředí v organizaci), ale pouze ***časově ohraničenou*** možnost službu využívat.

Specifickou oblastí cloud computingu je tzv. privátní cloud. Nejčastěji se tento kontroverzní pojem vykládá jako cloudové technologie (zejména virtualizace, tedy infrastruktura jako služba) umístěné v prostorách u zákazníka (v jeho datovém sále). V tomto případě ale zákazník není plně ušetřen starostem vzniklým z provozování takové infrastruktury, jelikož se provozování těchto cloudových služeb blíží spíš provozování běžné infrastruktury organizace. Provozování ve vlastní infrastruktuře může být ovšem i výhodou, zejména bezpečnostní, pokud zákazník má jistotu, že jeho data nejsou vystavena rizikům vzniklým ze sdílení infrastruktury s ostatními zákazníky.

4.1.6 Internet věcí

Internet věcí (Internet of Things) je koncept, který přichází s myšlenkou vzájemného propojování zařízení. Objevuje se v osmdesátých letech na Carnegie Mellon University, kde je k tehdejší síti Internet připojen první prodejní automaty s Coca Colou[2].

Do povědomí veřejnosti se dostává v období kolem roku 2000 a původně zahrnuje pouze zařízení, která komunikují mezi sebou pomocí různých bezdrátových technologií a mohou tak být jednoznačně identifikována, katalogizována a spravována[3].

[2] *The "Only" Coke Machine on the Internet* [online]. *Připisováno* Computer Science Department, Carnegie Mellon University, Pittsburgh, Pensylvánie, USA, c1970 [cit. 2016-04-11]. Dostupné z: https://www.cs.cmu.edu/~coke/history_long.txt

[3] EUR-Lex. *Internet of Things — An action plan for Europe* [online]. Brusel, Belgie, 2009 [cit. 2016-04-11]. Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0278:FIN:EN:PDF

S tím, jak postupuje miniaturizace zařízení a jak se časově a objemově neomezené připojení k síti Internet stává čím dál dostupnější a na celém světě rozšířenější, se principy Internetu věcí mění, zařízení už nežijí jen ve vlastním ekosystému, ale se začínají připojovat ke skutečnému Internetu[4].

Podle výzkumů organizací ABI research a Cisco Research bude do roku 2020 k síti Internet připojeno třicet až padesát miliard ***připojených zařízení***[5, 6] a Internet věcí se pomalu mění na Internet, ke kterému je připojené všechno (Internet of Everything).

Podobně jako mobilní zařízení, i zařízení Internetu věcí budou postupně pronikat do kybernetického prostoru organizací. Budou se stávat součástí kybernetického prostoru v případech, kdy bude organizace například přecházet na elektronickou evidenci zboží a zařízení. Při komunikaci zákazníků či zaměstnanců s kybernetickými systémy budou tyto systémy komunikovat s Internetem věcí. A Internet věcí bude aktivně komunikovat s kybernetickými systémy organizací. Tedy pokud se předpovědi analytiků vyplní.

Ke komunikaci mezi zařízeními a kybernetickými systémy lze v případě Internetu věcí zvolit jeden ze dvou hlavních přístupů:

- Přímé připojení „věci“ do sítě Internet
- Existence vlastní sítě pro „Internet věcí“, která je pomocí speciálního mostu připojena do sítě Internet

V případě přímého připojení „věcí“ do sítě Internet se každé takové připojené zařízení stává součástí kybernetického prostoru sítě Internet se všemi výhodami i riziky. Mezi ty lze zařadit dostupnost zařízení z jakéhokoli místa a nutnost vhodného řízení autentizace a autorizace přístupu, šifrování a ověřování autentičnosti dat pomocí protokolů sítě Internet, ale zároveň náchylnost k chybám v implementacích takových protokolů. Mohou se také stát snadným cílem (obětí) útoků iniciovaných ze sítě Internet. Mezi typické protokoly, které

[4] *ITU Internet Report 2005: The Internet of Things*. Geneva: ITU. International Telecommunication Union, 2005.

[5] *More Than 30 Billion Devices Will Wirelessly Connect to the Internet of Everything in 2020* [online]. Londýn, Velká Británie, 2013 [cit. 2016-04-11]. Dostupné z: https://www.abiresearch.com/press/more-than-30-billion-devices-will-wirelessly-conne/

[6] *10 Predictions for the Future of the Internet of Things* [online]. San Jose, USA, 2015 [cit. 2016-04-11]. Dostupné z: http://blogs.cisco.com/cle/10-predictions-for-the-future-of-the-internet-of-things

umožňují přímé připojení zařízení do sítě Internet, lze zařadit bezdrátové sítě LTE, resp. LTE-Advanced.

Existence vlastní sítě pro „Internet věcí“ obvykle vyžaduje využívání speciálních protokolů, jako například bezkontaktní identifikace (RFID), protokol Bluetooth s nízkou spotřebou (BTLE) a další. Zároveň se využívají proprietární sítě, jako například SigFox[7] a LoRa[8]. Sítě nejsou přímo připojeny do Internetu, zařízení komunikují jen v rámci této sítě a se speciální branou. Tato brána je pak připojena do sítě Internet a je hlavně na ní, aby správně implementovala protokoly v síti Internet využívané. Zároveň je možné v případě nově objevených zranitelností v této bráně rychle zajistit jejich ošetření a tím předejít riziku napadení či poškození celého ekosystému Internetu věcí.

Nevýhodou proprietárních sítí je samozřejmě nejistota ohledně vnitřního fungování brány mezi dvěma světy a neznámé zabezpečení samotné proprietární rádiové sítě.

4.1.7 Uživatelé a lidský faktor

Ačkoli uživatelé nejsou s kybernetickým prostorem spojeni technickými prostředky (pominu-li možnost implantace identifikačních čipů pod kůži), tvoří nezanedbatelnou součást kontextu všech výše zmiňovaných oblastí. Lidský faktor stojí za tvorbou programového i hardwarového vybavení, uživatelé ovládají terminály a mají hlavní dopad na bezpečnost celého kybernetického prostoru. Je tak třeba se jim a jejich činnosti věnovat a kybernetické prostředí zabezpečit s ohledem na potřeby a rizika vznikající u uživatelů či lidským faktorem.

4.1.8 Vnější vlivy

Kybernetické systémy bývají často vystaveny vlivům, které vznikají mimo tyto systémy. Jedná se o vlivy, které mohou mít různé cíle: může se jednat o výzkumné aktivity, které se snaží zmapovat aktuální stav kybernetických systémů, aktivity neúmyslné, kdy se vlivem shody náhod vyskytne specifická

[7] PETERKA, Jiří. SIGFOX: Internet věcí bez internetu a jen pro některé věci. In: *Lupa.cz* [online]. Praha: Internet Info, s.r.o., 2015 [cit. 2016-04-12]. ISSN 1213-0702. Dostupné z: http://www.lupa.cz/clanky/sigfox-internet-veci-bez-internetu-a-jen-pro-nektere-veci/

[8] *LoRa Technology* [online]. California, USA: LoRa Alliance, 2016 [cit. 2016-04-14]. Dostupné z: https://www.lora-alliance.org/What-Is-LoRa/Technology

vnější událost s významným vlivem na kybernetický systém, nebo útočné, kdy se původce útoku snaží kybernetický systém prolomit, narušit jeho funkčnost či systém alespoň dočasně omezit.

4.1.9 Referenční model ISO/OSI

Pro lepší pochopení kybernetických hrozeb v oblasti přenosu dat a propojení (sítí) v kybernetických systémech je vhodné zevrubně popsat tzv. referenční model ISO/OSI. Tento model vznikl ve snaze standardizovat počítačové sítě a v roce 1984 byl přijat mezinárodní organizací ISO jako standard s číslem ISO 7498.

Jedná se o vrstvový model o sedmi úrovních, přičemž každá z vrstev je nezávislá a snadno nahraditelná. Jednotlivé vrstvy spolu v praxi komunikují pomocí předem definovaných rozhraní – do detailů jednotlivých rozhraní zde však zacházet nebudu a zvídavého čtenáře odkážu ke studiu další literatury[9].

Chybná implementace protokolů různých vrstev, stejně tak jako možnost útočníka napadnout konkrétní vrstvu (a vydávat se za součást komunikačního řetězce) pak vede k mnohým kybernetickým hrozbám a rizikům. Ty budu popisovat v dalších podkapitolách a odkazovat přitom čtenáře na tento popis referenčního modelu ISO/OSI.

4.1.9.1 Fyzická vrstva

Úkolem této vrstvy je přenos ***surových dat*** (jedniček a nul) mezi komunikujícími stranami pomocí fyzického média. Fyzická vrstva nijak neinterpretuje obsah dat, zajišťuje pouze jejich přenos.

4.1.9.2 Linková (spojová) vrstva

Tato vrstva staví na surových datech přenesených fyzickou vrstvou a má za úkol zajistit bezchybný přenos celých bloků dat (***rámců***), opravu poškozených rámců, případně zaslání žádosti odesilateli rámců o znovuzaslání neopravitelných rámců.

[9] ISO/IEC 7498-1:1994. *Information Technology – Open Systems Interconnection – Basic Reference Model: The Basic Model.*

4.1.9.3 Síťová vrstva

Zatímco linková vrstva zajišťuje přenos dat mezi dvěma uzly, mezi kterými vede přímé spojení, síťová vrstva již pro přenášené rámce (***pakety***) dokáže sestavit cestu mezi odesilatelem a příjemcem, i když mezi nimi nevede přímé spojení. Pakety jsou od odesilatele k příjemci náležitě ***směrovány***.

4.1.9.4 Transportní vrstva

Síťová vrstva odstiňuje transportní vrstvu od nutnosti řešit cestu mezi komunikujícími uzly. Transportní vrstva se tak zabývá jen komunikací koncových uzlů mezi odesilatelem a příjemcem. Zatímco nižší vrstvy mají omezenou velikost rámců (paketů), transportní vrstva dokáže přenést ***libovolně velký blok*** informací a (v některých případech) zajišťuje i jejich doručení ve správném ***pořadí***.

4.1.9.5 Relační vrstva

Relační vrstva má na starost řízení spojení či komunikace mezi účastníky. Kromě jiného ví, co je třeba provést k úspěšnému navázání, udržování či ukončení spojení.

4.1.9.6 Prezentační vrstva

Prezentační vrstva dříve sloužila k převodu přenášených dat mezi koncovými uzly. Dnes je většinou využívána v případech, kdy je třeba data přenášet efektivněji (a tedy provést jejich kompresi či dekompresi) nebo bezpečněji (tato vrstva pak může provádět šifrování dat).

4.1.9.7 Aplikační vrstva

Na úrovni aplikační vrstvy dochází již k přenosu dat nebo informací mezi samotnými aplikacemi na koncových uzlech komunikace. Díky několika nižším úrovním abstrakce tak spolu dokáží aplikace na různých uzlech komunikovat bez složitého řízení nejnižších vrstev.

4.2 Identifikace rizik

V souladu s procesem identifikace kybernetických rizik, který jsem nastínil v kapitole 3.8, nyní rozdělím proces identifikace na identifikaci úmyslných a neúmyslných rizik

4.2.1 Identifikace úmyslných rizik

V oblasti kybernetických rizik identifikuji tři nejčastější původce úmyslných hrozeb. Jedná se o zaměstnance, dodavatele a vnějšího útočníka.

Mezi identifikované hrozby, které tito mohou působit, patří krádež zařízení, krádež dat, bezdůvodné smazání dat, průnik do kybernetické sítě, přetížení systému, zcizení autentizačních údajů, neautorizovaný přístup, odposlech datových přenosů, úmyslně nesprávný vývoj aplikací a chyby v aplikacích a neoprávněná publikace dat.

Typické incidenty, které jsou těmito původci hrozeb a hrozbami vyvolávány, jsou krádež dat, ztráty dat, odepření služby, zcizení autentizačních údajů, neoprávněný přístup a selhání zařízení.

Typicky ohroženými aktivy jsou zákaznická a firemní data, finanční aktiva podniku (incidenty vedoucí k finančním ztrátám) a nefinanční aktiva (zejména riziko ohrožení reputace a ztráty zakázek).

Původce hrozby	**Hrozba**	**Incident**	**Ohrožená aktiva**
Zaměstnanec	Krádež dat	Krádež dat	Data Reputace Finanční ztráty
Zaměstnanec	Neautorizovaný přístup	Krádež dat	
Vnější útočník	Průnik do sítě	Krádež dat	
Zaměstnanec Vnější útočník	Přetížení systému	Odepření služby	
Vnější útočník	Zcizení autentizačních údajů	Zcizení autentizačních údajů	
Zaměstnanec Vnější útočník	Infiltrace sítě	Krádež dat Odepření služby Zcizení autentizačních údajů Neoprávněný přístup k zařízením	
Zaměstnanec Vnější útočník	Krádež zařízení	Krádež zařízení	
Zaměstnanec	Bezdůvodné smazání dat	Ztráta dat	
Zaměstnanec	Neoprávněná publikace dat	Publikace dat	

Zaměstnanec Dodavatel	Nesprávný vývoj Chyby v aplikacích	Ztráta dat Krádež dat Publikace dat Odepření služby Zcizení autentizačních údajů Zcizení identity služby	
Vnější útočník	Chyby v aplikacích		
Vnější útočník	Odposlech dat	Krádež dat Publikace dat	
Vnější útočník	Neexistující šifrování	Krádež dat Publikace dat	
Dodavatel	Předčasné ukončení podpory	Odepření služby	
Zaměstnanec	Špatná péče o kybernetické prostředí	Selhání zařízení Ztráta dat Odepření služby	

4.2.2 Identifikace neúmyslných rizik

V případě neúmyslných rizik začínám s identifikací od ohrožených aktiv, mezi která patří typicky zákaznická a firemní data, finanční aktiva podniku (incidenty vedoucí k finančním ztrátám) a nefinanční aktiva (zejména riziko ohrožení reputace a ztráty zakázek).

Možné incidenty, které vedou k ohrožení aktiv, jsou nejčastěji ztráta dat, odepření služby, neoprávněný přístup k datům a přístup k datům bez autentizace (nevyžadování autentizace, žádná autorizace). Dále zcizení dat, neoprávněný přístup po síti k zařízením, ztráta kontroly nad zařízením. Mezi extrémní incidenty patří kolaps organizace v důsledku katastrofické události, proti které neexistují havarijní a kontingenční plány v oblasti kybernetických systémů.

Hrozby, které způsobují takové incidenty, jsou zejména selhání datového úložiště či nedostatečná datová redundance, neexistující, neotestované nebo nefunkční zálohování dat, nebo ztráta přístupu k datům, která má pod svou správou zaměstnanec (v případě využívání cloud computingu). Mezi nezanedbatelné hrozby patří i přítomnost počítačových virů v kybernetických systémech organizací, přetížení aplikace a datové infrastruktury. V oblasti přístupu k datům vedou nedostatečně nastavená oprávnění, chybějící autentizace a šifrování dat. Některé incidenty mohou být vyvolány i sdílením technologických a uživatelských infrastruktur (zejm. síťových), neřízeným

zaměstnancem a jeho zařízeními (v případě využívání konceptu Bring Your Own Device). Poslední, nejzávažnější hrozba, je neexistující plán pro zotavení z katastrofické události.

Typickými původci incidentu ztráty dat jsou zastaralý hardware, nedostatečná péče správce kybernetického systému, odchod zaměstnance, nedostatečné zabezpečení terminálů.

V oblasti incidentu odepření služby jde zejména o nedostatečnou redundanci a kapacitu aplikace, zastaralou architekturu aplikace, nedostatečnou kapacitu infrastruktury a neexistující nebo nefunkční síťovou redundanci.

V oblasti dat a přístupů jde zejména o nedostatečnou péči správce dat (nenastavování oprávnění), nevyžadování autentizace a nenastavené šifrování. Neoprávněný přístup po síti k zařízením pak je často způsoben neoddělením sítí nebo nedostatečnou vzájemnou ochranou těchto sítí. V oblasti kontroly nad zařízením identifikuji jako původce zejména zařízení přítomná v kybernetickém prostředí v rámci konceptu Bring Your Own Device.

Incident kolapsu organizace v důsledku neexistujících nebo nefunkčních plánů zotavení z katastrofické události má původce v managementu organizace, jehož povinností je takový plán sestavit a kontrolovat jeho platnost a funkčnost.

Ohrožená aktiva	Incident	Hrozba	Původce hrozby
Data Reputace Finanční ztráty	Ztráta dat	Selhání úložiště	Zastaralý hardware
		Nedostatečná redundance	Nedostatečná péče správce
		Neexistující, netestované nebo nefunkční zálohování	Nedostatečná péče správce
		Ztráta přístupu k datům, které má pod svou správou zaměstnanec (cloud computing)	Odchod zaměstnance
		Počítačové viry v organizaci	Nedostatečné zabezpečení terminálů
	Odepření služby	Přetížení aplikace	Nedostatečná redundance a kapacita aplikace, zastaralá architektura aplikace

		Přetížení datové infrastruktury	Nedostatečná kapacita infrastruktury
		Ztráta konektivity	Neexistující nebo nefunkční síťová redundance
	Neoprávněný přístup k datům	Nedostatečné nastavení oprávnění	Nedostatečná péče správce
	Přístup bez autentizace	Nenastavená autentizace	Nevyžadování autentizace
	Zcizení dat	Neexistující šifrování	Nenastavení šifrování
	Neoprávněný přístup po síti k zařízením	Společné uživatelské a technologické sítě	Nenastavení oddělených sítí, nedostatečná ochrana sítí
	Ztráta kontroly nad zařízením	Neřízený zaměstnanec	Vlastní zařízení v síti (BYOD, mobilní)
	Kolaps organizace	Neexistující nebo nefunkční plán pro zotavení z katastrofické události	Management

4.3 Určení významnosti a vyhodnocení rizik

Určení významnosti a pravděpodobnosti rizik a následné vyhodnocení je individuální pro každou organizaci. Obecně jsou rizika vyšší u organizací a služeb, které jsou nějakým způsobem otevřené vnějšímu světu, nebo jsou s takovým světem propojené (například připojení do sítě Internet, umístění serveru služby ve vnitřní datové síti organizace, nebo web).

Konkrétnější příklady určení významnosti a vyhodnocení rizik již byly uvedeny v sekci *2.3.3 Určení významnosti a vyhodnocení rizik*.

Určením významnosti, pravděpodobnosti a vyhodnocení se zabývají zejména Smejkal [8], Procházková [10], Doucek [9]. V oblasti programového vybavení pak například Boehm [7].

4.4 Ošetření kybernetických rizik

Zabezpečit se proti porážce je zcela v našich možnostech, ale příležitost porazit nepřítele nám dává sám nepřítel. Dobrý

válečník se proto dokáže zabezpečit proti porážce, ale nezáleží zcela na něm, zda porazí nepřítele [11, s. 26].

Opatření, která dále navrhuji, vedou k zabezpečení vlastních kybernetických systémů. Ani přesto, že organizace realizuje všechna opatření do posledního bodu, nelze nikdy garantovat stoprocentní úspěch. Ten záleží na síle, schopnostech a možnostech nepřítele.

4.4.1 Měkká vs. tvrdá opatření

4.4.1.1 Měkká opatření

Měkká opatření jsou opatření smluvního typu, která nezajišťují ochranu technickou (k tomu slouží opatření tvrdá). Jde zejména o stanovení zásad práce s daty, výpočetní technikou a chování v kybernetickém prostoru organizace.

Zákoník práce (zákon 262/2006 Sb.) nestanovuje žádnou obecnou povinnost ve vztahu ke kybernetickým systémům, kromě obecné povinnosti zaměstnance dodržovat právní předpisy státu a směrnice zaměstnavatele. Trestní zákoník zakládá zejména povinnosti v oblasti osobních údajů (např. údaje o zákaznících), povinnosti ve vztahu k tajemství dopravovaných zpráv (data přenášená datovou sítí) a dodržování práv autorských, práv s autorskými právy souvisejícími a práv k databázi.

Na organizaci samotné pak závisí, jaká další pravidla a opatření v oblasti kybernetické bezpečnosti přijme jako vnitřní směrnice. Mezi taková pravidla patří zejména:

- Určení účelu využívání firemní elektronické pošty a firemního přístupu k síti Internet pouze pro pracovní účely
- Zákaz neoprávněné instalace programového vybavení na techniku organizace
- Zákaz jakéhokoli neoprávněného zásahu do přiděleného technického vybavení či do kybernetické infrastruktury organizace
- Stanovení pravidel pro dohled nad chováním uživatelů
- Stanovení pravidel pro využívání služeb v cloudu
- Zpřístupňování e-mailové komunikace uživatele jeho přímému nadřízenému (v odůvodněných případech)
- Hlášení bezpečnostních hrozeb, incidentů a rizik, zjištěných uživatelem

- Zásady šifrování dat, pravidel pro zabezpečený přístup k prostředkům kybernetické infrastruktury a pravidel vzdáleného přístupu do kybernetické infrastruktury organizace

Porušení takových směrnic lze sankcionovat (v extrémním případě až ukončením pracovního poměru). Na druhou stranu by kybernetické prostředí organizace nemělo být k zaměstnancům nepřátelské a aktivně bránit ve vykonávání jejich činností.

Mezi další měkká opatření mohou patřit zejména dohody o dosahované úrovni služeb, dohody o zodpovědnosti za škodu či pojištění kybernetických rizik.

Dohody o dosahované úrovni služeb (angl. ***Service Level Agreement***, SLA) a zodpovědnosti za škodu jsou uzavírány mezi organizací a externím dodavatelem služby.

Dostupnost služby, často udávaná procentuálním vyjádřením ve vztahu k časovému období (měsíc, rok), definuje minimální dobu, po kterou bude služba funkční. V případě nedodržení dohodnuté dostupnosti by měl poskytovatel služby nabídnout organizaci kompenzaci. Kompenzace nabízená v rámci služeb však nemusí pokrývat skutečné ztráty, které za uvedenou dobu mohou organizaci vzniknout. Pro příklad uvádím některé používané úrovně dostupnosti a přepočet na maximální možnou dobu výpadku při vztažení k roku používání služby:

- 99,99 % dostupnost – výpadek do cca 53 minut ročně
- 99,90 % dostupnost – výpadek téměř až 9 hodin ročně
- 99,80 % dostupnost – výpadek téměř až 18 hodin ročně
- 99,00 % dostupnost – výpadek až cca 3 dny, 16 hodin ročně

V některých případech poskytovatelé do údajů o (ne)dostupnosti nezapočítávají časy plánovaných odstávek. Každá další setina a desetina procenta, kdy se dostupnost blíží ke stu procentům, však vede k exponenciálně rostoucím nákladům na službu, a proto je nutné při výběru úrovně dostupnosti pečlivě zvážit náklady a přínosy vyšší dostupnosti, stejně jako potenciální kompenzace.

Pojištění kybernetické bezpečnosti může organizaci pomoci překlenout krizové události, které by vedly k výplatám kompenzací třetím stranám (například za nedodržení dohodnuté dostupnosti služeb). Hlavní specifika a

dostupnost pojištění byla diskutována v sekci 3.8.6 Ošetření kybernetických rizik.

Poslední významná měkká opatření jsou průběžné vzdělávací kurzy na podporu osvojení kybernetické, informační a bezpečnostní gramotnosti, které by organizace měla pro zaměstnance zajišťovat. Opakováním kurzů, podobně jako dochází k opakování školení bezpečnosti práce a zdraví při práci, si zároveň zaměstnanci zásady budou pravidelně připomínat.

Ať organizace využívá jakýkoli kybernetický systém, vždy doporučuji zpracovat a aplikovat alespoň základní zásady kybernetické bezpečnosti. Ve vztahu k zaměstnancům doporučuji definovat pravidla využívání kybernetických systémů a infrastruktury. Je vhodné nabídnout a realizovat kurzy či školení pro zvýšení kybernetické, informační a bezpečnostní gramotnosti. Ve vztahu k dodavatelům nebo odběratelům je nutné smluvně zajistit příp. pojistit zodpovědnost. Dodržování pravidel je třeba kontrolovat. Vždy se ale jedná o měkká opatření, která je vhodné podpořit i tvrdými, technickými opatřeními.

4.4.1.2 Tvrdá opatření

Ačkoli měkká opatření mohou omezit některá neúmyslná rizika a hrozby tím, že se uživatelé kybernetických systémů vyvarují potenciálně nebezpečných aktivit, schopnost uživatelů dodržovat pravidla nelze garantovat. Proto se kromě měkkých opatření používají i opatření tvrdá: jsou to taková opatření, která jsou vynucená technickými prostředky. Použitím tvrdých opatření jsou rizika snižována na přijatelnou hodnotu mnohem lépe, než opatřeními měkkými.

Mezi tvrdá opatření zařazuji všechna systémově řízená opatření, řízení přístupu na základě autentizace a autorizace, auditování, auditní záznamy, záznamy aplikací a opatření realizovaná na základě jejich analýz, aktivní sledování, oznamování a blokování podezřelých aktivit, izolaci některých technických prostředků a kritické infrastruktury, a tak podobně.

Škála technicky dostupných tvrdých opatření je veliká, a proto se jimi budu zabývat podrobněji v následujících podkapitolách.

4.4.2 Auditní záznamy

Auditní záznamy jsou v kontextu kybernetických systémů záznamy činností, které byly v kybernetickém systému provedeny, včetně informací, kdy byly provedeny a kým. Auditní záznamy obvykle poskytují dostatečnou úroveň detailu a lze z nich rekonstruovat běh událostí v kybernetickém systému. Úroveň podrobnosti dat vznikajících v rámci auditování bývá vždy závislá na nastavení systému, který auditní data vytváří.

Generování auditních záznamů obvykle není spojeno se žádným rizikem (snad s výjimkou hrozby odepření možnosti ukládat data v případě, že na úložišti těchto záznamů dojde prostor, či zranitelnosti prozrazení přístupových údajů, např. hesel, pokud se nešťastnou náhodou stanou součástí záznamu událostí). Mohou nicméně poskytnout cenné informace v případě, kdy se původce hrozby nebo hrozba samotná stává reálnou, či v případě, kdy již došlo na nejhorší scénář a riziko se proměnilo z teoretického v praktické.

Auditní záznamy často obsahují detaily postačující k identifikaci, jakým způsobem došlo k prolomení zabezpečení systému, k jakým datům měl útočník přístup či doby, po jakou docházelo ke kompromitaci systému.

Správné nastavení generování auditních záznamů by tedy mělo být automaticky součástí jakéhokoli opatření proti kybernetickým rizikům.

4.4.3 Ochrana a prevence průniků

Mezi nejčastější hrozby v oblasti kybernetické bezpečnosti patří neoprávněný průnik do kybernetického systému. Množství potenciálních vektorů útoku, které může původce hrozby využít, je obrovské a v čase se mění. Závisí primárně na rozhraních mezi kybernetickým systémem a okolním světem.

Systémy detekce a prevence průniků do kybernetických systémů (***Intrusion Detection/Prevention Systems***, IDS/IPS) jsou obvykle umístěny na perimetru kybernetického prostoru (datové infrastruktury) nebo jsou součástí kybernetického systému.

Systém detekce průniku analyzuje provoz a v případě výskytu potenciálně rizikových vzorů chování (například opakované neúspěšné pokusy o přihlášení do kybernetického systému) může takové chování zaznamenat či vyvolat

poplach. Zaznamenaná data mohou být použita pro přípravu nápravných opatření.

Systém prevence průniku funguje podobně jako systém detekce průniku, oproti kterému navíc dokáže sám realizovat možná opatření. Mezi taková opatření může patřit zablokování útočníka, nahlášení pokusů o útok CSIRT týmům či poskytovateli datové konektivity útočníka. Může také provést opravu nebo zablokování poškozených dat, aby se taková data k cílovému systému dostala ve správné podobě, nebo vůbec.

Systémy IPS nabízejí obvykle velké firmy jako Cisco[10]. V omezené podobě jsou dostupné i zdarma, například v případě operačních systémů dostupných pod svobodnou licencí (jako například Fail2ban[11]).

Systémy IDS a IPS mohou ochránit kybernetické systémy organizace před útočníky a zodpovědné osoby včas varovat při začínajícím útoku, nebo pokusy o útok samy včas zvládnout. Doporučuji proto zvážit jejich nasazení.

4.4.4 Ochrana před (distribuovaným) odepřením služby

Pro ochranu před odepřením služby, ať už centralizovaným nebo distribuovaným, je nutné na kritická místa do kybernetické infrastruktury včlenit zařízení, která analyzují a filtrují datový provoz. Tato zařízení dokáží identifikovat nenadálé a neočekávané změny v datovém provozu a v případě, kdy dojde k útoku s cílem odepřít službu, zajistit odfiltrování škodlivých dat. Samotná služba, která je chráněná takovým zařízením, pak může být stále dostupná. Lze tak například kontrolovat a omezovat podezřelý datový provoz ze zahraničí, zatímco vnitrostátní datový provoz ke službě připustit.

Zařízení mohou mít podobu hardwarových přístrojů zapojovaných do sítě (například takových, jaké nabízí Arbor Solutions[12]) nebo softwarových produktů

[10] Next Generation Intrusion Prevention System (NGIPS). *Cisco.com* [online]. [cit. 2016-04-21]. Dostupné z: www.cisco.com/c/en/us/products/security/ngips/index.html

[11] *Fail2Ban Main Page* [online]. [cit. 2016-04-21]. Dostupné z: http://www.fail2ban.org/wiki/index.php/Main_Page

[12] DDoS Attack Solutions. *Arbor Networks* [online]. 2016 [cit. 2016-04-21]. Dostupné z: https://www.arbornetworks.com/ddos-protection-products

(například produkt ochrany webových aplikací, jaký nabízí např. CloudFlare[13]). Ale i běžná síťová infrastruktura musí řešit problémy odepření služby při pokusu o takové odepření z vnitřní sítě organizace.

Dále jsou rozlišovány dva druhy odepření služby: běžné odepření služby a distribuované odepření služby.

Běžné odepření služby (***Denial of Service, DoS***) je většinou způsobeno malým množstvím uživatelů nebo chybou v návrhu systému (může se jednat o chybu v programovém vybavení, technickém vybavení, nebo o kombinaci obojího). Odepření služby také může být následek vniknutí záškodníka (kybernetického nebezpečníka) do kybernetického systému a úmyslným odstavením služby.

Distribuované odepření služby (***Distributed Denial of Service, DDoS***) je obvykle realizováno prostřednictvím zvýšené aktivity mnoha na sobě nezávislých kybernetických systémů. Zvýšení aktivity může být generováno legitimními uživateli (například v okamžiku, kdy je aplikace přetížená a odpovídá pomalu, uživatelé se netrpělivě pokoušejí znovu a znovu s aplikací pracovat a vytvářejí tak ještě větší přetížení) nebo útočníkem, který pro své nečisté úmysly využívá síť napadených a ovladatelných kybernetických systémů (tzv. ***botnet***).

O vážnosti útoků a nutnosti ochrany před distribuovaným odepřením služby se v během tří dnů v březnu 2013 přesvědčily české on-line novinové weby[14], největší český webový portál a poštovní služba[15] (Seznam.cz, Email.cz) a české bankovní domy[16], na které postupně útočila neznámá skupina útočníků. Útok

[13] Under DDoS Attack? We Can Protect You. *CloudFlare* [online]. 2016 [cit. 2016-04-21]. Dostupné z: https://www.cloudflare.com/under-attack/

[14] SLÍŽEK, David. Česká média zaplavily vlny DDoS útoku, přicházel z Ruska. *Lupa.cz* [online]. Internet Info, s. r. o., 2013 [cit. 2016-04-22]. ISSN 1213-0702. Dostupné z: http://www.lupa.cz/clanky/ihned-cz-je-nedostupny-zrejme-celime-utoku-rika-redakce/

[15] VYLEŤAL, Martin. DDoS útoky pokračují, jejich cílem se stal Seznam.cz. *Lupa.cz* [online]. Internet Info, s. r. o., 2013 [cit. 2016-04-22]. ISSN 1213-0702. Dostupné z: http://www.lupa.cz/clanky/ddos-utoky-pokracuji-jejich-cilem-se-stal-seznam-cz/

[16] DOČEKAL, Daniel, Martin VYLEŤAL a David SLÍŽEK. Weby českých bank ochromil DDoS útok, NBÚ žádá od postižených data. *Lupa.cz* [online]. Internet Info, s. r. o., 2013 [cit. 2016-04-22]. ISSN 1213-0702. Dostupné z: http://www.lupa.cz/clanky/web-ceske-sporitelny-neni-dostupny-vcetne-online-sluzeb-servis24/

přicházel z ruských internetových sítí, mohl za ním ale být kdokoli – podle časopisu Infosecurity Magazine si bylo v roce 2010 možné pronajmout síť ovládaných kybernetických systémů za pouhých šest liber na hodinu[17] a iniciovat z nich útok na cíl dle vlastní libosti.

Ať už organizace provozuje jakoukoli službu, doporučuji přijmout opatření proti odepření služby. Dostupnost produktů pro takovou ochranu je dobrá a stejně tak je přijatelná i cena za takovou službu. Cílem útoku se může stát velká organizace i malý obchod a potenciální dopady na reputaci i příjmy mohou být obrovské.

4.4.5 Autentizace uživatelů a zařízení

Základem každého opatření pro zabezpečení přístupu je prokázání identity protistrany (uživatele služeb nebo původce zprávy). Aby kybernetický systém dokázal identitu zjistit, používá se tzv. ***autentizace***. Jedná se o proces, kdy se z neznámé protistrany (uživatele, zařízení) stane protistrana známá a ověřená.

Autentizaci si lze představit tak, že kybernetický systém při pokusu o přístup vyzve přistupujícího k prokázání ***identity***. Pokud se přistupující nepokusí prokázat žádnou identitou, je mu přístup k systému zamítnut.

V případě pokusu o prokázání se pak proběhne ověření identity. Je-li ověření neúspěšné, proces autentizace se opakuje od začátku (kybernetický systém vyzve přistupujícího k prokázání identity). Je-li ověření úspěšné, kybernetický systém pak prokázanou identitu používá pro zajištění ***autorizace*** (ověření) přístupu k dalším kybernetickým zdrojům. Autentizovat lze jak uživatele, tak zařízení.

Mezi nejčastěji používané principy zjištění identity patří autentizace na základě:

- znalostí protistrany (např. PIN, uživatelské jméno, heslo, klíčové slovo)
- vlastnictví prostředku, pomocí kterého ověření proběhne (například mobilního telefonu se SIM kartou se specifickým telefonním číslem,

[17] Rental of a botnet to launch a DDoS attack is available at under £6 an hour. *SC Magazine* [online]. Haymarket Media, Inc., 2010 [cit. 2016-04-24]. Dostupné z: http://www.scmagazineuk.com/rental-of-a-botnet-to-launch-a-ddos-attack-is-available-at-under-6-an-hour/article/170882/

používaným pro ověření, dále pak lze použít fyzický nebo virtuální privátní klíč k systému)
- biometrických prostředků (otisk krevního řečiště, otisk prstu, snímek duhovky, snímek sítnice)
- schopností uživatele (například schopnost uživatele zodpovědět dotaz)

Pokročilejší přístupy provádějí ověření identity více nezávislými způsoby (tzv. ***vícefázové ověření***, multi-factor authentication). Vzhledem k náročnější implementaci (a často dražšímu provozu) se hodí tam, kde je třeba vyšší úroveň zabezpečení. Mezi nejčastější příklady vícefázového ověření patří:

- ověření přístupovým jménem, heslem (faktor znalosti) a hardwarovým klíčem (přístupová karta, faktor vlastnictví)
- ověření přístupovým jménem, heslem (faktor znalosti) a kódem, zaslaným prostřednictvím krátké textové zprávy na mobilní telefon (faktor vlastnictví)

Často využívaný, ale ne vždy správně implementovaný, je přístup ***jednotné autentizace*** ke zdrojům (single sign-on). Princip je jednoduchý: existuje jedno centrální místo, které ověřuje identitu, a všem kybernetickým systémům pak předává informaci, jestli bylo ověření identity úspěšné (a pokud ano, s kým mají tu čest). V případě prostředí Microsoft Windows poskytuje služby jednotné autentizace už samotný operační systém v rámci ekosystému Active Directory. Ten umožňuje centrálně spravovat uživatelské účty, ověřovat jejich identitu, uživatele autorizovat (vizte dále) a produkovat auditní záznamy o uživatelských činnostech.

Platnost autentizačních dat je často omezená. Například autentizace uživatele jménem a heslem nesmí projít, pokud již uživatel v organizaci nepracuje. Z pohledu životnosti autentizačních dat je vhodné zavést proces řízení životnosti autentizačních dat, tedy definovat, kdy autentizační data vzniknou, jak a kdy se mění a kdy zanikají (authentication data lifecycle).

Málokterý kybernetický systém existuje s cílem poskytovat své zdroje bez omezení všem, kteří projeví zájem. Autentizace, ideálně vícefázová, je pak nutností a musí být přítomna v každém kybernetickém systému. Je-li kybernetických systémů více a mají-li využívat stejné identity, je nutné implementovat jednotnou

autentizaci. Autentizační data je třeba řídit a pravidelně prověřovat v rámci procesu řízení životnosti těchto dat.

4.4.6 Autorizace přístupu k datům a sítím

Na základě identity zjištěné během fáze autentizace dochází v kybernetických systémech k autorizaci identifikované protistrany ke konkrétním úkonům. Autorizační proces často využívá ***seznamy přístupů*** (access lists), na základě kterých autorizaci uděluje či zamítá. Autorizovat lze jakákoli aktiva, data i kybernetické sítě.

Během autorizace přístupu k aktivům lze aplikovat jednu ze dvou ***výchozích akcí autorizace***:

- K aktivu má přístup každý kromě vyjmenovaných (ti přístup nemají)
- K aktivu nemá přístup nikdo kromě vyjmenovaných (ti přístup mají)

Výchozí akce se aplikuje v okamžiku, kdy není v seznamu přístupů žádný záznam, nebo se kdy žádný existující záznam ze seznamu přístupů neuplatnil. Volba základního principu autorizace je na tvůrcích kybernetického systému a obecně je vhodnější používat jako výchozí akci variantu „nikdo kromě vyjmenovaných."

Záznamy v seznamech přístupů mohou mít podobu od nejjednodušších (má přístup/nemá přístup) až po komplexní definici přístupových oprávnění (např. „má přístup ke čtení a zápisu souboru, ale nesmí soubor smazat ani přejmenovat" nebo „může číst data o všech zákaznících, ale měnit může pouze zákazníky, kteří mu byli přiděleni"). Podoba záznamu přístupů je často individuální pro každý kybernetický systém.

Seznamy přístupů mají často podobu ***seřazeného seznamu***, jehož zpracování probíhá sekvenčně od začátku seznamu až do konce. Je-li tak na začátku seznamu záznam „povol všem čtení" a až za ním záznam „zakaž uživateli Janu Novákovi vše", bude mít Jan Novák právo číst vše (protože pravidlo „zakaž" je až za pravidlem „povol"). To je třeba při přípravě seznamů přístupů vzít v potaz.

Podobně jako v případě autentizačních dat, i ***platnost*** autorizačních dat bývá omezená. Pokud povaha pracovní činnosti na pozici, kterou obsadil uživatel Jan Novák, vyžaduje oprávnění přístupu k datům zákazníků, načež pan Novák pozici změní na takovou, která již taková oprávnění nevyžaduje (byť stále

zůstane v organizaci), mělo by dojít k revizi (odebrání) jeho oprávnění z patřičných autorizačních seznamů. Z pohledu životnosti autorizačních dat je vhodné zavést proces řízení životnosti těchto dat, tedy definovat, kdy data vzniknou, jak a kdy se mění a kdy zanikají (authorization data lifecycle).

Každý kybernetický systém, který obsahuje citlivá data, musí implementovat autorizační principy. Je vhodné, aby takové principy implementoval i kybernetický systém, který citlivá data neobsahuje. Správce systému musí znát výchozí akci autorizace, způsob správy autorizačních seznamů, chápat význam položek autorizačních seznamů a vyhodnocování dat v těchto seznamech. Autorizační data je třeba řídit a pravidelně prověřovat v rámci procesu řízení životnosti těchto dat.

4.4.7 Bezpečnost zařízení

Bezpečnost zařízení je nutnou součástí kybernetické bezpečnosti. Organizace obvykle realizují opatření pro zvýšení fyzické bezpečnosti (ochrana před vstupy neoprávněných osob do prostor organizace).

V případě datových sálů je nutné fyzickou bezpečnost řešit pomocí fyzické autentizace a autorizace přístupu ke kybernetickým zařízením, v extrémních případech mohou být zařízení chráněna na několika úrovních. U bankovních aplikací nejsou výjimkou ani na míru vyráběné ochranné klece.

Pro osobní počítače a počítače přenosné (notebooky) se obvykle používají speciální zámky, které uzamknou počítač k pracovnímu stolu a poskytují tak základní ochranu před zcizením.

Podobným způsobem by měla být řešena bezpečnost kybernetická. Při neoprávněném vniknutí do zařízení (například při otevření počítačové skříně) je například možné vyvolat alarm a upozornit tak na možného narušitele.

Bezpečnost zařízení na úrovni programového vybavení je nutné řešit autentizací a autorizací (viz výše), žádné zařízení by nemělo poskytovat přístup bez autentizace/autorizace (tzv. otevřený přístup pro hosty, přístup bez hesel, apod.).

Správcovské účty, které obvykle mají vyšší oprávnění (a jsou tak spojeny s vyšším rizikem), by neměly být používány pro běžnou práci. Měly by mít nastavenou vyšší úroveň zabezpečení a tedy například nemožnost přihlášení

pouhým heslem (vhodnější je používat pro přístup do správcovských účtů osobní certifikáty). Správcovské účty by dále neměly být přidělovány běžným uživatelům.

Správci infrastruktury doporučuji zamezení přístupu bez autentizace/autorizace. Přidělování správcovských účtů doporučuji omezit a podmínit schválením nadřízeného nebo osoby zodpovědné za kybernetickou bezpečnost. Správcovské účty doporučuji zabezpečit ještě lépe, než běžné účty. Pokud to lze, navrhuji nepovolovat autentizaci správcovských účtů pomocí obyčejných hesel – jedná se o velmi slabou a napadnutelnou autentizaci.

4.4.8 Opatření pro zabezpečení datových sítí

4.4.8.1 Řízení přístupu zařízení do sítě a zabezpečení sítí

Podobně jako u bezpečnosti zařízení, i síť by měla využívat autentizaci a autorizaci (například pomocí protokolu 802.1x). Neautorizovaná zařízení nemají v síti co pohledávat. Není-li síť zabezpečena, může neautorizované zařízení zneužívat některé slabiny síťových protokolů. Na úrovni fyzické a spojové vrstvy může dojít k fyzickému odposlechu či předstírání identity, kdy útočník zcizí data, která pro něj nejsou určená. Síťová vrstva nezabezpečené sítě pak umožňuje útočníkovi provést odepření přístupu (vizte též podkapitolu *4.4.4 Ochrana před (distribuovaným) odepřením služby*). Příkladem odepření přístupu v oblasti datových sítí je vyčerpání dostupných zdrojů (adres přidělitelných jednotlivým počítačovým uzlům) nebo falešné tvrzení, že adresa, kterou počítačový uzel chce využít, je již v síti používána (jedná se o skutečnou hrozbu v běžné implementaci protokolu IPv6).

Kromě autentizace a autorizace je třeba pamatovat na nevyužívané protokoly. Mezi základní protokoly síťové vrstvy patří tzv. Internetový protokol verze 4 (pochází ze sedmdesátých let minulého století) a Internetový protokol verze 6 (z přelomu tisíciletí). Dnešní kybernetické systémy jsou v různé míře schopné využívat protokoly oba, nicméně je třeba je mít pod kontrolou. Pokud v síti jsou provozovány systémy, které podporují oba protokoly, ale síť zvládá pouze jeden protokol (IPv4), může útočník narušit provoz tím, že se začne vydávat za řídící prvek protokolu druhého (IPv6). Pak mu nic nebrání v tom,

aby na sebe strhl datový provoz protokolu IPv6 z kybernetických systémů – a snadno se může dostat k datům, ke kterým nemá mít přístup.

Nezávisle na tom, zda jsou v síti využívány oba protokoly, doporučuji ochranu proti možným útokům. K tomu slouží principy tzv. zabezpečení nejbližšího skoku (***first-hop security***). Moderní síťové prvky umožňují realizovat first-hop security pro IPv4 i IPv6, a dosáhnout tak maximálního zabezpečení.

Pokud je v síti zařízením nabízena otevřená konektivita do sítě Internet (s využitím veřejných adres protokolu IPv4 nebo globálních adres protokolu IPv6), doporučuji na perimetru sítě nastavit taková síťová pravidla, aby se útočníci zvenku nedostali ke zdrojům, které mají být dostupné jen z vnitřní sítě organizace. Jak nebezpečné může být zanedbání tohoto pravidla (zejména, ale nejen v případě Internetu věcí), ukazuje experiment, který realizoval Andrew Auernheimer – na tisíce tiskáren po celém světě zaslal pomocí jednoduchého postupu pseudoplakát s nacistickou tématikou.[18]

Doporučuji autentizovat a autorizovat přístup zařízení do sítě. Navrhuji realizovat ochranu před napadením na nejnižších vrstvách ISO/OSI modelu a před útoky odepření přístupu. Bez ohledu na to, který síťový protokol organizace aktivně používá, doporučuji implementovat nástroje first-hop security pro oba protokoly (IPv4 i IPv6). Na perimetru sítě navrhuji chránit organizaci před neoprávněným přístupem ke zdrojům, které mají sloužit pouze pro vnitřní potřebu organizace.

4.4.8.2 Oddělení technologických a uživatelských sítí

Aby bylo možné zajistit zabezpečení firemních kybernetických aktiv, je nutné striktně oddělovat datové sítě podle jejich použití. Přístup, kdy je v jedné datové síti přítomno mnoho druhů zařízení (výpočetní technika zaměstnanců, síťové tiskárny, telefony využívající počítačovou síť, datová úložiště), jen nahrává potenciálním útočníkům a vystavuje celý kybernetický systém rizikům.

Proto je vhodné vytvořit více sítí a ty vzájemně oddělit. Oddělení lze provést fyzicky, kdy je pro každou síť stavěna vlastní fyzická infrastruktura, nebo

[18] AUERNHEIMER, Andrew: A brief experiment in printing. *Storify.com* [online]. 2016 [cit. 2016-04-26]. Dostupné z: https://storify.com/weev/a-small-experiment-in

logicky, kdy dochází k oddělení pomocí pokročilých síťových technologií na linkové vrstvě, jako jsou Virtual Local Area Network – VLAN – nebo Multi-Protocol Label Switching – MPLS, a sítě se tak tváří jako oddělené, i když využívají společnou fyzickou vrstvu.

Obecně je vhodné mít alespoň dvě oddělené sítě: uživatelskou síť, která bude podléhat principům autentizace a autorizace přístupu uživatelů, a technologickou síť, do které jsou připojeny telefony, tiskárny, senzory a další zařízení. Pro zpřístupnění přístupu do sítě Internet návštěvníkům pomocí infrastruktury organizace doporučuji připravit pro tyto návštěvníky oddělenou síť. Komunikaci mezi sítěmi je nutné na síťové vrstvě pomocí směrovače (anglicky router, vizte následující sekci).

Nedoporučuji používání jedné sítě pro všechny typy zařízení v organizaci. Navrhuji oddělení technologické, uživatelské a návštěvnické sítě. Doporučuji zabezpečení komunikace mezi těmito sítěmi pomocí směrovače se správně nastavenými bezpečnostními pravidly.

4.4.8.3 Zabezpečení kabelových sítí

Kromě zásad popsaných v odstavci *4.4.8.1 Opatření pro zabezpečení datových sítí* vyžadují kabelové sítě ještě některé další specifické zacházení.

V rámci datové sítě organizace je třeba dbát na evidenci uživatelů datových zásuvek a ochranu nezapojováním nevyužívaných datových zásuvek. Datová zásuvka, která není přiřazena žádnému zaměstnanci, poskytuje potenciálnímu útočníkovi vektor útoku.

Pro datové sítě typu WAN, které se rozpínají po městech, krajích či dokonce více státech, je nutné dbát na zabezpečení přenášených zpráv. Datové kanály je proto třeba šifrovat dostatečně silnou šifrou, je vhodné ověřovat jejich autentičnost (obojí dokáže realizovat protokol IPSec nebo jiné řešení pro propojování privátních sítí).

Navrhuji registrovat datové zásuvky ke konkrétním uživatelům. Doporučuji nezapojovat nevyužívané zásuvky. Dodržování těchto pravidel usnadní dohledávání potenciálních problémů a znesnadní útočníkovi pokusy o průnik do sítě. Datové kanály v sítích typu WAN navrhuji zabezpečit šifrováním a ověřováním dat, čímž dojde

k realizaci ochrany proti odposlechům a útokům na infrastrukturu organizace.

4.4.8.4 Bezdrátové sítě v malé společnosti

Bezdrátové sítě hýbou světem. Následujících pár řádků se budu zabývat standardem IEEE 802.11, od jehož uvedení uplyne v roce 2017 dvacet let. Čtenář bude tento standard jistě znát pod marketingovým označením ***Wi-Fi***, obecně se jedná o standard pro lokální bezdrátové sítě (lokální je zde použito ve stejném významu jako výše uvedené lokální kabelové sítě).

Ačkoli původní standard neposkytoval dostatek prostředků pro ošetření kybernetických hrozeb, v průběhu času došlo k významnému zlepšení situace. V případě malé společnosti je tak možné zajistit základní autentizaci i autorizaci a dále i šifrování datových přenosů mezi bezdrátově propojenými zařízeními.

Vzhledem k ekonomické stránce, technologie bezdrátové sítě v malé společnosti často umožňuje pouze ***základní metody autentizace, autorizace a šifrování***.

Mezi základní pravidla pro bezdrátové sítě typu Wi-Fi patří nutnost šifrování provozu. Ačkoli původní standard šifrování nevyžadoval, je provozování takové sítě doslova hrou s ohněm. Nešifrovanou síť je extrémně snadné odposlouchávat[19]. Mezi první způsoby šifrování sítí Wi-Fi, specifikované již ve standardu 802.11, byl algoritmus WEP. Ten je však nedostačující, jelikož jej útočník dokáže prolomit za méně než jednu minutu[20]. Podobně špatně je na tom i šifrovací algoritmus WPA, který taktéž lze prolomit za velmi krátkou dobu[21].

Jediným dosud bezpečným a odolávajícím způsobem šifrování bezdrátových sítí je kombinace bezpečnostního protokolu WPA2 v kombinaci s šifrovacím

[19] ŠPAČEK, Michal: Přechod na HTTPS. *MichalSpacek.cz* [online]. 2015 [cit. 2016-04-29]. Dostupné z: https://www.michalspacek.cz/prednasky/https-ctvrtkon

[20] TEWS, Erik, Ralf-Philipp WEINMANN a Andrei PYSHKIN. *Breaking 104-bit WEP in less than 60 seconds* [online]. Darmstadt, NSR, 2007 [cit. 2016-04-29]. Dostupné z: https://eprint.iacr.org/2007/120.pdf

[21] OHIGASHI, Toshihiro, Masakatu MORII a Andrei PYSHKIN. *A Practical Message Falsification Attack on WPA* [online]. Japonsko, 2009 [cit. 2016-04-29]. Dostupné z: http://jwis2009.nsysu.edu.tw/location/paper/A%20Practical%20Message%20Falsification%20Attack%20on%20WPA.pdf

režimem CCMP (uživatelsky častější název je WPA2-AES, ze kterého CCMP vychází).

Bezdrátové sítě standardu 802.11 také podporují některé vlastnosti, které měly zlepšit uživatelskou přívětivost. Jednou z takových vlastností je protokol WPS, který měl umožnit zjednodušené nastavování zařízení (bez nutnosti zadávat složité přístupové heslo ručně). Bohužel v tomto protokolu je chyba, která umožňuje komukoli do několika hodin přístupové heslo do sítě zjistit[22]. Mezi základní doporučení tak patří ***zákaz WPS***.

Autentizace je v bezdrátových sítích standardu 802.11 spojena s použitým šifrováním. V případě malé firmy se tak nejčastěji používá kombinace ***zabezpečení a šifrování WPA2-AES s tzv. před-sdíleným klíčem*** (Pre-Shared Key, PSK). Tento klíč je vlastně autentizačním heslem pro přístup do sítě a zároveň i šifrovacím klíčem symetrické kryptografie. Správce sítě volí klíč o délce minimálně osm znaků. Nevýhodou je ***sdílení téhož klíče všemi uživateli*** bezdrátové sítě.

Autorizace v bezdrátové síti v případě malé firmy může mít podobu ***seznamu výslovně povolených zařízení*** (white-list; povolují se podle fyzické, tzv. MAC, adresy zařízení). Méně obvyklá je pak autorizace, která umožňuje přístup všem zařízením a pouze vyjmenovaným zařízením přístup blokuje (black-list; blokování probíhá taktéž podle fyzické adresy zařízení). Jelikož ale útočník může fyzickou adresu snadno změnit a tvářit se tak jako autorizovaný uživatel, jedná se o autorizaci, která zabezpečení sítě zvyšuje jen minimálně. Zařízení na seznam přidává správce bezdrátové sítě.

Mezi doporučované praktiky patří ***oddělení firemní a návštěvnické bezdrátové sítě*** na úrovni fyzické vrstvy ISO/OSI modelu – tedy použít pro každou ze sítí jiný název sítě a jiné heslo pro šifrování. Návštěvnická síť také pravděpodobně nebude omezovat přístup neautorizovaných zařízení pomocí black-listu (autorizace bude umožněna všem).

Je-li využívání bezdrátových sítí nezbytné a není-li možné využívat zabezpečení bezdrátových sítí pomocí technologií pro střední a velké organizace, navrhuji zabezpečit bezdrátovou síť

[22] BONGARD, Dominique. WPS Insecurity. *8th International Conference on Passwords (Passwords14 Norway)* [online]. 2014 [cit. 2016-04-30]. Dostupné z: http://www.passwordresearch.com/papers/paper503.html

pomocí WPA2-AES s dostatečně dlouhým přístupovým heslem. Přístup do firemní sítě navrhuji umožnit pouze zařízením se známými fyzickými adresami. Dále doporučuji zakázat nebezpečný protokol WPS a realizovat oddělení firemní a návštěvnické sítě.

4.4.8.5 Bezdrátové sítě ve střední a velké organizaci

Podobně jako v malé společnosti, i střední a velké organizace používají pro své zaměstnance a technologická zařízení sítě standardu 802.11. Platí zde stejná doporučení pro nepoužívání vybraných vlastností standardů bezdrátových sítí. Oproti malé firmě mají ale střední a velké organizace často k dispozici lepší zařízení pro tvorbu bezdrátových sítí a tak mohou použít i ***pokročilejší řízení přístupu.***

Za předpokladu, že organizace má k dispozici centrální autentizační a autorizační seznamy (databáze, servery), lze každého připojeného uživatele k síti ***autentizovat jeho vlastním uživatelským jménem a heslem*** a na základě přidělených oprávnění pak autorizovat (umožnit nebo zamítnout) přístup do sítě**.** Bezdrátová síť pak používá zabezpečení ***WPA2-Enterprise v kombinaci s firemním autentizačním a autorizačním serverem*** (ten využívá technologie RADIUS). Jako malý bonus pak toto řešení umožňuje zaznamenávat a dohledávat, kdo, kdy, jak dlouho a odkud byl k síti připojen.

Ve střední a velké organizaci navrhuji zabezpečit síť organizace před hrozbou neoprávněného průniku pomocí technologie WPA2-Enterprise v kombinaci s firemním autentizačním a autorizačním serverem (RADIUS). Uživatelé budou mít individuální přístupová hesla a správce lepší kontrolu nad autorizací přístupu. Organizace navíc získá přehled o tom, kdo, kdy, na jak dlouho a odkud se k síti připojil.

4.4.8.6 Vzdálený přístup do sítě organizace

Vzdáleným přístupem se rozumí sestavení a využívání kanálu pro přístup do kybernetického prostoru organizace z místa, které není součástí tohoto kybernetického prostoru. Typickým příkladem je vzdálený přístup zaměstnance na cestách či z domova.

Jelikož vzdálený přístup otevírá cesty k aktivům organizace z prostor, které obvykle nejsou důvěryhodné, je třeba jej řádně chránit. Je tedy nutné využívat

principů ***autentizace*** (umožnit vzdálený přístup jen oprávněným uživatelům) a po otevření kanálu mezi vzdáleně přistupujícím a kybernetickým prostorem organizace pak pomocí principů ***autorizace*** zajišťovat přístup jen k těm aktivům, ke kterým má vzdáleně přistupující obvykle (při práci v kybernetickém prostoru organizace) přístup. Je také nutné do ***auditních záznamů*** zaznamenávat pokusy (úspěšné i neúspěšné) o vzdálené přístupy. Samotný komunikační kanál pak doporučuji ***šifrovat*** moderní šifrou (např. AES).

Při udělování oprávnění vzdáleného přístupu je třeba postupovat podle zásad správy autentizace a autorizace, tedy ***řídit se procesem*** přidělování, odebírání a změn takových přístupů.

Bez vzdáleného přístupu v dnešní globalizované době přežije málokterá organizace. Vzdálené přístupy je ale nutné mít pod kontrolou a řídit je. Dále je nutné dodržovat principy autentizace, autorizace a auditování. Kanál vzdáleného přístupu doporučuji šifrovat.

4.4.8.7 Síťová redundance

Vhodným způsobem pro zajištění spolehlivých síťových služeb je redundance, kdy jsou datové cesty mezi zařízeními jištěny vícenásobným zapojením. Mezi typické příklady síťové redundance je možné zařadit více nezávislých datových tras (vedených jinou cestou v objektu nebo i mimo objekt), případně více bezdrátových přístupových bodů se stejným názvem a nastavením, kdy se přístupové body mohou vzájemně zastupovat.

Redundantní datové cesty mohou pracovat v režimu jedna cesta aktivní-ostatní cesty záložní (některá ze záložních cest přebírá roli aktivní cesty, pokud doposud aktivní cesta přestane fungovat), nebo v režimu sdílení zátěže, kdy je aktivních více cest naráz a datový provoz se mezi ně rozkládá.

Pokud organizace provozuje síťovou infrastrukturu, doporučuji realizovat síťovou redundanci a to jak uvnitř organizace, tak i navenek (např. pro přípojku k síti Internet). Organizace tak získá zálohu pro případ selhání jedné z datových linek a při vhodném nastavení může docílit i vyšší propustnosti datových kanálů.

4.4.9 Ošetření využívání mobilních zařízení

Na mobilní zařízení se vztahují již dříve zmíněná opatření. Kromě nich je ale třeba počítat s některými hrozbami, které jsou pro mobilní zařízení specifické. Jde zejména o ztrátu či zcizení zařízení a o registraci zařízení pro přístup do sítí.

Ať už se jedná o přenosný počítač (notebook), mobilní telefon, tablet, chytré hodinky či jiné zařízení, je třeba zajistit bezpečnost dat v nich uložených a ošetřit situace, kdy dojde k bezpečnostním incidentům.

Pro zajištění bezpečnosti dat je nutné šifrovat obsah zařízení (všechna úložiště v zařízení), řídit přístup do zařízení (nedovolit přístup bez autentizace a autorizace), mít možnost zařízení vzdáleně ovládnout a vyčistit z něj data, případně zařízení lokalizovat.

V případě mobilních telefonů a tabletů se pro zajištění této úrovně bezpečnosti hodí používat programové vybavení pro správu mobilních zařízení (Mobile Device Management, MDM), jako je například MobileIron[23]. Pro přenosné počítače je vhodné použít kombinaci správy firemních bezpečnostních zásad (například pomocí služeb Active Directory) a bezpečnostního softwaru jako Absolute DDS[24] (dříve Computrace).

Pokud je přístup do sítě chráněn, je nutné každé nové mobilní zařízení do korporátní sítě zaregistrovat (povolit mu přístup – autentizovat a autorizovat je).

Kromě standardních bezpečnostních pravidel je třeba obsah mobilních zařízení šifrovat, řídit na nich vzdáleně bezpečnostní zásady pro autentizaci a autorizaci, mít možnost je vzdáleně ovládat, smazat, případně lokalizovat.

4.4.10 Ošetření ‚BYOD'

Principy ošetření ‚BYOD' dále rozšiřují ošetření mobilních zařízení. Zatímco v případě vlastních mobilních telefonů a tabletů je obvykle možné využít stejné

[23] Možnosti zmiňovaného nástroje může laskavý čtenář prozkoumat na internetových stránkách společnosti MobileIron, dostupných na https://www.mobileiron.com/en/solutions/enterprise-mobile-management-emm

[24] Popis funkcionality Absolute DDS je k dispozici na https://www.absolute.com/en/products/dds

bezpečnostní nástroje, zásady a pravidla, jaká se používají pro zařízení poskytnutá organizací.

V případě vlastních přenosných počítačů (na které se princip ‚BYOD' také obvykle uplatňuje) je ale situace složitější. Obecné přístupy řízení bezpečnosti v organizaci (například centrálním řízením, autentizací a autorizací pomocí nástrojů Active Directory v prostředí Microsoft Windows) obvykle nejsou pro vlastní přenosné počítače použitelné (došlo by k výraznému omezení uživatele) nebo vůbec dostupné (uživatel nepracuje s platformou Microsoft Windows a tedy centrální řízení bezpečnosti nelze vůbec použít). Proto organizace, které ‚BYOD' umožňují, využívají technik virtualizace aplikací a pracovní plochy. Uživatel pak prostřednictvím webového prohlížeče nebo specializovaného programu přistupuje k aplikacím, které organizace umístí do virtualizovaného pracovního prostředí. Aplikace se pak tváří jako nativní: panuje zdání, že aplikace jsou spuštěné přímo na soukromém počítači uživatele. Ve skutečnosti jsou spuštěny na počítačovém serveru organizace a k uživateli se přenáší jen ovládání vstupů (myš, klávesnice), výstupů (zobrazení, tisk). Aplikace má též zpřístupněné uživatelovy soubory a složky. Mezi příklady produktu, který umožňuje podobné fungování v režimu ‚BYOD' (ale nejen v něm), patří Citrix App and Desktop Virtualization[25].

‚BYOD' si tak zachovává svůj původní účel, tedy umožnit uživateli používat jeho zařízení, a zároveň zprostředkovává zabezpečené prostředí organizace s plným řízením autentizace, autorizace.

Oproti mobilním zařízením poskytnutým organizací není nicméně v případě ‚BYOD' automaticky udělován přístup do datové sítě organizace, protože nad některými jejich aspekty (zejm. v případě přenosných počítačů) nemá organizace plnou kontrolu.

Zařízení v režimu ‚BYOD' doporučuji šifrovat a řídit stejně jako běžná mobilní zařízení (jde-li to). Pokud to není možné, navrhuji použít technik virtualizace pracovní plochy. Zařízením v tomto režimu ale nedoporučuji přímý přístup do datové sítě organizace (není-li to bezpodmínečně nutné), mohou způsobovat bezpečnostní rizika.

[25] App and Desktop Virtualization. *Citrix.cz* [online]. 2016 [cit. 2016-05-01]. Dostupné z: https://www.citrix.cz/solutions/desktop-virtualization/overview.html

4.4.11 Ošetření využívání cloud computingu

V případě cloud computingu se v této části omezím na způsoby licencování a technické realizace. Bezpečnosti využívání produktů cloud computingu se budu věnovat v další části, a to *4.4.12 Ošetření bezpečnosti a konzistence dat*.

Organizace by měla v případě cloud computingu pečlivě prozkoumat, jaký je licenční model takové služby. Licence obvykle může zapovídat využití v podnikovém prostředí (buď úplně, nebo v případě verzí zdarma). Zároveň je nutné pečlivě prozkoumat model licencování takových produktů a jejich ceny.

Kromě licence je vhodné prozkoumat i datovou jurisdikci cloud computingu a využívat spíše služeb, které jsou pod evropskou jurisdikcí.

Specifickou skupinou je privátní cloud computing – pokud bude technologie umístěna v datových sálech organizace a plně pod interní správou, je obecně možné cloud computing doporučit (zejm. oblast virtualizace může přinést organizaci významné úspory za infrastrukturu). Má-li být privátní cloud pod částečnou nebo úplnou správou externího subjektu, je nutné pečlivě obsloužit případy, kdy může externí subjekt přijít do styku s firemními daty (nebo dokonce s osobními údaji zákazníků).

V případě cloud computingu je nutné znát licenční model, prozkoumat jeho kompatibilitu s představami organizace. V případě privátního cloudu je nutné vyřešit otázky správy a případné ochrany firemních či zákaznických dat (je-li správa privátního cloudu řešena externím subjektem).

4.4.12 Ošetření bezpečnosti a konzistence dat

Kromě základního řízení v bezpečnosti přístupu k datům prostřednictvím autentizace, autorizace, auditních a aplikačních záznamů je pro bezpečnost a konzistenci dat potřeba zabezpečit ještě několik dalších oblastí. Těmi jsou: zálohování, šifrování dat na externích datových nosičích a řízení dostupnosti použitelných externích nosičů, využívání cloudových služeb pro ukládání dat, řízení bezpečnosti dat v e-mailové komunikaci (uvnitř i vně firmy). Nezanedbatelná je i datová redundance a plány pro zotavení z katastrofických událostí.

4.4.12.1 Zálohování dat a datová redundance

Data běžně vznikají a zanikají. Občas se ztratí či poškodí vinou technologie, někdy je vina na straně uživatele, občas může jít o aktivitu útočníka. Data, která jsou digitálními aktivy, je nicméně třeba před ztrátou či poškozením chránit. K takovému účelu slouží zálohování dat a datová redundance.

Zálohování dat je proces, kdy je z existujících dat vytvořena kopie a ta je umístěna odděleně od původních dat. V některých případech je záloha umístěna na stejném úložišti, jako původní data – v případě poruchy tohoto úložiště je tak ztracena záloha i původní data. Pokud je záloha umístěna na jiném úložišti, které je ale trvale dostupné z prostředí, kde vznikají původní data, může kompromitace původního prostředí vést k poškození nebo ztrátě i zálohovaných dat. Obě nevýhody dokáže vyřešit zálohování na jiná (off-line) média, která jsou následně umístěna na bezpečné místo (např. trezor, bankovní schránka).

V případě zálohování dat tak lze doporučit následující opatření:

- Proti selhání úložiště, kde jsou umístěna původní data, lze použít redundanci úložiště (zrcadlení, příp. úložiště s paritou dat – technologie RAID)
- Zálohovaná data je vhodné umisťovat na vzdálené, trvale připojené úložiště (které se v ideálním případě rozprostírá přes více fyzických lokalit)
- Z trvale připojeného úložiště je vhodné data odlévat na fyzické médium (datová páska, DVD, Blu-ray, CD, flash-disk), které může být umístěno do bezpečnostní schrány. Jde-li o data opravdu důležitá, mohou být umístěna na více fyzických médií, a tato média pak rozprostřena do více bezpečnostních schrán.

Zálohování by mělo probíhat pravidelně, alespoň jednou denně. Dochází-li během jednoho dne k velkým změnám v datech, je možné zálohovat i častěji. Proces zálohování by měl být prověřován nástroji monitoringu, aby nedošlo k incidentu, že data zálohována nebudou, o kterém se navíc nikdo nedozví.

Životnost záloh a schopnost obnovy z těchto by měla být testována. Pravidla pro četnost takových testovacích obnov budou individuální pro každou organizaci, doporučit lze interval jednou měsíčně.

Doporučuji používat úložiště s datovou redundancí. Dále pak zálohování na jiná úložiště, než která obsahují zálohovaná data.

Jako ochranu před poškozením on-line záloh navrhuji zálohování i na média, která bude možné umístit do bezpečnostní schrány, které doporučuji využívat. Navrhuji zálohovat alespoň jednou denně a životnost a schopnost obnovy ze záloh pravidelně testovat.

4.4.12.2 Šifrování dat na externích nosičích

Doporučuji dbát na bezpečnost dat, která jsou umisťována na externí nosiče (CD, DVD, Blu-ray, USB flash-disk, paměťové karty a podobné). Buď celé externí nosiče, nebo alespoň jednotlivé soubory doporučuji šifrovat.

Pro šifrování celých nosičů lze použít nástroje jako Microsoft Bitlocker To Go nebo VeraCrypt (následovník kdysi populárního nástroje TrueCrypt). Bitlocker To Go je součástí Microsoft Windows ve verzích pro podniky (Professional, Enterprise, Ultimate). VeraCrypt je dostupný zdarma, nicméně správce počítače jej musí nejprve nainstalovat.

Šifrování jednotlivých souborů a adresářů je možné pomocí většiny nástrojů pro komprimaci dat (namátkou: 7zip, který je zdarma, dále např. WinRAR, WinZip, které jsou placené).

Heslo pro dešifrování nosičů či souborů nesmí být nikdy sděleno kanálem, kterému nedůvěřujete (například nezabezpečený e-mail). Pro předání hesla doporučuji využít nezávislý kanál (například je možné heslo protistraně zatelefonovat nebo odeslat pomocí krátké textové zprávy). Pokud ani těmto kanálům není možné důvěřovat, doporučuji heslo protistraně sdělit osobně.

V případě využívání externích nosičů doporučuji jejich obsah šifrovat. Šifrovat lze jak celý nosič, tak jednotlivé soubory. Nástroje pro šifrování jsou dostupné i zdarma. Heslo k šifrovaným nosičům či souborům nedoporučuji předávat nedůvěryhodným kanálem.

4.4.12.3 Dostupnost externích nosičů

V krajních případech může správce kybernetického systému využívání externích nosičů (Blu-ray, DVD, CD, USB flash-disk, paměťové karty a podobné) omezit. Uživatel v takovém případě nemá možnost omezený externí nosič vůbec připojit (nebo má možnost jej připojit, ale nedostane se k datům na něm uloženým, případně na nosič nemůže pouze zapisovat).

Tento způsob omezování je však poměrně drastický.

Pokud organizace uživatelům nevěří, může jim omezit k externím datovým nosičům přístup. Jedná se však o poměrně drastické opatření, které uživatelům může dost zkomplikovat výkon pracovní činnosti.

4.4.12.4 Využívání cloudových služeb pro ukládání dat

Ukládání dat mimo infrastrukturu organizace je obecně vzato velmi špatný nápad. Ačkoli existuje mnoho služeb pro ukládání dat (některé jsou i zdarma, případně si za jejich využívání zaměstnanci mohou z vlastní iniciativy platit), málokterá z nich bude splňovat požadavky na bezpečnost, datovou jurisdikci, autentizaci a autorizaci pro firemní účely, šifrování dat, případně převzetí dat po odchodu zaměstnance.

Nepoužívání neřízených úložišť dat (např. Dropbox, Google Drive, Microsoft OneDrive, Ulož.to, Evernote) lze zaměstnancům doporučit jako měkké opatření. Technicky lze používání takových úložišť zamezit při přístupu z firemní infrastruktury, ale omezení už se nevztáhne na případ, kdy zaměstnanec použije taková úložiště z vlastního zařízení nebo z internetové konektivity mimo vlastní organizaci.

Častým problémem těchto dat je absence autentizace a autorizace, příp. nenapojení na autentizační a autorizační služby organizace. To vede k neřízenému zpřístupňování dat jiným zaměstnancům a zároveň k nemožnosti převzetí dokumentu jiným zaměstnancem v případech, kdy zaměstnanec společnost opustí (nebo je s ním ukončena spolupráce).

Problém bohužel lze řešit pouze osvětou a poskytnutím adekvátních prostředků organizací pro tytéž účely, jaké zaměstnanec hledá u externího dodavatele. V případě služeb privátního cloudu, kdy je infrastruktura ve správě organizace, se obvykle výše uvedené výtky neuplatní.

Navrhuji zaměstnancům doporučit nevyužívat cloudové služby, případně jejich využívání administrativně zakázat. Nad daty, která se v takových službách objeví, ztrácí organizace kontrolu. Je-li dostupná technologie pro znepřístupnění těchto služeb, může organizace jejich využívání zablokovat technicky. V případě služeb privátního cloudu není situace tak problematická a proto doporučuji mírnější přístup.

4.4.12.5 Řízení bezpečnosti dat v e-mailové komunikaci

Komunikaci v rámci firmy je možné šifrovat. Pokud jsou zasílány citlivé údaje, které by útočník neměl vidět, je jejich šifrování nutné. Šifrování e-mailové komunikace mimo infrastrukturu organizace je obvykle náročnější na realizaci (je nutné si s protistranou vyměnit veřejné klíče pro šifrování), nicméně také možné, proto doporučuji šifrovat i tuto formu komunikace. Citlivá data e-mailovým komunikačním kanálem, pokud možno, doporučuji vůbec nezasílat.

Navrhuji zprovoznit šifrování uvnitř a vně kybernetické infrastruktury organizace. Doporučuji e-mailovou komunikaci šifrovat, pokud obsahuje citlivá data. Citlivá data doporučuji e-mailem raději nezasílat vůbec.

4.4.12.6 Plány pro zotavení z katastrofických událostí

Katastrofické události nastávají, i když je akceptace tohoto faktu obtížná. Proto je třeba mít připravené plány, jak se s takovými událostmi vyrovnat. Nesprávné jednání v okamžiku katastrofické události může mít velmi negativní dopad na vliv a chod organizace. V extrémních případech může dokonce vést k zániku organizace, která nebude schopná plnit své primární poslání (podnikání).

Důrazně doporučuji připravit a otestovat plány pro případ zotavení z katastrofických událostí. Pro takové události je nutné mít aktuální, funkční a testované zálohy dat, stejně jako postupy instalace programového vybavení.

4.4.12.7 Ochrana dat před škodlivým softwarem

V některých případech nebezpečného chování může uživatel do svého počítačového systému zanést škodlivý kód, který může způsobit ztrátu dat, případně data zpřístupnit neautorizovaným uživatelům, nebo data zašifrovat a za jejich odšifrování požadovat výkupné.

Mezi nejčastější typy takového škodlivého kódu patří viry, trojské koně, malware a ransomware.

Viry a trojské koně napadají uživatelův počítač, běží na pozadí a provádějí různou nečistou činnost, přičemž se zároveň mohou množit a rozšiřovat. V některých případech se maskují proti odhalení (tzv. rootkity), v jiných se vůči

uživateli tváří jinak, než čím opravdu jsou (trojské koně). Malware se obvykle snaží šířit z napadeného systému dál a zároveň uživateli nekontrolovatelně zobrazuje reklamy (často na nelegální produkty). Ransomware zašifruje některá uživatelská data a za poskytnutí dešifrovacího klíče požaduje výkupné.

Proti tomuto typu škodlivého programového vybavení lze bojovat jen aktivní ochranou. Tu lze realizovat pomocí specializovaných ochranných programů, zejm. antiviru a antimalware. Oba programy by měly být na každé uživatelské i serverové stanici a monitorovat provoz. V případě detekce škodlivého kódu pak takový kód okamžitě izolovat a informovat o incidentu správce sítě. Aby detekce byla spolehlivá, je nutné pravidelně a často (obvykle denně) aktualizovat databázi antiviru a antimalware (databáze obsahuje popis detekce škodlivého kódu).

Organizace nesmí podcenit schopnost uživatelů zanést do firemní infrastruktury škodlivý kód. Doporučuji proti škodlivému kódu aktivně bojovat používáním antiviru a antimalware s pravidelnými aktualizacemi databáze. Antivir a antimalware doporučuji neumisťovat pouze na klientské stanice, ale použít je i na serverové straně. Doporučuji kontrolovat na přítomnost škodlivého kódu vše, co může být vyprodukováno uživatelem.

4.4.13 Ošetření bezpečnosti programového vybavení

Bezchybný software neexistuje. Má-li být programové vybavení užitečné, stane se dříve či později komplexním souborem programového kódu od různých autorů, s různou mírou otestování. V čase se často mění zadání a software je průběžně rozšiřován nebo jsou z něj odebírány některé funkcionality. To vše vede k tomu, že vytvořit bezchybné programové vybavení je úkol nesmírné složitosti. A tak ke slovu opět přichází Paretovo pravidlo – testují se ty nejdůležitější scénáře, řeší se jen skutečně palčivé problémy.

Proti chybám však lze bojovat. V oblasti programového vybavení je třeba sledovat bezpečnost v celém životním cyklu programového vybavení, alespoň tak je možné dosáhnout určité úrovně zabezpečení. Životní cyklus programového vybavení zpravidla zahrnuje fáze

1. návrhu, vývoje a testování
2. podpory, provozování a údržby

3. ukončení podpory a používání aplikace

Dále je třeba sledovat, jaké programové vybavení se v organizaci používá a případně zakročit proti potenciálně rizikovému vybavení; k tomu slouží auditování programového vybavení. Specifický přístup pak vyžadují zejména aplikace provozované jako webové, tj. s uživatelským rozhraním ve webovém prohlížeči.

Bezpečností programového vybavení se v dostupné literatuře zabývá zejména Boehm [7] a dále pak Trim [3], Ulsch [4], částečně Smejkal [8] a Doucek [9].

4.4.13.1 Ve fázi návrhu, vývoje a testování

Již během fáze návrhu, vývoje a testování je třeba dodržovat bezpečnostní zásady. Není například vhodné tvořit si vlastní komunikační protokoly a vyvíjet vlastní nástroje pro komunikaci – zdroje a znalosti vývojového týmu bývají často omezené. Do rozhraní, která využívají vlastní komunikační protokoly, se tak může snadno dostat bezpečnostní chyba, jejímž důsledkem může být zpřístupnění dat neoprávněným uživatelům, ztráta dat, nebo odepření služby.

S odepřením služby se pojí nutnost věnovat návrhu programového vybavení dostatek péče a tvořit skutečně robustní architekturu, která bude předvídat rizikové situace a už při návrhu myslet na jejich ošetření. Zajistí tak stabilní fungování aplikace a zabrání odepření služby.

Mezi bezpečnostní zásady, které ochraňují uživatelská data, patří využívání protokolů s vysokou úrovní zabezpečení. Například během sestavování spojení nebo výměny citlivých dat se používá asymetrická kryptografie se silným zabezpečením a vysokou náročností na výpočetní výkon, kterým by musel disponovat i útočník, aby dokázal asymetrické šifry prolomit (lze uvést např. eliptické křivky používané během tzv. Diffie-Hellmanovské výměny klíčů). Používá-li se symetrická kryptografie (například během již sestaveného spojení, kdy byl klíč pro symetrickou kryptografii předán zabezpečením pomocí asymetrické kryptografie), měla by taktéž používat co nejsilnější šifrování (např. AES).

Pro ukládání hesel nebo vyhledávání v množině dat podle určitého klíče se používají hashovací funkce (někdy též hašovací, od slova haš, angl. hash). Účelem těchto funkcí je z libovolně velkého množství vstupních dat vygenerovat otisk, který má vždy stejnou datovou velikost. Z otisku nicméně nelze žádným rychlým, jednoduchým a spolehlivým způsobem získat původní data. Protože je

množství výstupních hodnot omezené, dochází v každé hashovací funkci k existenci tzv. kolizí – stavů, kdy na základě různých vstupů dojde k vytvoření stejného výstupu. Pro situaci, kdy dochází k pokusu o narušení systému, ve kterém se hesla ukládají pomocí hashe s častými kolizemi, pak útočník vůbec nepotřebuje najít prolamované heslo. Stačí mu najít jakékoli jiné heslo, které má stejný hash, a systém mu přístup umožní. Proto je třeba volit takové hashovací funkce, pro jejichž fungování není znám způsob generování kolizí, a které omezují hledání kolizí hrubou silou (opakovaným zkoušením generování hashovacích výstupů pro různé vstupní hodnoty lze kolize hledat; náročnější způsob hledání kolizí vychází ze znalosti vnitřního fungování hashovací funkce a netriviální matematiky).

Používané symetrické i asymetrické šifrovací algoritmy, stejně tak jako algoritmy pro vytváření haší, je třeba sledovat a vyhodnocovat. Objeví-li se v některém z používaných algoritmů bezpečnostní zranitelnost, stávají se takové protokoly hrozbou a je třeba je co nejrychleji opustit.

K ukládání hesel se ještě vrátím, tentokrát z pohledu možného získání databázových dat o uživatelích a jejich heslech – stejně jako není vhodné používání hashovacích funkcí s vysokým počtem kolizí, není vhodné ukládat hesla na základě pouhého získání hashe ze vstupních dat. Existují (nebo se dají vytvořit) totiž tzv. rainbow tables, což jsou tabulky, které k různým kombinacím slovníkových hesel, číslic a speciálních znaků obsahují předgenerované hashe. Zpětné dohledání uživatelova hesla na základě znalosti (uniklého) hashe je pak otázkou prohledání takových tabulek. Takto zpětně identifikované heslo pak může útočník zneužít pro přístup k dalším kybernetickým systémům. Při tvorbě hashů je nutné do vstupu hashovací funkce kromě samotného uživatelského hesla nutné přidat ještě náhodně vygenerovanou hodnotu, tzv. salt. Tím se vstup „osolí“ a při případném úniku dat z databáze pak útočník nebude moci rainbow tables využít.

Podobně nebezpečné je ukládání uživatelských hesel v databázích v nehashované podobě (tj. ve formě čitelné pro běžného uživatele), kde má útočník zjednodušenou práci o nutnost vyhledávání v tabulkách hashů.

Pracuje-li aplikace s daty z jiných systémů, měla by tato data přenášet šifrovaně (na úrovni relační až aplikační vrstvy OSI modelu). Neměla by nicméně implicitně důvěřovat, že komunikuje se správnou protistranou. Měla

by si vždy ověřovat časovou platnost certifikátů, informaci, kdo certifikáty vydal, a to, že certifikáty byly vydány skutečně tomu, s kým chce komunikovat.

Organizace by měla využívat možností kontroly zdrojových kódů, jsou-li k dispozici, a provádět jejich audit (tzv. code review, revizi kódu na případné bezpečnostní nedostatky). Tento audit by měla provádět vždy, pokud se bude jednat o aplikaci, kterou pro organizaci vyvíjí externí dodavatel na zakázku. V případech, kdy není zdrojový kód k dispozici (např. licencovaný software s uzavřenou licencí), je nutné věnovat zvýšenou péči black-box testování (testování bez znalosti toho, jak aplikace funguje uvnitř).

Aplikaci je vždy nutné otestovat, a to na funkčnost základní (kontrolované vstupy, očekávané výstupy), tak i na výkon aplikace pod zátěží. V případě testování je třeba pamatovat na případy, kdy aplikace musí správně zpracovat data platná, ale i data, která jsou neplatná. Je tedy třeba vytvořit takové testovací schéma, kdy dochází k testování aplikace pomocí neplatných dat a kontrolám, zda jsou na jejím výstupu (očekávané) chybové stavy.

Pro testování aplikace často bývá nutností získat vzorek aplikačních dat, na kterém je testování možné provést. V tomto okamžiku může dojít k bezpečnostnímu incidentu, jsou-li vývojovému týmu poskytnuta citlivá produkční data bez jejich zastření či anonymizace.

Výslovně nedoporučuji návrh a vývoj vlastních komunikačních protokolů a knihoven. Navrhuji využití již hotových a osvědčených řešení a komponent. Doporučuji věnovat péči tvorbě architektury aplikace a ošetření potenciálně rizikových situací. Dále doporučuji využívat komunikační protokoly s vysokou úrovní zabezpečení přenášených dat a šifrování dat.

Při spojování šifrovaného kanálu je nutné kontrolovat časovou platnost certifikátu, vydavatele certifikátu, a zda je certifikát určen pro tu protistranu, se kterou je komunikace navazována. Pro výměnu klíčů doporučuji používat asymetrickou kryptografii se silným šifrováním (např. s využitím eliptických křivek), v případě přenosu dat již sestaveným bezpečným kanálem navrhuji používat symetrickou šifru s vysokým zabezpečením (např. AES).

Hesla nesmí být uložena tak, aby byla čitelná pro správce i útočníky (a to ani v šifrované podobě). Pro uložení hesel doporučuji

využít silné hashovací funkce, jejíž vstupy doporučuji „osolit“. Staré, nebezpečné šifry a hashovací funkce doporučuji rychle opouštět. Zdrojové kódy aplikací navrhuji auditovat (provádět revizi kódu), aplikaci testovat, a to i pod zátěží. Aplikační data z produkčních systémů by nikdy neměla být nikdy předávána k testování v původní podobě – doporučuji je anonymizovat.

4.4.13.2 Ve fázi podpory, provozu a údržby

V produkčním prostředí je vhodné mít aplikace pod kontrolou. O instalaci aplikací (a jejich aktualizací) proto by proto organizace měla rozhodovat centrálně a centrálně tento proces i řídit. Databáze zranitelností (CVE) by měly být pravidelně kontrolovány a organizace by měla rychle reagovat v případech, kdy se objeví bezpečnostní zranitelnost (v aplikaci či v podpůrných knihovnách). Během instalace aplikací doporučuji kontrolovat přítomnost digitálních podpisů od důvěryhodných vydavatelů a časovou platnost těchto podpisů.

Doporučuji pravidelně provádět audit nainstalovaného vybavení, revizi nainstalovaného programového vybavení a minimalizovat množství programů, které uživatel používá. Čím méně programů, tím menší je pravděpodobnost, že se v některém z nich vyskytne bezpečnostní chyba, která způsobí bezpečnostní incident.

Aplikace k nainstalování doporučuji volit a instalovat centrálně. Objeví-li se bezpečnostní zranitelnost, doporučuji jednat rychle. Během instalace aplikace doporučuji kontrolovat přítomnost platných digitálních podpisů. Doporučuji provádět audit programového vybavení.

4.4.13.3 Po skončení fáze podpory

Zejména komerční aplikace jsou vydavateli podporovány jen po určitou, předem danou dobu. Skončí-li podpora aplikace ze strany výrobce (nebo dodavatele zdrojového kódu), nejsou k dispozici bezpečnostní aktualizace a je nutné aplikaci přestat používat. Neaktualizovaná aplikace se stává bezpečnostní hrozbou (v aplikaci může například existovat chyba, kvůli které dojde k napadení systému).

Doporučuji hlídat, kdy aplikacím končí doba podpory a vydávání bezpečnostních aktualizací. Navrhuji aplikace

nahrazovat jinými včas před koncem podpory. Nedoporučuji ponechávat náhradu aplikace až na dobu po skončení období podpory.

4.4.13.4 Elektronické obchody a webové aplikace

Pro elektronické obchody a webové aplikace samozřejmě platí obecná pravidla bezpečnosti aplikací. Protože ale webové prostředí je specifické (prochází bouřlivým rozvojem, ale zároveň si s sebou nese nemalé dědictví z minulosti), je třeba v některých případech zabezpečení ještě zvýšit.

Například z pohledu bezpečnosti přenosu je vždy vhodné použít zabezpečené spojení s certifikáty. Díky novým službám jako je Let's Encrypt[26] je zabezpečení pomocí certifikátů dostupné již každému. Správně zabezpečená aplikace pak má v adresní liště webového prohlížeče zelený zámeček, zatímco aplikace s chybně nastaveným zabezpečením má zámeček červený a prohlížeč uživatele před návštěvou takové aplikace varuje.

Obrázek 7 - Zabezpečená aplikace se zeleným zámečkem

Nezabezpečené aplikace zatím červený zámeček v adresní liště nemají, nicméně společnost Google (autor webového prohlížeče s více než dvoutřetinovým podílem na trhu prohlížečů – má již téměř sedmdesátiprocentní podíl na trhu[27]) se vyjádřila, že již na konci roku 2016 začne červeným zámečkem označovat i takové webové aplikace, které se o zabezpečení přenosu vůbec nepokoušejí[28].

Společnosti, které chtějí ještě více posílit důvěru ve své webové aplikace, mohou zvolit tzv. Extended Validation certifikát. Při vydávání tohoto certifikátu dochází k detailnějšímu prověřování žadatele. Odměnou pak je název společnosti, pro kterou byl certifikát vydán, zobrazující se v adresním řádku webového prohlížeče.

---

[26] *Let's Encrypt* [online]. 2016 [cit. 2016-05-03]. Dostupné z: https://letsencrypt.org/

[27] Browser Statistics. *W3schools.com* [online]. 2016 [cit. 2016-05-05]. Dostupné z: http://www.w3schools.com/browsers/browsers_stats.asp

[28] Marking HTTP As Non-Secure. *The Chromium Projects* [online]. 2016 [cit. 2016-05-05]. Dostupné z: https://www.chromium.org/Home/chromium-security/marking-http-as-non-secure

Obrázek 8 - Zabezpečení webu pomocí EV certifikátu

Kontrolu správného nastavení certifikátů takto zabezpečené aplikace lze realizovat pomocí testovacího rozhraní SSLTest společnosti SSLLabs[29], kontrolu nastavení aplikace samotné pak pomocí nástroje SecurityHeaders[30].

Webové aplikace a elektronické obchody musejí věnovat obzvlášť důkladnou péči kontrole uživatelských vstupů. Neošetření vstupu může snadno pomoci útočníkovi k vložení nečistého kódu do kódu jinak bezpečné webové aplikace – toto se označuje jako XSS, ***Cross-Site Scripting***[31]).

Pro webové aplikace a elektronické obchody vždy doporučuji zabezpečit aplikace pomocí certifikátů. Pro zvýšení důvěryhodnosti (nikoli bezpečí) je možné zvolit i EV certifikáty. Kontrolu nastavení zabezpečení webového serveru i aplikace samotné doporučuji provádět pravidelně. Vstupy a výstupy aplikace navrhuji ošetřit a tím je ochránit.

4.4.14 Ošetření bezpečnosti hardware

4.4.14.1 Provozování hardware a bezpečnost dat

Doporučuji pravidelně aktualizovat firmware v zařízení. Tím bude snížena hrozba potenciální ztráty dat, která by plynula z chyb ve firmware. V případě reklamací datových úložišť doporučuji pamatovat na datovou bezpečnost a taková úložiště mazat nástroji k tomu určenými (např. DBAN, viz níže).

Doporučuji pravidelně aktualizovat firmware v zařízení a pamatovat na datovou bezpečnost reklamovaných datových úložišť.

[29] SSL Server Test. *Qualys SSL Labs* [online]. 2016 [cit. 2016-05-05]. Dostupné z: https://www.ssllabs.com/ssltest/

[30] Securityheaders.io. *Securityheaders.io* [online]. 2016 [cit. 2016-05-05]. Dostupné z: https://securityheaders.io/

[31] PEJŠA, Jan. Co je Cross-site scripting jak mu předcházet. *Zdroják.cz* [online]. 2009 [cit. 2016-05-06]. ISSN 1803-5620. Dostupné z: https://www.zdrojak.cz/clanky/co-je-xss-jak-mu-predchazet/

4.4.14.2 Decomissioning a pravidelné obměny hardware

Životnost hardware se může počítat na měsíce, roky či dlouhá desetiletí. I hardware ovšem stárne a je třeba o něj pečovat. Výrobce zpravidla poskytuje záruční lhůtu či podporu v délce několika let, během které se stará o obměnu komponent, kterým skončila životnost. Pokud však skončí hardwaru záruční lhůta, může začít docházet k selháním, která nebudou řešitelná. To může způsobit odepření služby, je-li služba provozována v omezeném režimu. Proto je třeba řádně plánovat obměnu hardwaru před ukončením záruční lhůty nebo podpory a data preventivně vždy přesouvat ze systémů, kterým životnost končí, na systémy nové.

Staré systémy je třeba posléze vyřadit. Při vyřazování je třeba pamatovat na bezpečnost dat – veškerá vyřazovaná datová úložiště je nutné smazat programovými nástroji k tomu vhodnými (např. DBAN[32], který dokáže bezpečně smazat data z datových úložišť a zajistit tak ochranu dat při případném vyřazování hardwarových komponent). Nelze-li data z úložišť vymazat programovým vybavením (například z důvodu selhání elektronických komponent datového úložiště), je nutné takové úložiště bezpečně fyzicky zlikvidovat.

Navrhuji pravidelnou obměnu hardware, nejpozději po konci záruční nebo podpůrčí doby. Doporučuji včasnou migraci služeb a dat ze systémů, kterým záruka nebo podpora končí. Systémy bez podpory doporučuji vyřadit a při vyřazení pamatovat na bezpečnost dat – a datová úložiště bezpečně smazat. Nelze-li data smazat programově, navrhuji využít bezpečné a certifikované likvidace takových úložišť.

4.4.15 Ošetření zařízení Internetu věcí

Internet věcí vyžaduje kromě standardní fyzické bezpečnosti ***důkladnější evidenci***, která zjistí, zda jsou technologie na svém místě a funkční. Vyžaduje i důkladné zabezpečení – dnes snad již nikdo nepoužije pro komunikaci analogové přenosové protokoly, které je možné odposlechnout a snadno zjistit jejich obsah, nebo dokonce zopakovat analogové vysílání a zařízení tak plně

[32] *DBAN: Data Wiping Software* [online]. 2016 [cit. 2016-05-08]. Dostupné z: http://www.dban.org/

ovládnout. Ani bezpečnost v případě digitální komunikace ale nebývá dokonalá. ***Data z věcí proto doporučuji šifrovat.***

Programové vybavení Internetu věcí by, vzhledem k dlouhodobé použitelnosti věcí, mělo mít ***dlouhou, garantovanou podporu výrobcem***, a to nejen provozování samotné platformy Internetu věcí, ale i pravidelných aktualizací programového vybavení. Zároveň by neměla existovat přílišná závislost věcí na jejich dodavateli.

Jako ***odstrašující případ*** podpory nakonec může sloužit produkt Revolv, který odkoupila společnost Nest (součást koncernu společností Google/Alphabet). Tento produkt, který se měl stát domácím centrem automatizace, stál kupce 300 amerických dolarů. Produkt, který byl na trhu pouhých 18 měsíců, byl zlikvidován[33] a jeho vlastníci ponecháni napospas osudu…

4.5 Monitorování řízení rizik

Tato část procesu řízení rizik vychází z principů popsaných v kapitole *3.8.7 Monitorování a prověřování kybernetických rizik* a je individuální pro každou organizaci.

Mezi obecná doporučení lze zařadit sledování katalogů zranitelností v používaných produktech a rychlou, kvalifikovanou reakci na nově vzniklé hrozby.

Sílu automatizace lze využít k automatizovanému zkoumání a vyhodnocování dat ze zavedených opatření – ať už se jedná o auditní záznamy, systémy detekce/prevence průniku, autentizační či autorizační systémy, jejich pravidelné a automatizované vyhodnocování je základem pro rychlou reakci v případě bezpečnostního incidentu.

Plnění nastavených opatření je také vhodné monitorovat. Proto lze doporučit průběžné automatizované testování zavedených opatření, případně hlášení nefunkčních opatření bezpečnostnímu týmu.

[33] FINLEY, Klint. Nest's Hub Shutdown Proves You're Crazy to Buy Into the Internet of Things. *Wired* [online]. 2016 [cit. 2016-05-06]. ISSN 1059-1028. Dostupné z: http://www.wired.com/2016/04/nests-hub-shutdown-proves-youre-crazy-buy-internet-things/

Proces hodnocení rizik doporučuji opakovat s každým nově zaváděným systémem (alespoň pro tento systém). Nelze připustit, aby kybernetickou infrastrukturu ohrozily potenciální zranitelnosti v takovém systému.

Hodnocení rizik navrhuji opakovat i pro existující systémy, zejména v okamžiku významné změny stavu techniky (například v okamžiku dostupnosti o několik řádů výkonnějších zařízení pro dešifrování dat) – četnost takového opakování je nutné stanovit na základě zkušeností organizace.

5.Závěr

Cílem mé diplomové práce bylo seznámit čtenáře s vybranými kybernetickými riziky, informovat jej o vážnosti konkrétních rizik a zároveň navrhnout opatření, kterými lze rizika snížit.

Čtenáře jsem nejprve v teoretické části seznámil s konceptem rizika, přístupy řízení rizika (risk management) a způsoby hodnocení rizika.

V další části jsem pronikl do konceptu kybernetického prostoru a kybernetických systémů. Poté jsem popsal řízení kybernetických rizik a jeho specifika (zejm. ve vztahu k úmyslným a neúmyslným rizikům). Nakonec jsem krátce zmínil zákonnou úpravu kybernetické bezpečnosti v ČR, kterou se je možné inspirovat při zavádění řízení kybernetických rizik v organizacích.

V praktické části jsem pak popisoval některé teoretické koncepty kybernetických systémů a často používané přístupy v oblasti řízení bezpečnosti. Bez vztahu na konkrétní organizaci jsem se pokusil identifikovat často se vyskytující úmyslná a neúmyslná rizika a hrozby. V poslední části práce jsem navrhl opatření pro eliminaci identifikovaných rizik a hrozeb.

Oblast kybernetických rizik je nicméně velmi rozsáhlá a tato práce si nekladla za cíl rozebrat ji do posledních podrobností. Přesto se domnívám, že svůj hlavní cíl, tedy navrhnout opatření pro předcházení některým kybernetickým rizikům, splnila, že zájemce zasvětila do problematiky řízení (nejen kybernetických) rizik, seznámila jej s častými kybernetickými riziky a pomůže tak zlepšit přístup manažerů i technických pracovníků ke kybernetické bezpečnosti a ochránit kybernetický prostor organizací.

Použitá literatura a zdroje

[1] VEBER, Jaromír. *Management: základy, moderní manažerské přístupy, výkonnost a prosperita*. 2., aktualiz. vyd. Praha: Management Press, 2009, 734 s. ISBN 978-80-7261-200-0.

[2] KRULIŠ, Jiří. *Jak vítězit nad riziky: aktivní management rizik - nástroj řízení úspěšných firem*. Praha: Linde, 2011, 568 s. ISBN 978-80-7201-835-2.

[3] TRIM, Peter R a Yang-Im LEE. *Cyber security management: a governance, risk and compliance framework*. Burlington, VT: Gower, 2014, xxii, 240 s. ISBN 978-1-472432094.

[4] ULSCH, N. *Cyber threat!: how to manage the growing risk of cyber attacks*. Hoboken, New Jersey: Wiley, 2014, 227 s. Wiley corporate F & A. ISBN 978-1-118-93596-5.

[5] REFSDAL, Atle, Bjornar SOLHAUG a Ketil STOLEN. *Cyber-Risk Management*. 1. Cham: Springer International Publishing, 2015, 145 s. ISBN 978-3-319-23569-1.

[6] ANDERSON, Ross. *Security engineering: a guide to building dependable distributed systems*. 2nd ed. Indianapolis: Wiley Publishing, c2008. ISBN 978-0-470-06852-6.

[7] BOEHM, Barry. *Software risk management*. Los Alamitos: IEEE Computer Society Press, c1989. ISBN 0-8186-8906-4.

[8] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada, 2010. Expert (Grada). ISBN 978-80-247-3051-6.

[9] DOUCEK, Petr. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. 2., přeprac. vyd. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.

[10] PROCHÁZKOVÁ, Dana. *Analýza a řízení rizik*. V Praze: České vysoké učení technické, 2011. ISBN 978-80-01-04841-2.

[11] SUN-C'. *Umění války: the art of war*. 1. vyd. Překlad Radim Pekárek. Brno: B4U, 2008. ISBN 978-80-903850-6-1.

[12] ROSS, Ronald S. *Guide for Conducting Risk Assessments* [online]. 2012 [cit. 2016-05-01]. Dostupné z: http://www.nist.gov/manuscript-publication-search.cfm?pub_id=912091.

[13] *Cyberspace* [online]. Oxford University Press, 2016 [cit. 2016-03-21]. Dostupné z: http://www.oxforddictionaries.com/us/definition/american_english/cyberspace

[14] *CVE List Main Page*. *Common Vulnerabilities and Exposures* [online]. 2016 [cit. 2016-04-01]. Dostupné z: https://cve.mitre.org/cve/

[15] *OWASP Dependency Check*. *The Open Web Application Security Project* [online]. 2016 [cit. 2016-04-01]. Dostupné z: https://www.owasp.org/index.php/OWASP_Dependency_Check

[16] ČSN ISO/IEC 27005 *Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací*. Praha: Český normalizační institut, 2009.

[17] *OWASP Top Ten Project*. *The Open Web Application Security Project* [online]. 2016 [cit. 2016-04-02]. Dostupné z: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

[18] *FBI Agent Says No Computer is Safe*. *The Open Web Application Security Project* [online]. Greensburg, Pennsylvania: The Pittsburgh Tribune-Review, 2014 [cit. 2016-04-03]. Dostupné z: http://www.govtech.com/security/FBI-Agent-Says-No-Computer-is-Safe.html

[19] *Insurance 2020 & beyond: Reaping the dividends of cyber resilience*. [online]. London, UK, 2015 [cit. 2016-04-05]. Dostupné z: http://pwc.to/cyber

[20] REJIMOL ROBINSON, R. R. a Ciza THOMAS. Evaluation of mitigation methods for distributed denial of service attacks. *2012 7th IEEE Conference on Industrial Electronics and Applications (ICIEA)* [online]. IEEE, 2012, , 713-718 [cit. 2016-05-05]. DOI: 10.1109/ICIEA.2012.6360818. ISBN 978-1-4577-2119-9. Dostupné z: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6360818

[21] WANG, Shujuan a Mangui LIANG. A Network Access Control Approach for QoS Support Based on the AAA Architecture. *2010 International Symposium on Intelligence Information Processing and Trusted Computing* [online]. IEEE, 2010, , 507-511 [cit. 2016-05-06]. DOI: 10.1109/IPTC.2010.116. ISBN 978-1-4244-8148-4. Dostupné z: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5663617

[22] ELDEFRAWY, Mohamed Hamdy, Khaled ALGHATHBAR a Muhammad Khurram KHAN. OTP-Based Two-Factor Authentication Using Mobile Phones. *2011 Eighth International Conference on Information Technology: New Generations* [online]. IEEE, 2011, , 327-331 [cit. 2016-05-08]. DOI: 10.1109/ITNG.2011.64. ISBN 978-1-61284-427-5. Dostupné z: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5945255

[23] DOWNER, Kathleen a Maumita BHATTACHARYA. BYOD Security: A New Business Challenge. *2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity)* [online]. IEEE, 2015, , 1128-1133 [cit. 2016-05-11]. DOI: 10.1109/SmartCity.2015.221. ISBN 978-1-5090-1893-2. Dostupné z: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7463876

Obsah přiloženého CD

```
+- readme.txt ..................... stručný popis obsahu CD
+- src
|  +- thesis.docx .. zdrojový text práce ve formátu MS Word
|  +- poster.docx ............... poster ve formátu MS Word
|  +- data ...................... zdrojové obrázky, nákresy
+- thesis
   +- thesis.pdf ................ text práce ve formátu PDF
   +- poster.pdf ................... poster ve formátu PDF
   +- zadani.pdf ............... zadání práce ve formátu PDF
```

Evidence výpůjček

Prohlášení:

Dávám svolení k půjčování této diplomové práce. Uživatel potvrzuje svým podpisem, že bude tuto práci řádně citovat v seznamu použité literatury.

V Praze, 18. května 2016

.....
Radek Zajíc

Jméno	Katedra / Pracoviště	Datum	Podpis