VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

SPRÁVA UŽIVATELŮ JAKO ZDROJE RIZIK

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR

Bc. Petr Pospíšil

VEDOUCÍ PRÁCE
SUPERVISOR

Ing. Petr Sedlák

BRNO 2017

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Petr Pospíšil**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2016/17

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

Správa uživatelů jako zdroje rizik

Charakteristika problematiky úkolu:

Úvod
Vymezení problému a cíle práce
Teoretická východiska
Analýza současného stavu
Vlastní návrh řešení
Zhodnocení a přínosy práce
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Pro vybranou společnost (organizaci) na základě analýzy vypracujte metodický postup pro řízení uživatelských rizik v rámci zavádění ISMS.

Základní literární prameny:

ČSN ISO/IEC 27001, Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky. Praha: Český normalizační institut, 2014.

ČSN ISO/IEC 27002, Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Soubor postupů. Praha: Český normalizační institut, 2014.

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

ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2016/17

V Brně dne 28.2.2017

L. S.

doc. RNDr. Bedřich Půža, CSc. ředitel	doc. Ing. et Ing. Stanislav Škapa, Ph.D. děkan

Abstrakt

Tato diplomová práce se zaměřuje na problematiku lidského faktoru, především u KII a VIS. Práce se zabývá analýzou nejčastějších hrozeb spojených s uživateli a návrhem možného řešení snížení dopadů. Nedílnou součástí výstupu je dále návrh koncepce školení uživatelů tak, aby bylo nejen v souladu se ZKB, ale aby bylo zároveň efektivní.

Klíčová slova

Zákon o kybernetické bezpečnosti, kritická informační infrastruktura, významné informační systémy, uživatel jako hrozba, zvyšování bezpečnostního povědomí.

Abstract

This diploma thesis focuses on human resources mainly in Critical information infrastructure and Important information systems. Thesis focuses on the most frequent threats for users and design possible model of threat reduction. Integral part of results is designing of effective security awareness education program according to the Law on Cyber Security.

Keywords

The Law on Cyber Security, Critical information infrastructure, Important Information Systems, user as a threat, Security Awareness Education.

Bibliografická citace:

POSPÍŠIL, P. *Správa uživatelů jako zdroje rizik.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2017. 70 s. Vedoucí diplomové práce Ing. Petr Sedlák.

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenůje úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 26. května 2017

.....

podpis studenta

Poděkování

Na tomto místě bych rád poděkoval svému vedoucímu, Ing. Petru Sedlákovi, za jeho odbornou pomoc a návrhy k teoretické části práce. Dále bych chtěl poděkovat své rodině za podporu při celé délce studia.

Obsah

ÚVOD

Jelikož se o informační a kybernetickou bezpečnost již několik let ve svém volném čase aktivně zajímám, jsem o problematice bezpečnostního povědomí dobře obeznámen. I přes veškerá bezpečnostní opatření jsou téměř vždy největším rizikem v oblasti ochrany informací uživatelé ICT. Hned za nimi jsou však majitelé a ředitelé společností. Jakmile nemají povědomí o rizicích, tak lidé ani netuší, co všechno je ohrožuje. Proto jsou systematické vzdělávání a osvěta uživatelů tak důležité. Pokud uživatel nemá ohrožovat nejen sebe, ale ani ostatní, musí si toho být vědom a musí dodržovat základní bezpečnostní pravidla.

Je třeba si uvědomit, že úroveň bezpečnosti organizace jako celku je vždy při nejlepším taková, jaká je úroveň bezpečnosti nejslabšího článku tohoto celku. Toto konečně platí v podstatě o jakékoliv oblasti jakéhokoliv oboru. Dlouhodobá oborová praxe zcela jasně poukazuje na skutečnost, že nejslabším článkem v oblasti bezpečnosti bývá v mnoha případech, ne-li ve většině případů lidský faktor.

Zdroje dokonce uvádí, že bezpečnostní incidenty jsou zaviněny vlastními zaměstnanci ve více než 75 % případů. Zde je však potřeba uvést, že většina těchto incidentů není způsobena úmyslně. Na vině je v takových případech především nedbalost zaměstnanců a jejich neznalost bezpečnosti informací. Čím je tento závažný nedostatek zapříčiněn, a proč navzdory snahám o jeho eliminaci tento nedostatek v oblasti firemní bezpečnosti přetrvává?

Ačkoliv by se mohlo zdát, že za špatnou informovaností zaměstnanců o problematice bezpečnosti stojí především malá snaha vedení o zvyšování bezpečnostního povědomí, případně snaha vedení při provádění odpovídajících školení ušetřit, není tomu tak. Problém tkví především ve formě, jakou jsou tato školení a opatření realizována a v nízké míře jejich efektivity.

Společnosti sice často investují do této oblasti nemalé peníze a zavádí různé bezpečnostní politiky, ale nedbají při tom na jejich reálné vnímaní a přijetí ze strany zaměstnanců, coby uživatelů systémů. Podpisy rozsáhlých dokumentů, jež zaměstnance zavazují jednat v souladu s bezpečnostními politikami, kterým reálně ani nerozumí v kombinaci

s jednorázovými školeními tak univerzální recept na bezpečnou společnost nepřináší. Je tedy třeba odpověď na tento, pro společnosti, do budoucna stále kritičtější problém, hledat jinde. Právě analýzou zmíněné problematiky a následným návrhem řešení problému se zabývá tato práce.

1 CÍLE PRÁCE A VYMEZENÍ PROBLÉMU

Pro vybranou společnost (organizaci) na základě analýzy vypracujte metodický postup pro řízení uživatelských rizik v rámci ISMS.

Bezpečnost informací neznamená pouze fyzické zabezpečení organizace a jejich aktiv, ale je nutné na tuto problematiku nahlížet komplexněji. Značnou část bezpečnostních incidentů mají na svědomí sami uživatelé (zaměstnanci) organizací, kteří tak často konají zcela neúmyslně a nevědomky.

Dílčími cíli jsou z těchto důvodů zpracování organizačních opatření za účelem minimalizace prostoru k chybnému jednání a redukce potenciálně nebezpečného chování, které by mohlo způsobit bezpečnostní incident. Zavedení proaktivních opatření nezajistí dostatečnou bezpečnost, proto je dalším cílem zvyšování povědomí o bezpečnosti informací.

2 TEORETICKÁ VÝCHODISKA PRÁCE

2.1Zkratky

ZKB – zákon o kybernetické bezpečnosti

IS – informační systém

KII – kritická informační infrastruktura

VIS – významné informační systémy

AR – analýza rizik

SAE – security awareness education

BCM – business continuity management

DRP – disaster recovery plan

2.2Zákon o kybernetické bezpečnosti

Dne 1. ledna 2015 vstoupil v účinnost zákon č. 181/2014 Sb., o kybernetické bezpečnosti (ZKB). Tento zákon doplňují vyhlášky č. 316/2014 Sb., (o kybernetické bezpečnosti) a vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích. ZKB upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti.

Zákon 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) v § 4 a § 5 uvádí bezpečnostní opatření organizačního a technického charakteru, která jsou odpovědné osoby povinny v příslušném rozsahu zavést a to pro informační systém KII, komunikační systém KII nebo VIS. V § 8 ukládá povinnost odpovědným osobám hlásit bezpečnostní incidenty ve VIS provozovateli národního CERT

a v KII pak Národnímu bezpčnostnímu úřadu (NBÚ). V § 17 je vysvětlena role národního CERT, který funguje jako kontaktní místo, přijímá hlášení o kybernetických bezpečnostních incidentech, vyhodnocuje je a poskytuje metodickou podporu a pomoc při jejich výskytu. Dále takto nahlášené kybernetické bezpečnostní incidenty předává NBÚ. Vládní CERT je součástí NBÚ a vykonává podobnou činnost jako národní CERT s tím rozdílem, že vládní CERT ji provádí pro kritickou infrastrukturu.

Stavem kybernetického nebezpečí, jak je uvedeno v § 21, se rozumí stav, ve kterém je ve velkém rozsahu ohrožena bezpečnost informací v informačních systémech nebo bezpečnost a integrita služeb nebo sítí elektronických komunikací, a tím by mohlo dojít k porušení nebo došlo k ohrožení zájmu České republiky ve smyslu zákona upravujícího ochranu utajovaných informací.

Vyhláška 316/2014 Sb. o kybernetické bezpečnosti uvádí konkrétní doporučení a bezpečnostní opatření organizačního i technického charakteru.

Organizační opatření se ve vyhlášce nacházejí v § 3 až § 15 a v následujících § 16 až § 27 pak opatření technická. Všechna tato opatření jsou uvedena i v mezinárodně uznávaných normách standardu ISO/IEC 27001 a 27002. Jinými slovy se jedná o účinná a v praxi ověřená doporučení a postupy.

Vyhláška se sice týká pouze organizací, pro které platí zákon o kybernetické bezpečnosti, ale užitečné informace z ní mohou čerpat i malé či střední firmy, které se nad zavedením systému řízení bezpečnosti informací zamýšlejí. Příbývá totiž i bezpečnostních incidentů mířené na tyto firmy, protože je obecně známo, že bezpečnost informací podceňují.

2.2.1 Kritická infrastruktura

Narušení funkce systémů určených jako kritická informační infrastruktura by mělo závažný dopad např. na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu. (1) Prvky kritické infrastruktury určuje vyhláška

č. 315/2014 Sb., kterou se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.

Odvětvová kritéria pro určení prvku kritické infrastruktury jsou dle vyhlášky určeny následujícím způsobem:

- **energetika** – elektřina, plyn, ropa, zásobování teplem
- **vodní hospodářství**
- **potravinářství a zemědělství** – rostlinná, živočišná nebo potravinářská výroba
- **zdravotnictví**
- **doprava** – silniční, železniční, letecká a vnitrozemská vodní doprava
- **komunikační a informační systémy** – technologické prvky pevné a mobilní sítě elektronických komunikací, rozhlasové a televizní vysílání, satelitní komunkace, poštovní služby, technologické prvky informačních systémů a oblast kybernetické bezpečnosti
- **finanční trh a měna** – činnost ČNB, poskytování služeb v bankovnictví
- **nouzové služby** – integrovaný záchranný systém, radiační monitorování, předpovědní, varovná a hlásná služba
- **veřejná správa** – veřejné finance, sociální ochrana a zaměstnanost, ostatní státní správa, zpravodajské služby. (5)

2.2.2 Významné informační systémy

Významný informační systém je komplex informačních systémů podle zákona o kybernetické bezpečnosti, které spravují orgány veřejné moci, které nejsou kritickou informační infrastrukturou a u kterých by mohlo narušení bezpečnosti informací omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci.

Dle vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, se určující kritéria VIS člení na:

- dopadová určující kritéria a

- oblastní určující kritéria.

Vyhláška o VIS jednak stanovuje výše zmíněná oblastní a dopadová určující kritéria pro identifikaci VIS, a jednak vyjmenovává konkrétní informační systémy (např. portál veřejné správy, IS katastru nemovitostí, redakční systém JMK, personální IS VEMA aj.).

Dopadová určující kritéria jsou definována v § 4. Jedním z nich je určení úplné nebo částečné nefunkčnosti IS způsobené narušením bezpečnosti informací, které by mohlo způsobit ohrožení nebo narušení prvku KI, zásah do života nebo práv nejméně 50 000 osob, oběti na životech přesahujících 10 mrtvých nebo výrazné ohrožení nebo narušení veřejného zájmu (za předpokladu, že uvedené hodnoty nepřesáhnou hodnoty pro určení prvku KI).

Nutno podotknout, že se jedná o výhradně IS spravované orgány veřejné moci, tedy pod ni nespadají žádně soukromé osoby.

2.2.3 Bezpečnost informací

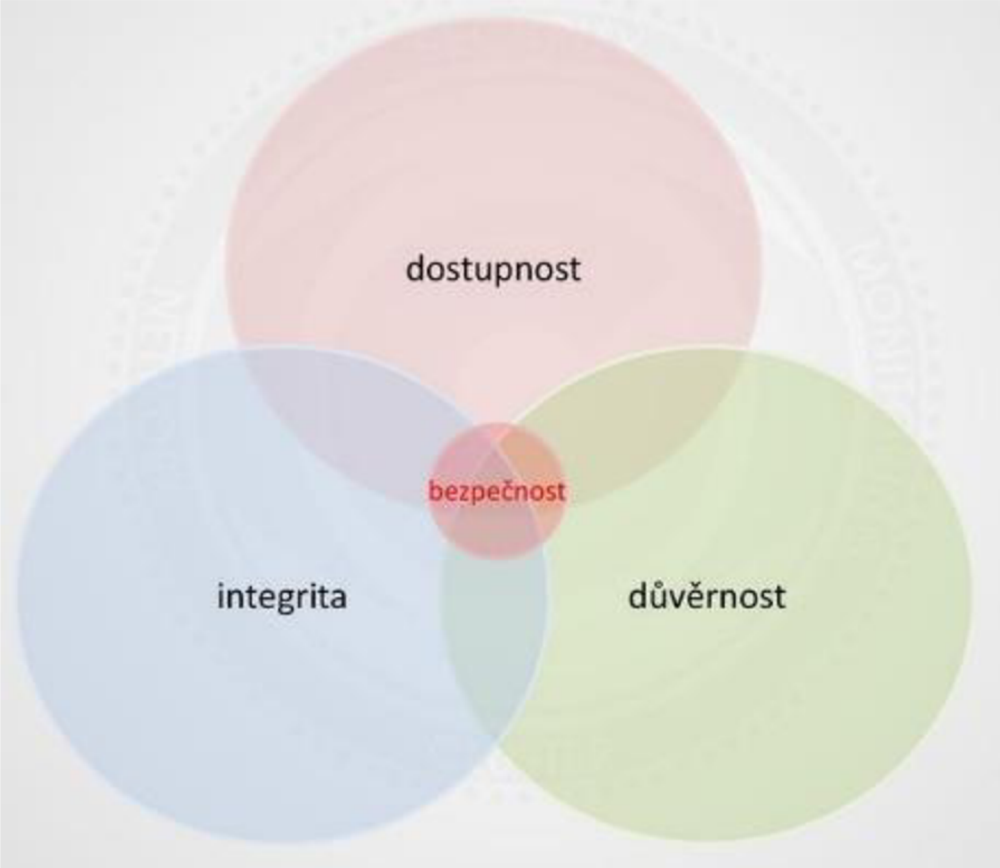
Zachování (ochrana) důvěrnosti, dostupnosti a integrity informací. Kromě těchto vlastností může zahrnovat další obecná bezpečnostní opatření a postupy sloužící k ochraně informací před jejich ztrátou nebo kompromitací (ztráta nepopiratelnosti, autentičnosti, odpovědnosti a spolehlivosti) a k zachování dostupnosti informací a schopnosti s nimi pracovat v rozsahu přidělených oprávnění. (6)

2.2.4 Důvěrnost, dostupnost, integrita

Důvěrnost je zajištěna schopností ujistit se, že je vynucena nezbytná úroveň míry utajení v každém okamžiku, kdy dochází ke zpracování dat a je zajištěna prevence jejich neautorizovaného vyzrazení.

Zapříčinění nedostupnosti dat je populární metodou útočníků, kteří se tak snaží ovlivnit produktivitu, či daný systém zcela vyřadit z provozu. Proto musí být dostupnost zajištěna spolehlivou a včasnou dispozicí dat a zdrojů autorizovaným jednotlivcům.

Integrita je udržena, když je zajištěno, že data jsou přesná, se zaručeným obsahem a jsou provedena opatření proti jejich neautorizované změně.



Obr. 1 - Důvěrnost, dostupnost, integrita

2.2.5 Hrozba

Bezpečnostní hrozbu lze chápat jako potenciální příčinu nežádoucí události, která může mít za následek poškození systému a jeho aktiv, například zničení, nežádoucí zpřístupnění (kompromitaci), modifkaci dat nebo nedostupnost služeb. (6)

Hrozba má potenciální schopnost způsobit nežádoucí incident, který může mít za následek poškození systému nebo organizace a jejich aktiv. Základní rozdělení hrozeb je dle jejich původu, dle úmyslu, podle zdroje a podle dopadu na systém.

Hrozby dle jejich původu:

- přírodní – zemětřesení, požár, povodně, blesk,
- způsobené lidským faktorem – odposlech, chyba uživatele, kybernetický útok. (3)

Dělení hrozeb dle úmyslu:

- náhodné – vymazání souboru, hardwarová vada,
- úmyslné – zcizení, krádež. (3)

Hrozby podle zdroje:

- vnitřní – pomstychtivý zaměstnanec, účetní,
- vnější – cracker. (3)

Hrozby podle dopadu na systém:

- aktivní – přesměrování komunikace, man-in-the-middle útoky,
- pasivní - odposlech. (3)

2.2.6 Bezpečnostní událost a incident

Bezpečnostní událost představuje událost, která může způsobit nebo vést k narušení informačních systémů a technologií a pravidel definovaných k jeho ochraně (bezpečnostní politika). (6) Zjednodušeně se dá také říct, že událost je příčina incidentu.

Bezpečnostní incident je porušení nebo bezprostřední hrozba porušení bezpečnostních politik, bezpečnostních zásad nebo standardních bezpečnostních pravidel provozu informační a komunikační technologie (ICT). (6) Kybernetický bezpečnostní incident nastává v důsledku kybernetické bezpečnostní události. (1)

2.3 Analýza rizik

Jedná se o analýzu, která se provádí za účelem identifikace zranitelných míst v organizaci. Následně zachycuje seznam hrozeb, která na organizaci či firmu působí a stanovuje rizika příslušná každému zranitelnému místu a hrozbě. Účelem takové analýzy je snížení rizik na přijatelnou úroveň, respektive akceptaci zbytkových rizik tam, kde se jejich minimalizace nevyplatí. (3)

- Bezvýznamné riziko (váha 1) – není vyžadováno žádné zvláštní opatření. Nejedná se však o riziko, které by nikdy nemohlo nastat, proto je nutné takové riziko uvést a upozornit na něj (organizační, výchovná opatření). Riziko možno přijmout.
- Akceptovatelné riziko (váha 2) – riziko, které je přijatelné se souhlasem vedení. Je nutné zvážit náklady na případné řešení nebo zlepšení. Pokud se nepovede zavést technická bezpečnostní opatření ke snížení rizika, je nutné zavést alespoň přiměřená organizační opatření, jakými často postučují např. školení. Možné riziko, zvýšit pozornost.
- Mírné riziko (váha 3) – nutnost bezpečnostní opatření realizovat dle zpracovaného plánu podle rozhodnutí vedení organizace. Zavedení opatření na snížení rizika není dobré odkládat a na snížení rizika se musí reagovat ve stanoveném časovám období. Potřeba nápravné činnosti.

- Nežádoucí riziko (váha 4) – je nutné urychleně provést odpovídající bezpečnostní opatření, které riziko sníží na přijatelnou úroveň. Ke snížení rizika musí být přiděleny potřebné prostředky. Vysoké riziko vyžadující bezprostřední bezpečnostní opatření.
- Nepřijatelné riziko (váha 5) – nepřípustné, značné, kritické riziko, permanentní možnost úrazů, nutnost okamžitého zastavení činnosti, odstavení z provozu do doby realizace nezbytných opatření a nového vyhodnocení rizik a přijetí potřebných opatření. Činnost nesmí být zahájena ani v ní nesmí být pokračováno dokud riziko není sníženo. Velmi vysoké riziko, zastavení činnosti. (3)

2.3.1 Aktivum

Aktivum (asset) je všechno, co má pro subjekt hodnotu, která může být zmenšena působením hrozby. Aktiva se dělí na hmotná (nemovitosti, cenné papíry, peníze apod.) a hmotná (informace, předměty průmyslového a autorského práva, morálka pracovníků, kvalita personálu, pověst firmy apod.). Aktivem ale může být sám subjekt, protože hrozba může působit na jeho celou existenci. (21)

Identifikace aktiv je závislá na úrovni podrobnosti, která je zvolena. Příkladem může být o pár řádků výše zmíněná dobrá pověst, která se může vztahovat k organizaci nebo firmě jako takové, k jejím výrobkům, k posyktování služeb, vyřizování reklamací atd.

Základní charakteristikou aktiva je hodnota aktiva, která je založena na objektivním vyjádření obecně vnímané ceny nebo na subjektivním ocenění důležitosti (kritičnosti) aktiva pro daný subjekt, případně kombinací obou těchto přístupů. Hodnota aktiva je relativní v závislosti na úhlu pohledu hodnocení. (21)

2.3.2 Zranitelnost

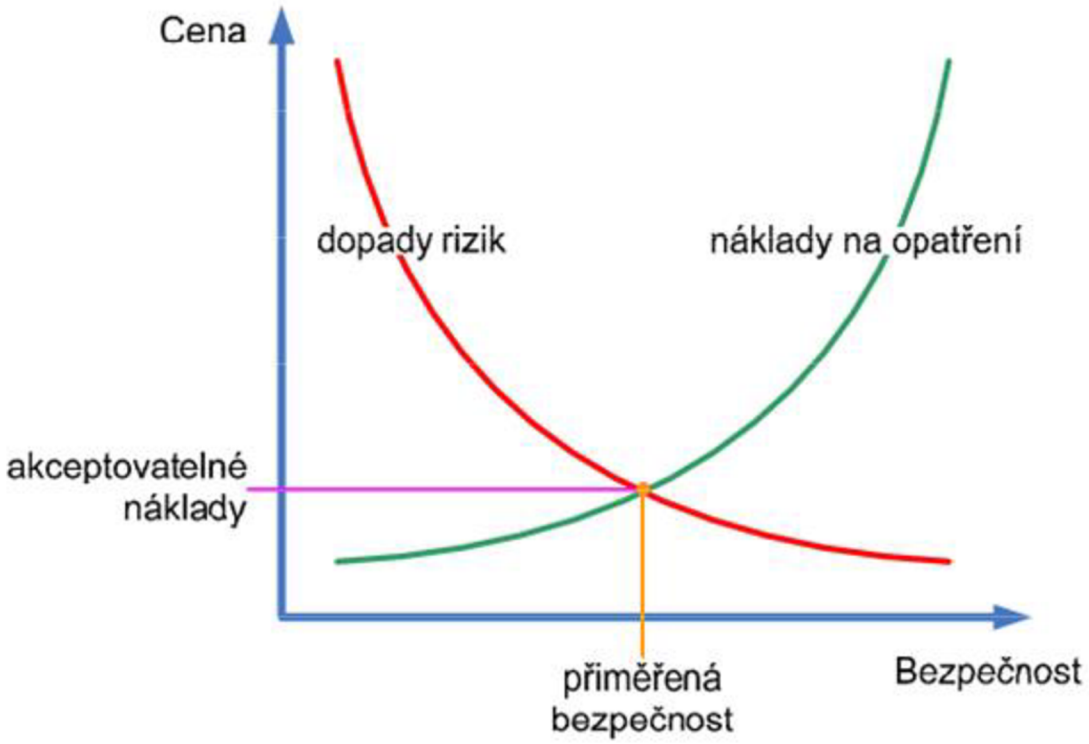
Zranitelnost je nedostatek, slabina nebo stav analyzovaného aktiva (případně subjektu nebo jeho části), který může hrozba využít pro uplatnění svého nežádoucího vlivu. Tato veličina je vlastností aktiva a vyjadřuje, jak citlivé je aktivum na působení dané hrozby. Samotný

výskyt zranitelnosti ještě škodu nepůsobí, protože musí existovat hrozba, která ho využije. Zranitelnost, která nemá odpovídající hrozbu, nemusí vyžadovat přijetí opatření, ale měla by být rozpoznána a monitorována, jestli se nemění. Je nutno poznamenat, že nesprávně přijaté či nefunkční opatření nebo opatření, které se používá nesprávně, by samo o sobě mohlo představovat zranitelnost. Opatření může být účinné nebo neúčinné v závislosti na prostředí, v němž funguje. Naopak hrozba, která nemá odpovídající zranitelnost, nemusí vyústit v riziko. (21)

Zranitelnosti mohou souviset s vlastnostmi aktiva, které lze použít způsobem nebo pro účel, který je jiný, než bylo zamýšleno, když bylo aktivum zakoupeno nebo zhotoveno. Je nutno posuzovat zranitelnosti vyplývající z různých zdrojů, například ty, které jsou pro aktivum podstatné nebo vedlejší. Zranitelnost vznikne všude tam, kde dochází k interacki mezi hrozbou a aktivem. (21)

2.3.3 Přiměřená bezpečnost

Velikost úsilí a investic do bezpečnosti IS musí odpovídat hodnotě aktiv a míře možných rizik. To stanovuje zejména bezpečnostní politika organizace. (3) Grafické znázornění přiměřené bezpečnosti s ohledem na přiměřené náklady je na obrázku č. 1.



Obr. 2 - Přiměřená bezpečnost (zdroj: prezentace předmětu Management informační bezpečnosti)

Výhodou obránce je to, že může implementovat obranu na vícero úrovních, čímž se zvyšuje pravděpodobnost zamezení průniku do systému a vzniku incidentu. V případě obránce stačí přerušit jakoukoliv z probíhajících fází útoku a systém je ochráněn.

Obecně lze tvrdit, že firemní počítačový systém je bezpečný tehdy, když je cena průniku větší než cena aktiv, která může hacker získat.

2.3.4 Metody analýzy rizik

ITIL

Nejedná se o normu ani o metodiku. ITIL (Information Technology Infrastructure Library) obsahuje doporučení a osvědčené postupy vycházející z nejlepších praktických zkušeností „best practise“ mnoha společností po celém světě. Jedná se o mezinárodní standard pro řízení

IT služeb. Knihovnu spravuje Office of Government Commerce (OGC) a je šířena prostřednictvím knih, CD, školení, knzultací a certifikací. Na ITIL je dnes již nahlíženo jako na mezinárodní standard pro oblast řízení IT služeb. (3)

V původní podobě měl ITIL 31 knih, takže je otázkou, zda všechny knihy někdo (kromě autorů) opravdu přečetl a podle uvedených doporučení procesy zaváděl. Od roku 2000 byly původní verze revidovány až do podoby ITIL V2, která čítala pouze 7 knih. V roce 2007 se objevuje ITIL V3, který čítal už jen 5 knih a popisuje až 26 procesů. Jednotlivé knihy kopírují životní cyklus služby, tedy:

- **Service Strategy** (strategické procesy) – kniha řeší problematiku IT Governance a je určena spíše pro osoby na pozici CIO. Popisuje 3 základní procesy – Financial Management (správa financí), Service Portfolio Management (správa portfolia služeb) a Demand Management (správa požadavků).
- **Service Design** (návrh služeb) – účelem této publikace je návrh takové služby, která uspokojí současné i budoucí požadavky businessu. Sestává z těchto částí:
    - Service Catalogue Management (správa katalogu služeb)
    - Service Level Management (správa úrovně služeb
    - Capacity Management (správa kapacit)
    - Availability Management (správa dostupnosti)
    - IT Service Continuity Management (správa kontinuity služeb IT)
    - Information Security Management (správa bezpečnosti informací)
    - Supplier Management (správa dodavatelů)
- **Service Transition** (uvedení služby do provozu) – kniha řeší problematiku dodávky služby požadované businessem až do produkčního prosředí. Jsou popisovány následující procesy:
    - Change Management (správa změn)
    - Service Asset and Configuration Management (správa aktiv a konfigurace)
    - Knowledge Management (správa znalostí)
    - Transition Planning and Support (Plánování a podpora přechodu)
    - Release and Deployment Management (správa releasů a nasazení)

    - Service Validation and Testing (ověření a testování služby)
    - Evaluation (Vyhodnocení)
- **Service Operation** (provoz služeb) – problematika dodávky služby v požadované kvalitě. Mluví se o těchto procesech:
    - Event Management (správa událostí)
    - Incident Management (správa incidentů)
    - Problem Management (správa problémů)
    - Access Management (správa přístupů)
    - Request Fullfilment (provádění požadavků)
    - IT Operation Management (správa provozu IT)
    - Application Management (správa aplikací)
    - Technical Management (technická správa)
- **Continual Service Improvement** (neustálé zlepšování)
    - Service Measurement (měření služeb)
    - Service Reporting (vykazování služeb) (28)

V roce 2011 byly ve verzi ITIL V3 provedeny změny a vznikla tak nová verze označovaná jako **ITIL 2011 EDITION**, ve které došlo ke sjednocení osnovy všech 5 ústředních knih a tím byly zpřehledněny struktury popisu procesů, aktivit, rolí a funkcí. Názvy jednotlivých knih i jejich počet zůstal nezměněn, ale došlo k revizi obsahu a názvu. (28)

COBIT

Metodika COBIT (Control OBjectives for Information and related Technology) je mezinárodně uznávanou metodikou, která se opírá o soubor všeobecně uznávaných praktik řízení informačních a komunikačních technologií tak, aby využití informací a nasazení ICT přispívalo k dlouhodobému rozvoji organizace, prohlubovalo její strategické cíle a snižovalo rizika související s použitím ICT. Je určen spíše do rukou vrcholného managementu k posuzování fungování ICT a auditorů. Na rozdíl od ITIL, který je určen spíše pro CIO. (3)

Kostka COBIT je tvořena třemi osami, které se dělí do dalších skupin:

- informační kritéria – efektivita, účinnost, důvěryhodnost, integrita, dostupnost, soulad, spolehlivost,
- IT zdroje – aplikace, informace, infrastruktura, lidé
- IT procesy – domény, procesy, aktivity (3)

2.3.5 BCM

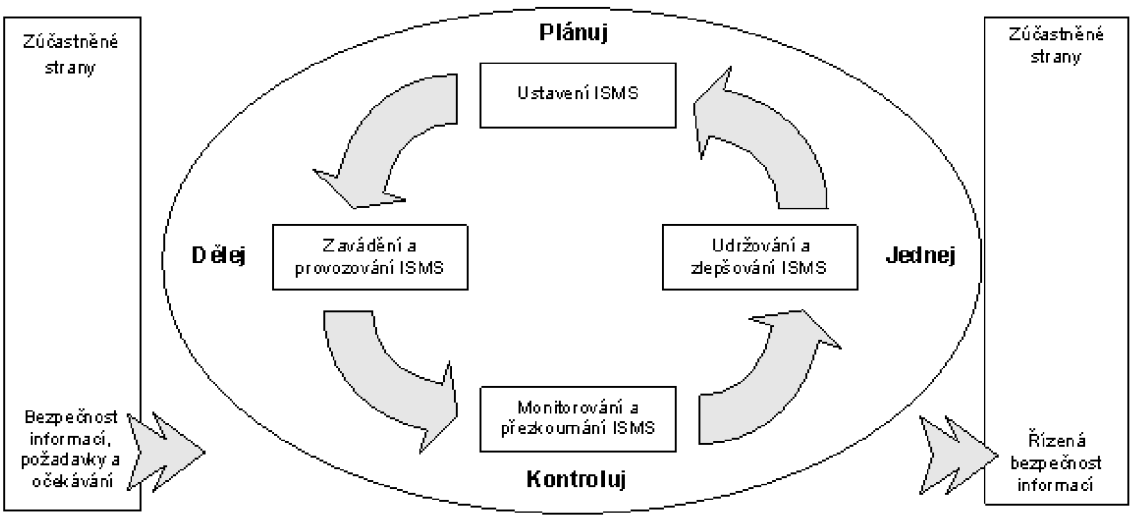
Každá organizace je vystavena určitému množství různých rizik a ohrožení, která mohou mít dopad na dostupnost části činnosti organizace nebo na organizaci jako celek. Cílem řízení kontinuity činností (BCM - Business Continuity Management) organizace, je zabezpečit fungování důležitých procesů uvnitř organizace v případě neočekávané rušivé události. Součástí řízení kontinuity činností je DRP (Disaster Recovery Plan), kterým je zpracován postup v případě výskytu události.

2.3.6 PDCA

Demingův cyklus PDCA (plan-do-check-act) je iterativní metoda, která je v businessu využívána při zavádění a postupném zlepšování kvality služeb, procesů a výrobků. Jedná se o model opakující čtyři základní činnosti, kterými jsou plánuj, dělej, kontroluj a jednej. Autorem modelu je americký statistik William Edwards Deming, který je považován za tvůrce mnoha moderních metod vedení kvality. Model je též známý pod označením Shewhartův cyklus.

- Plan – první fáze zahrnuje stanovení cílů, úkolů a procesů nezbytných k dosažení cílů. Vhodné je určení konkrétního způsobu řešení. Mělo by rovněž dojít k personálnímu obsazení projektu kvalifikovanými pracovníky.
- Do – v tomto kroce dochází k implementaci navrženého plánu a zapracování procesů. Následně dochází ke sběru dat a měření výsledků realizace. Vše je řádně zadokumentováno.

- Check – data z předchozí fáze jsou analyzována a dále zkoumána. Naměřené výsledky měření jsou porovnávány s očekávanými výsledky.
- Act – na základě výsledků z předchozí fáze dochází k rozhodnutí. Pokud naměřené výsledky prokazují zlepšení procesu, dochází k implementování navrhované změny. Pokud však naměřené výsledky nedosahují očekávaného zlepšení, původní postup zůstává zachován a celý proces se znovu opakuje.



Obr. 3 - PDCA (zdroj: ČSN ISO/IEC 27001)

2.4Uživatel

Celková úroveň bezpečnosti je tak velká jako její nejslabší článek. Mnohaleté zkušenosti dokazují, že nejslabším článkem je v drtivé většině případů lidský faktor. Zaměstnance můžeme rovněž chápat jako první linii obrany.

2.4.1 Základní dělení uživatelů

- **IT profesionál** – bezproblémový uživatel s potenciálem IT administrátora
- **Aplikační profesionál** – odborník v daném oboru využívající možnosti poskytované ICT technologiemi
- **Vyškolený uživatel** – uživatel dodržující bezvýhradně pravidla hry (IT bezpečnosti)
- **Nevyškolitelný uživatel** – IT analfabet
- **IT výzkumník** – škodič, který nevyužívá své IT schopnosti správným směrem
- **IT ignorant** – škodič s přesvědčením své nevyškolitelnosti
- **IT rebel** – škodič nejhoršího kalibru, na nějž platí pouze IT karanténa (3)

Běžně se uvádí, že za více než 75 % bezpečnostních incidentů mohou vlastní zaměstnanci. O čem se mluví méně je fakt, že většina těchto incidentů nebyla spáchána vědomě, ale spíše z neznalosti nebo nedbalosti. Po rozhovorech s několika administrátory blíže nespecifikovaných organizací jsem došel k závěru, že problém není ve snaze vedení ušetřit na školení, nýbrž v tom, že školení neplní svůj účel. Organizace často neví, jak by takové školení mělo vypadat. Nejčastější chybou bývá to, že zaměstnancům je sice sděleno, co musí a nesmí dělat, ale chybí konkrétní příklady, na kterých by bylo názorně vysvětleno, proč se po nich takové chování vůbec chce a hlavně k čemu by mohlo dojít, když daná pravidla nebudou dodržovat.

Značná část organizací má tato pravidla sepsaná v podobě několikastránkové bezpečnostní politiky, která je závazná, a kterou všichni zaměstnanci při nástupu do pracovního poměru podepsali. Otázkou spíše je, zda jí všichni zaměstnanci rozumí a zda ji aplikují při každodenní činnosti.

Školení uživatelů se nedá považovat za jednorázovou aktivitu, ale stejně jako např. u ISMS se jedná o proces, který je nutné neustále sledovat, analyzovat a vylepšovat, aby odpovídal aktuálním potřebám a situacím (PDCA).

Odchod zaměstnance může být v zásadě přátelský, nepřátelský nebo konkurenční.

2.4.2 Opatření

Ochranná opatření pro zajištění bezpečnostních požadavků kladených na systém. Mohou mít různý charakter (fyzická ochrana zařízení a informace, personální bezpečnost – kontrola pracovníků, organizační opatření – provozní předpisy apod.) (6)

Jinými slovy se dá opatření rovněž popsat jako prostředek řízení rizik, který zahrnuje politiky, směrnice, metodické pokyny, praktiky nebo organizační struktury, které mohou být povahy administrativní, technické, řídící nebo legislativní. (25)

Bezpečnostním opatřením se dle ZKB rozumí souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v IS a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru před hrozbou v oblasti kybernetické bezpečnosti nebo před kybernetickým bezpečnostním incidentem. (1)

Fyzická bezpečnost

Fyzické zabezpečení objektu se dá rozdělit na technická opatření a lidské zdroje. Technická zabezpečení mohou být následující:

- mechanické zábranné prostředky – zámky, dveře, mříže, bezpečnostní skla aj.,
- zařízení elektrické zabezpečovací signalizace,
- prostředky omezující působení požárů,
- prostředky omezující působení projevů živelních událostí,
- systémy pro kontrolu vstupu – čipové karty atd.,
- kamerové systémy,
- režim pohybu osob – omezení přístupových práv mimo vymezený čas atd.,
- zařízení pro zajištění ochrany před selháním dodávky elektrického napájení a
- zařízení pro zajištění optimálních provozních podmínek. (11)

Obsluha kamerových systémů vyžaduje přítomnost lidských zdrojů. Totéž platí pro recepce a vrátnice, kde je přítomnost vyškoleného zaměstnance nutná. U důležitých objektů se fyzická ostraha objektu zajišťuje nepřetržitě.

Personální bezpečnost

Všichni zaměstnanci musí být o nutnosti bezpečnosti informací dostatečně proškoleni, tj. jsou si vědomi rizik, povinností a odpovědnosti při jejich nedodržení a vzniku potenciálního bezpečnostního incidentu. Blíže jsou návrhy a doporučení pro bezpečnost lidských zdrojů popsány v návrhové části.

2.5 Sociální inženýrství

Nejznámějším průkopníkem sociálního inženýrství je americký, dříve trestaný, dnes uznávaný bezpečnostní konzultant, autor a hacker Kevin Mitnick. Jak ve své knize Umění klamu vysvětluje, nejjednodušším způsobem, jak se dostat k utajovaným informacím, je prostřednictvím sociálního inženýrství. Několikrát mu k neoprávněnému přístupu k informacím stačilo obsluze zavolat a vysvětlit jí, že jej má do systému pustit – o heslo si zkrátka a jednoduše řekl. (7)

Všechny techniky sociálního inženýrství jsou založeny na specifických způsobech lidského rozhodování známých jako kognitivní chyby úsudku. Tyto chyby úsudku, založené na nedokonalosti lidského mozku, jsou využívány mnoha způsoby. Jednoduše řečeno, hacker útočí na nejslabší článek zabezpečení jakéhokoliv systému, kterým je člověk. Proč je člověk tou největší slabinou? Protože není strojem, který lze bezpečně naprogramovat, ale živým jedincem, který jedná na základě svých zkušeností, znalostí a emocí. Útočník tak může pomocí specifické přípravy a psychologické manipulace ovlivnit některá rozhodnutí člověka tak, že provede určitou konkrétní činnost, které by se za jiných okolností nedopustil. Takto oklamaný člověk pak může mylně důvěřovat informaci, která mu byla podána (e-mail, SMS, telefonát) a jednat podle sdělených instrukcí (klikne na odkaz, otevře přílohu e-mailu, prozradí jinou důležitou informaci). To, jakou chybu udělal, se zpravidla dozví mnohem později na základě škod, které jeho jednáním vznikly (infikovaný počítač, prázdný bankovní účet, ztráta kontroly nad firemními systémy, atd.). (27)

Phishing

Pojmem phishing se nejčastěji označuje podvodné či klamavé jednání, jehož cílem je získat informace o uživateli, jako jsou např. uživatelské jméno, heslo, číslo kreditní karty, PIN apod.

V užším slova smyslu phishing představuje jednání, které po uživateli vyžaduje navštívení podvodné stránky (zobrazující např. webovou stránku internetového bankovnictví, e-shopu apod.) a následné vyplnění přihlašovacích údajů. Často jsou tyto informace vyžadovány přímo prostřednictvím formulářů.

V širším slova smyslu se za phishing dá označit jakékoliv podvodné jednání, které má v uživateli vzbudit důvěru, snížit jeho ostražitost či jej jinak donutit akceptovat scénář, který si útočník předem nachystal. V tomto širším slova smyslu již není po uživateli vyžadováno pouze vyplnění údajů, ale je mu doručena zpráva (nebo je uživatel na podvodnou stránku přesměrován) typicky obsahující malware, který si potřebné údaje posbírá sám.

V obou dvou případech dochází k oklamání uživatele, který je cílem phishingového útoku. Rozdíl spočívá v míře interakce, která je od uživatele vyžadována.

Podstatou phishingu je využívání sociálního inženýrství. Phishing je možné provádět i ve světě reálném, avšak virtuální svět umožňuje útočníkovi rozesílat podvodné zprávy obrovskému množství potenciálních obětí a s minimem námahy. Phishing není zaměřen jen na e-maily, ale je možné jej spatřit i v rámci instant messengerů (Skype, ICQ, ...), sociálních sítí, SMS a MMS zpráv, scamu (podvodné nabídky práce nebo zboží), podvodných doplňků do prohlížeče, aplikací do telefonu atd.

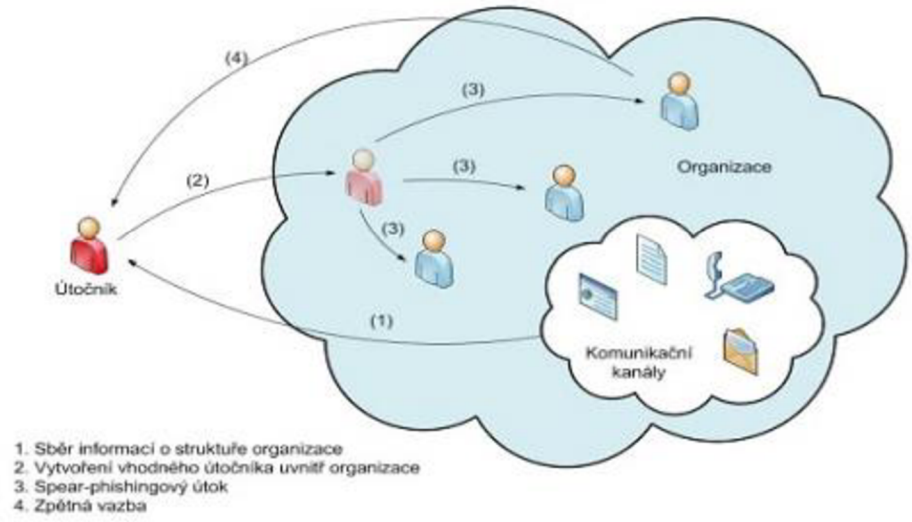
Princip běžného phishingového útoku spočívá nejčastěji v zaslání tzv. phishingového e-mailu poškozenému, který na první pohled nevzbuzuje žádné podezření, že by mělo jít o podvodné sdělení. V těle takového e-mailu bývá odkaz, na nějž je uživatel vyzván kliknout. Po kliknutí na odkaz se uživatel dostane na podvodnou webovou stránku, která se svým vzhledem i funkcemi od originální legitimní webové schránky téměř neliší. Pokud se jedná o napodobeninu webové stránky, pomocí které je možné realizovat platební styk, pak jsou uživatelem zadaná data ihned odesílána útočníkovi. Ten tímto způsobem získává

identifikační údaje uživatelů internetového bankovnictví a další údaje o platebních kartách, které dále může vhodně zneužít.

Spear phishing

Spear phishing je jednou z forem phishingového útoku, ale s tím rozdílem, že se jedná o přesně cílený útok (na rozdíl od phishingu, který je útokem spíše plošným). Cílem útoků obvykle bývá konkrétní skupina, organizace nebo jednotlivec, konkrétně informace a data, která se v této organizaci nacházejí (duševní vlastnictví, obchodní strategie, utajované informace apod.).

U spear phishingu je oproti klasickému phishingu rozdíl v tom, kdo je odesílatelem předmětných zpráv. V počátku útoku je to vlastní útočník, který využije otevřené zdroje, aby zajistil co nejvíce informací o napadené organizaci a její struktuře. Následně vytvoří velmi kvalitní e-mail či jinou zprávu a začne komunikovat s osobou uvnitř organizace jako s kolegou. Tuto osobu pak útočník využije jako prostředek pro šíření dalších zpráv, které mohou být infikovány malwarem, v rámci organizace. Jelikož se jedná o osobu obětem známou, nemají problém s ní komunikovat a méně, pokud vůbec, prověřovat její zprávy.



Obr. 4 - Struktura spear-phishingového útoku

Vishing

Pojem vishing označuje telefonický phishing, při kterém útočník využívá technik sociálního inženýrství a snaží se od uživatele vylákat citlivé informace (přihlašovací údaje, čísla účtů apod.). Útočník se záměrně snaží zfalšovat svoji identitu. Útočníci se často představují jako zástupci skutečných bank či jiných významných institucí, aby u uživatele vzbudili co největší důvěru a nevzbudili sebemenší podezření.

IDN phishing

Čínský bezpečnostní expert Xudong Zheng zveřejnil informaci, jak může být zneužito způsobu, jakým Google Chrome a Mozila Firefox zacházejí s názvy domén, které jsou zakódovány pomocí algoritmu Bootstring, známého spíše pod jménem Punycode k homografním útokům. V zásadě jde o to, že pomocí výše uvedeného algoritmu může být libovolných řetězec, např. i název domény převeden z Unicode na ASCII a naopak. Výstupem tohoto algoritmu je pak řetězec složený jen ze základních písmen, číslic a pomlček. (25)

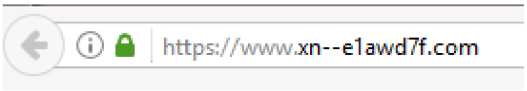
Například čínský název domény „短.co“ lze pomocí Punycode zapsat jako „xn--s7y.co“, což je pro našince jistě srozumitelnější. Punycode však nefunguje jen pro enkódování čínštiny, ale i cyrilice, a zde nastává zásadní problém, protože v okamžiku, kdy má tento algoritmus v adresním řádku prohlížeče zobrazit doménu „xn--80ak6aa92e.com“, zobrazí místo ní „apple.com“, a pokud je tato doména navíc opatřena i certifikátem (viz další podkapitola), nikoho nenapadne zkoumat, že uvedený název není v latince, nýbrž v cyrilici a že ony dvě „pé“ jsou vlastně „er“ a „el“, tedy tzv. paločka, kterou je možné zadat jako Alt+1231. (25)

Důležité je v té cyrilici napsat celý název domény, protože v okamžiku, kdy je část názvu domény napsána v jednom jazyce a část zase v jiném, tak zafunguje ochrana a prohlížeč zobrazí punycode. Byť je tato staronová zranitelnost jistě závažná, možnosti jejího zneužití jsou částečně omezené množinou znaků, které lze použít. (25)

Google Chrome od verze 58 problém s IDN doménami odstraňuje, takže pokud je název domény složen výhradně ze znaků cyrilice, které by mohly být zaměněny se znaky latinky, zobrazí název domény jako punycode. Internet Explorer má tuto zranitelnost od verze 11

rovněž opravenou. Mozilla Firefox umožňuje manuální opravu: v adresním řádku zadat *about:config*, vyhledejte výraz *punycode* a u nalezené položky „*network.IDN_show_punycode*“ doporučuji změnit hodnotu z výchozího *false* na *true*.

Obr. 5 - IDN phishing, Mozilla Firefox punycode false (zdroj: vlastní)



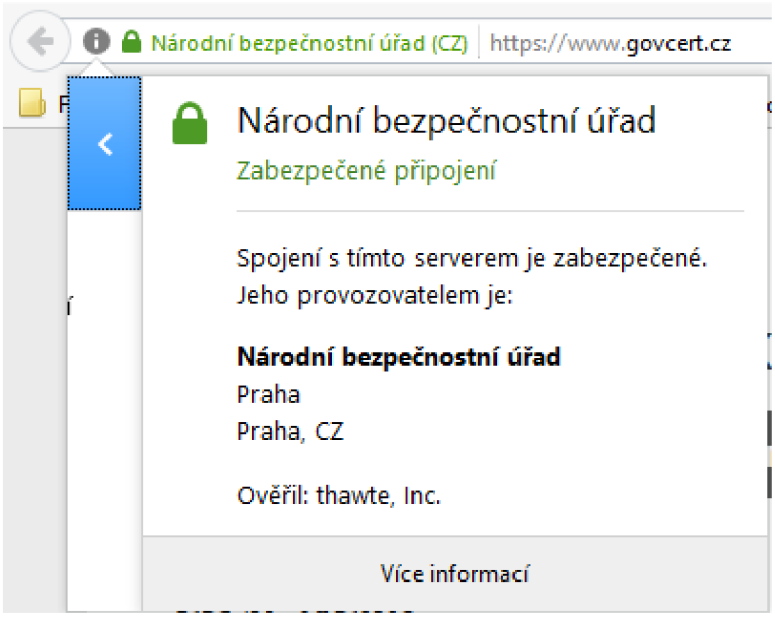
Obr. 6 - IDN phishing, Mozilla Firefox punycode true (zdroj: vlastní)

Možnosti podobného útoku jsou z důvodu nutnosti kombinace znaků omezené, ale v testu neobstáli ani někteří bezpečnostní experti, proto je dobré mít o podobné zranitelnosti alespoň povědomí.

SSL certifikát

SSL (Secure Sockets Layer) je nekomerční otevřený protokol a v současné době jeden z nejčastěji používaných způsobů pro zabezpečení datových přenosů v rámci internetu mezi serverem, na kterém webová prezentace běží a prohlížečem (uživatelem).

SSL protokol zajišťuje šifrování přenášených dat a autentizaci serveru pomocí digitálních certifikátů. To, zda se nacházíme na webové stránce, která je pomocí SSL zabezpečená, poznáme podle adresy stránky, která v adresním řádku obsahuje navíc písmeno „s“, např. https://www.govcert.cz/ a podle zeleného zámku před touto adresou.

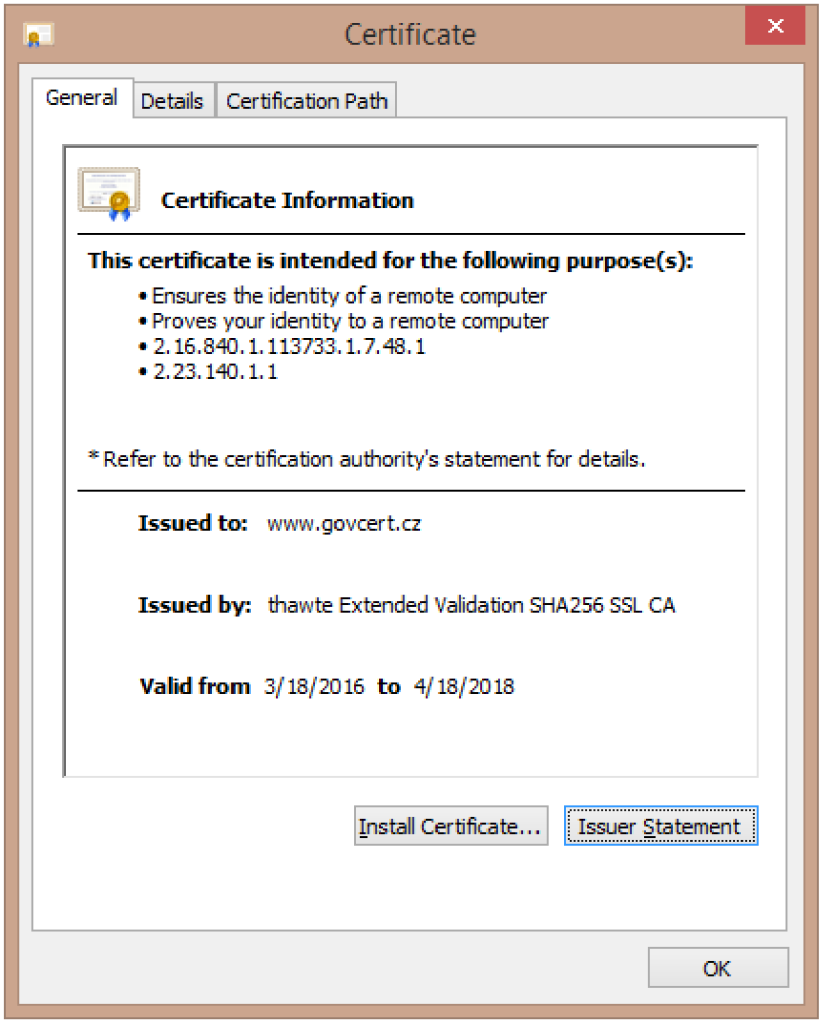


Obr. 7 - zabezpečené spojení pomocí SSL

SSL certifikáty by měl používat každý majitel webové prezentace, který jakýmkoliv způsobem shromažďuje od svých uživatelů důvěrné údaje ve formulářích nebo nabízí například přihlašování na stránky pomocí hesel. U intranetových portálů a hlavně elektronických obchodů by mělo být používání SSL zabezpečení samozřejmostí.

Certifikát obsahuje více údajů, které jsou pro běžného uživatele nepodstatné jako jsou např. šifrovací algoritmus, veřejný klíč, otisk, aj. Uživatele by měly na SSL certifikátu zajímat hlavně údaje:

- komu byl certifikát vydán,
- kým byl certifikát vystaven – certifikát mohl být podepsán útočníkovou certifikační autoritou. Mezi nejznámější certifikační autority patří Thawte, Symantec (dříve VeriSign), GeoTrust, RapidSSL, Trustwave, DigiCert nebo Comodo,
- platnost certifikátu (od kdy do kdy).



Obr. 8 - SSL certifikát

2.6Malware

Malware (složenina z anglických slov malicous software – škodlivý software) je označení pro jakýkoliv škodlivý kód, tedy jakýkoliv software využitý k karušení standardní činnosti počítačového systému, zisku informací (dat), či využitý k získání přístupu k počítačovému systému. Dříve pro škodlivý software existovala řada nejrůznějších termínů, která je v současnosti označována souhrnným slovem malware. Jedná se například o počítačové viry, trojské koně, červy či spyware (špionážní software), adware, ransomware, keylogger, rootkit,

bootkit, backdoor aj. Dnes běžně malware plní více funkcí naráz. Může se tedy například jako červ šířit prostřednictvím e-mailů (v rámci příloh), získávat data o e-mailové schránce, která posléze posílá útočníkovi spolu se zaznamenanými stisky všech kláves (keylogger). (22)

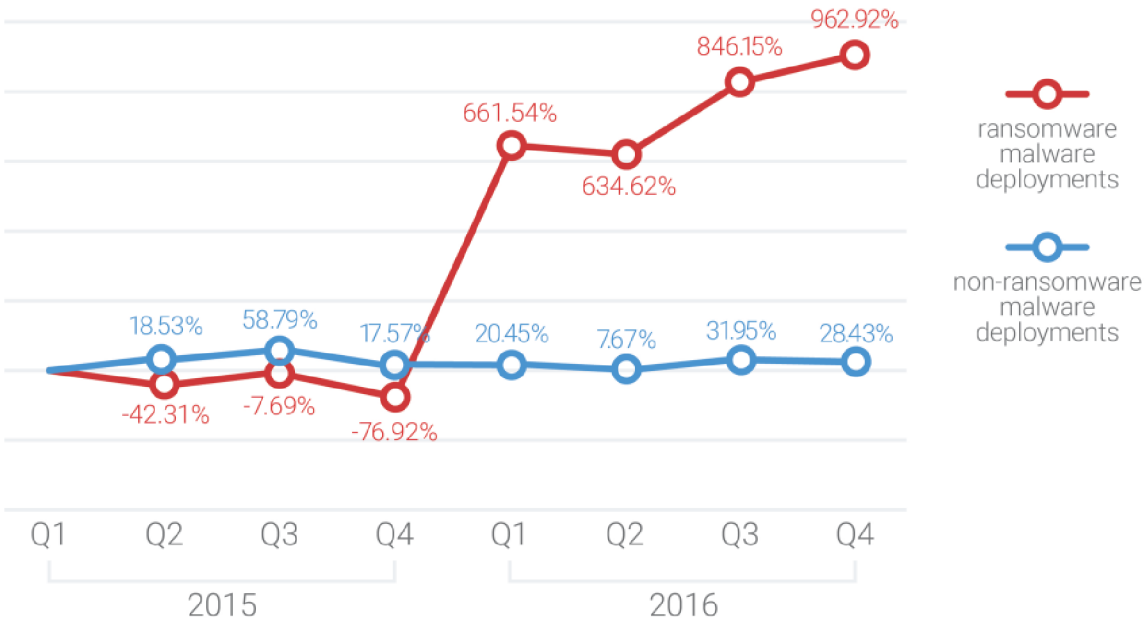
Ransomware

Do skupiny označované jako malware se řadí i tzv. vyděračský malware, kterému se říká ransomware (z anglického ransom – výkupné). Jedná se o druh malwaru, který určitým způsobem napadenému zabraňuje přístupu k řádnému užívání počítače. Dříve autoři ransomwarů „pouze" zablokovali plochu instrukcemi k platbě pro odblokování a znemožnili tak uživateli běžnou činnost. Odstranění malwaru tohoto typu je pro zkušeného uživatele otázka několika minut, což se útočníkům nelíbí a proto jsou způsoby znemožňující práci na PC stále sofistikovanější. V posledních několika letech jsou na vzestupu kryptoviry, což je malware, který na napadeném stroji zašifruje soubory a uživatel se k nim nedostane (mají podobu tzv. rozsypaného čaje a jsou tak nečitelné). Útočníci využívají znalostí z kryptografie a pokud správně celý postup dodrží (generování a distribuce klíčů, použití správného algoritmu apod.), jedinou možností, jak data dešifrovat, je zaplacení výkupného, což se nedoporučuje, ze dvou důvodů – není 100% jisté, že data budou dešifrována, ale hlavně dochází k finanční podpoře zločinců, kteří tak dostávají motivaci s podobnými útoky pokračovat. Bez použití kvantového počítače je při správné implementaci dešifrovací klíč téměř nemožné v rozumně krátkém čase nalézt.

Existují stovky tisíc modifikací tohoto druhu malwaru a nejčastěji útočníci šifrují soubory, o kterých předpokládají, že pro uživatele/firmu mají vysokou hodnotu. Jsou známy varianty, které šifrují pouze klasické kancelářské typy souborů jako jsou .xls, .xlsx, .doc, docx., pdf apod., ale i druhy, které jsou zaměřeny výhradně na hráče počítačových her. (24) Pro jejich znovuzpřístupnění dešifrováním od obětí požadují výkupné (ransom) velice často v kryptoměně – BitCoinech - která je nejen mezi kyberzločinci oblíbená právě z důvodu anonymity.

Ransomware je aktuálně nejoblíbenější technikou kyberzločinců, jak z postižených uživatelů vymámit nezanedbatelné finanční částky. Průměrná cena výpalného vzrostla za jediný rok

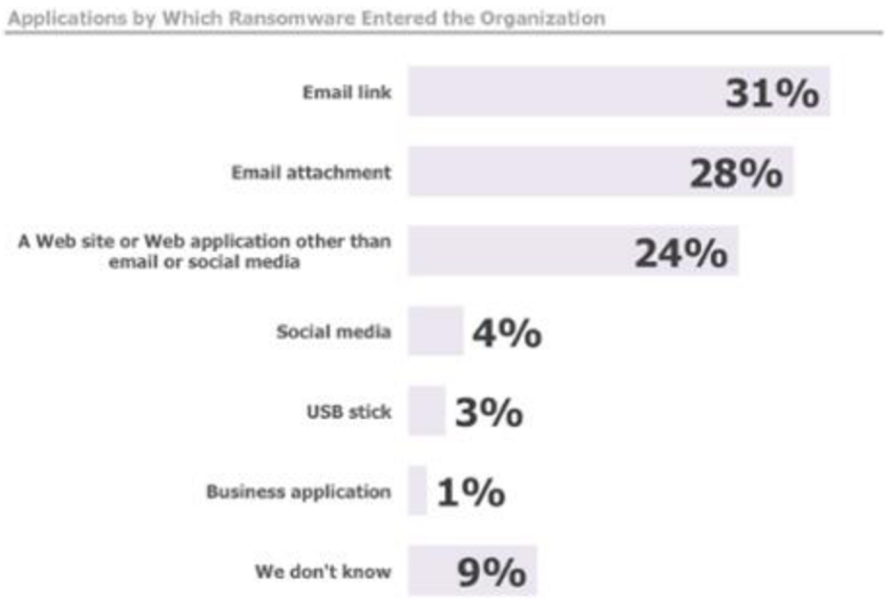
více než dvakrát (z 294 dolarů na konci roku 2015 na aktuálních 679 dolarů). Očividně tedy jde o velmi výnosný business model, který jen tak nezkrachuje. Dá se předpokládat, že tento trend bude i nadále pokračovat. Stejný závěr lze vyvodit i z grafu níže, který informuje o meziročním nárůstu výskytu ransomwaru o stovky procent.



Obr. 9 - Množství útoků ransomwarem (zdroj: PhishMe.com)

V tomto trendu hraje nezanedbatelnou roli vznik služeb **ransomware-as-aservice** poskytovaných na dark netu (část deep webu, která není indexována vyhledávači a jsou zde poskytovány nelegální služby – drogy, cracking, násilí apod.), což znamená, že si ransomware může nechat „vytvořit" i člověk, který v daném oboru nemá dostatečné znalosti. Stačí vyplnit základní údaje jako jsou pokyny co dělat pro dešifrování (ransom notes), BitCoin adresu, kam má napadený uživatel poslat výpalné a odkaz, kde lze zkontrolovat průběh platby a kde bude zveřejněn dešifrovací klíč. Autoru nástroje (ne vygenerovaného droppera) samozřejmě náleží procentuální podíl z každé platby.

Nejčastější způsob, jakým ransomware do firemních sítí proniká, je dle výzkumu provedeného společností Osterman Research, odkaz v e-mailu nebo příloha. Jeden nevhodný klik může rozšířit ransomware do celé firemní sítě. O tato fakta se opírá značná část návrhové části této práce.



Obr. 10 - Způsob infikování firemních sítí ransomwarem (zdroj: Osterman Research, Inc.)

Kybernetická špionáž

Tímto termínem se rozumí získávání strategicky citlivých či strategicky důležitých informací od jednotlivců nebo organizací za použití či cílení prostředků IT. Používá se nejčastěji v kontextu získávání politické, ekonomické nebo vojenské převahy. (6)

3 ANALYTICKÁ ČÁST

3.1 Analýza rizik

V této části práce provádím analýzu rizik organizace a na základě jejich výsledků navrhnu opatření, která budou snižovat dopad na organizaci a/nebo pravděpodobnost výskytu rizika.

Jak již bylo zmíněno v teoretické části, aktiva jsou souhrnné označení pro veškerý hmotný i nehmotný majetek organizace. Pro účely této práce však nebyla identifikována všechna aktiva, nýbrž jen ta, která se týkají uživatelů. Aktiva organizací byla vybrána po několika rozhovorech se zaměstnanci firem nebo organizací, které jsou součástí KII nebo VIS a tedy se pro ně vztahuje současné znění ZKB.

3.1.1 Identifikace aktiv

Aby se dalo provést ohodnocení aktiv, je nutné nejprve aktiva identifikovat. V tabulce uvedené níže jsem nejprve stanovil stupnici ohodnocení aktiv, která poslouží jako základ pro analýzu rizik.

Váha aktiva	Barva	Hodnocení dopadu
1		Bezvýznamné riziko – žádný dopad na organizaci
2		Akceptovatelné riziko – zanedbatelný dopad na organizaci
3		Mírné riziko – potíže či finanční ztráty
4		Nežádoucí riziko – vážné potíže či podstatné fin. ztráty
5		Nepřijatelné riziko – existenční potíže

Tabulka 1 - Hodnocení rizik

3.1.2 Váha aktiv v organizaci

Každému aktivu byly přiřazeny parametry pro důvěrnost, dostupnost a integritu, jenž byly číselně ohodnoceny dle předcházející tabulky. Pro ohodnocení jednotlivých aktiv organizace byl použit aritmetický průměr z těchto tří parametrů, čímž se stanovila konečná váha. Hodnoty jsem zaokrouhloval dle matematických pravidel.

Aktiva	Důvěrnost	Dostupnost	Integrita	Váha
Prac. stanice	3	3	3	3
Server	1	3	3	2
Data	3	3	4	3
Mail server	3	2	2	2
DB zákazníků	4	3	4	4
ICT infrastruktura	5	5	5	5

Tabulka 2 - Váha aktiv organizace

3.1.3 Identifikace hrozeb

Dalším krokem bylo stanovit pravděpodobnost výskytu hrozeb. Stupnici ohodnocení jsem zvolil následovně.

Pravděpodobnost	Slovní vyjádření
1	Žádná
2	Nízká
3	Střední
4	Vysoká
5	Velmi vysoká

Tabulka 3 - Úroveň výskytu hrozby

Hrozba	Pravděpodobnost
Napadení virem	3
Napadení hackerem	2
Neuvědomělá škodlivá činnost	4
Záměrná škodlivá činnost	3
Zneužití oprávnění	3
Výpadek dodávky el. energie	1
Neoprávněný fyzický přístup	4
Únik interních dat	3
Nezájem nadřízených	2
Neúmyslná modifikace	4
Krádež technického vybavení	2
Průmyslová špionáž	4
Neoprávněné vynášení dat	3
Porušení mlčenlivosti	3

Tabulka 4 - Pravděpodobnost výskytu konkrétních hrozeb

3.1.4 Matice zranitelnosti

Matice zranitelnosti představuje vliv možných hrozeb, které na organizaci působí, aktiva organizace a úroveň zranitelnosti. Stupnice zranitelnosti je ve stejném rozmezí jako váha aktiv a pravděpodobnost výskytu hrozeb, tedy 1 až 5.

Zranitelnost	Prac. stanice	Server	Data	Mail server	DB zákazníků	ICT infrastruktura
Napadení virem	4	3	3	2	3	3
Napadení hackerem	2	4	3	4	4	3
Neuvědomělá škodlivá činnost	5	3	4	2	5	3
Záměrná škodlivá činnost	4	3	2	2	3	2
Zneužití oprávnění	2	2	2	3	3	4
Výpadek dodávky el. energie	3	4	3	2	4	5
Neoprávněný fyzický přístup	4	4	4	2	4	4
Únik interních dat	2	3	3	2	3	4
Nezájem nadřízených	2	3	3	2	2	3
Neúmyslná modifikace	4	3	3	2	4	3
Krádež technického vybavení	2	3	3	2	3	5
Průmyslová špionáž	3	4	4	3	4	5
Neoprávněné vynášení dat	2	4	4	2	4	5
Porušení mlčenlivosti	1	4	4	2	4	4

Tabulka 5 - Matice zranitelnosti

3.1.5 Matice rizik

Pro výpočet míry rizika jsem použil maticovou metodu se třemi parametry. Výpočet probíhal podle formule:

$$R = T * A * V$$

kdy **R** značí míru rizika, T hrozbu, A hodnotu aktiva a V zranitelnost. Hranice pro různé stupně rizika jsem si stanovil následovně:

Hranice	Stupeň rizika
<1;35)	Přijatelné
<35;70)	Střední
<70;125>	Vysoké

Tabulka 6 - Stanovení hranice pro stupně rizika

Riziko	Prac. stanice	Server	Data	Mail server	DB zákazníků	ICT infrastruktura
Napadení virem	48	36	27	12	36	45
Napadení hackerem	16	32	18	16	32	30
Neuvědomělá škodlivá činnost	80	48	48	16	80	60
Záměrná škodlivá činnost	48	36	18	12	36	30
Zneužití oprávnění	24	24	18	18	36	60
Výpadek dodávky el. energie	16	16	9	4	16	25
Neoprávněný fyzický přístup	64	64	48	16	64	80
Únik interních dat	24	36	27	12	36	60
Nezájem nadřízených	16	24	18	8	16	30
Neúmyslná modifikace	64	48	36	16	64	60
Krádež technického vybavení	16	24	18	8	24	50
Průmyslová špionáž	48	64	48	24	64	100
Neoprávněné vynášení dat	24	48	36	12	48	60
Porušení mlčenlivosti	12	48	36	12	48	60

Tabulka 7 - Matice rizik

3.1.6 Vyhodnocení

Z výsledné matice rizik můžeme vyčíst, že nejčastější hrozbou s vysokým stupněm rizika je *neuvědomělá škodlivá činnost* uživatele. Dalšími hrozbami, které jsou rovněž ohodnoceny vysokým stupněm rizika, jsou *průmyslová špionáž* ICT infrastruktury a *neoprávněný fyzický přístup* k prvkům ICT infrastruktury.

Na základě výsledků této analýzy se návrhová část bude zaměřovat zejména na zvyšování bezpečnostního povědomí s cílem snížit dopad tří ze čtyř hrozeb s vysokým dopadem. Poslednímu, neoprávněnému fyzickému přístupu, je rovněž věnována pozornost.

4 VLASTNÍ NÁVRHY

Jak již bylo zmíněno v odstavci „Přiměřená bezpečnost“, k úspěšnému přerušení činnosti útočníka stačí, když dojde k přerušení jakékoliv z probíhající fáze. Bezpečnost je tedy velmi důležité řešit na více vrstvách počínaje fyzickým zabezpečením objektu a fyzických aktiv přes ochranu duševního vlastnictví a utajovaných informací (obchodní strategie apod.) až po školení samotných zaměstnanců, kteří v celkovém zabezpečení zastupují velice významnou roli.

Na přelomu loňského roku se šířily informace o ovlivnění průběhu voleb amerického prezidenta ze strany Ruska. Tohoto činu se měly údajně dopustit ruské tajné služby a ruští hackeři. Jednou z technik údajného procesu bylo sociální inženýrství a podvodné e-maily, kdy se útočníci snažili od lidí zodpovědných za hlasování získat přístupové údaje do interních systémů, což se v několika případech povedlo. Nejméně v jednom případě došlo k napadení počítače otevřením zavirované přílohy. Sociální inženýrství je i dle tohoto příkladu velice účinné a proto je nutné zvyšovat bezpečnostní povědomí zaměstnanců.

4.1 Nevzdělaný uživatel

Téměř 75 % incidentů mají na svědomí uživatelé. Drtivá většina těchto incidentů není způsobena úmyslně, nýbrž z nedbalosti či neznalosti.

4.1.1 Politika čistého stolu

Politika čistého stolu znamená úklid pracovního prostoru při vzdálení od tohoto prostoru ať už na odchodem na toaletu, oběd, či domů.

Zaměstnanci by měli být obeznámeni o důležitosti zachování důvěrnosti informací v elektronické i jiné podobě ať už na konci pracovního dne nebo i kdykoliv během dne, kdy od počítače odcházejí. Počítač by měly v době své nepřítomnosti v kanceláři uzamknout. V operačních systémech Microsoft Windows k tomuto účelu byla vytvořena klávesová

zkratka Win+L (klávesa Win se nachází mezi levým Ctrl a levým Alt), což je nejrychlejší řešení. Pracuje-li zaměstnanec s důvěrnými nebo tajnými informacemi mimo počítač, musí je v době své nepřítomnosti na pracovním místě uzamknout nebo podobným způsobem zabránit jejich zneužití. V případě fyzického uzamčení takových dokumentů (např. do skříně) pak nesmí ponechat klíče na stole.

Někdy se pod politikou čistého stolu v širším slova smyslu rozumí méně rušivých elementů (tikající hodiny, fotky ratolestí, blikající zařízení), což prokazatelně zvyšuje soustředěnost a vyšší produktivitu. Podobný pohled je často vyžadován u zaměstnanců, kteří přichází k přímému styku se zákazníky.

4.1.2 Důležitost hesel

Přístup k veškerým informacím prostřednictvím ICT je obvykle přídelován na základě oprávnění po přihlášení do systému. Přihlášení často spočívá v zadání loginu a hesla. Je velice důležité, aby si zaměstnanci byli vědomi důsledků a že budou v případě zneužití hnáni k odpovědnosti. Pro manipulaci s hesly z pohledu uživatele platí několik jednoduchých doporučení:

- heslo zadávejte tak, aby ho nikdo nemohl odpozorovat,
- heslo nikomu nesdělujte,
- heslo si nikam nezapisujte – papírky nalepené na monitoru nebo ukryté pod klávesnicí,
- nepoužívejte stejné heslo do více systémů – tohle je velice podceňované pravidlo. Často se i v médiích zmiňuje, že došlo k úniku databází s přihlašovacími údaji. Pokud se jedná například o službu (diskuzní fórum, e-shop), kterým jste při registraci svěřili svoji e-mailovou adresu a navíc se útočník dostane i k heslům, praktické zkušenosti dokazují, že značná část uživatelů používá stejné heslo i k samotnímu e-mailu a dalším službám. Útočník tak získal mnohem víc než jen přístup k uživatelským účtum na diskuzním fóru,
- v případě vzdálení od počítače uzamkněte obrazovku (viz předchozí podkapitola). (24)

4.1.3 Sociální média a sociální sítě

V teoretické části jsem vysvětlil problematiku phishingu a spear phishingu. Podle nedávného průzkumu EY (Ernst & Young) jsou pro cílené útoky důležitým zdrojem dat sociální média. Sociální média a sociální sítě jsou velmi cenným zdrojem dat pro kyberzločince, kteří tuto platformu využívají k páchání kybernetické kriminality. Zaměstnanci (často i vysoce postavení představitelé) zde totiž zveřejňují více informací než je vhodné. Útočníci se tedy nemusí v tomto případě ohlížet po undergroundových databázích, ale mohou informace shánět naprosto legálním způsobem.

4.2 Uživatel, který vědomě škodí

Bezpečnostní politika je na úrovni organizace základní dokument, který vymezuje strukturu bezpečnostního rizika, odpovědnost za ochranu informací v organizaci, úroveň ochrany informací. (2) Na úrovni systému soubor pravidel a praktik, které specifikují nebo regulují, jak systém (nebo organizace) poskytuje bezpečnostní služby, aby chránil citlivé nebo kritické zdroje systému. (6)

Základní dělení opatření je dáno dle životního cyklu zaměstnance:

- před vznikem pracovního vztahu,
- během pracovního vztahu,
- ukončení a změna pracovního vztahu.

Dohody o ochraně důvěrnosti nebo o povinnosti zachovávat mlčenlivost by měli zajistit požadavek na ochranu důvěrné informace s využitím zákonem vymahatelných prostředků. Při určování požadavků na dohody o ochraně důvěrnosti nebo povinnost zachovávat mlčenlivost by měly být brány v úvahu:

- určení informace, která má být chráněna,

- očekávaná dělka dohody, včetně upřesnění případů, kdy požadavek na ochranu důvěrnosti trvá i po jejím vypršení,
- upřesnění kroků, které následují po vypršení dohody,
- kroky, které budou podniknuty v případě, že dojde k porušení dohody.

ČSN ISO 27001:2014

A.7 Bezpečnost lidských zdrojů

4.2.1 A.7.1 Před vznikem pracovního vztahu

Potenciální uchazeči a zájemci o pracovní pozici by měli být náležitě prověřeni, zejména v případě citlivých pracovních míst. Všichni zaměstnanci využívající zařízení organizace pro zpracování informací, by měli podepsat dohodu odpovídající jejich rolím a povinnostem.

A.7.1.1 Prověřování – všichni uchazeči o zaměstnání musí být prověřeni podle platných zákonů, předpisů a v souladu s etikou. Prověření musí být prováděna na základě požadavků týkajících se činností organizace, dále s ohledem na klasifikaci informací, ke kterým by měli získat přístup, a také z hlediska potenciálních rizik.

S informacemi o všech uchazečích na pracovní pozici, které jsou v rámci prověrek získány, by mělo být nakládáno v souladu s existujícími právními normami. Pokud to zákon vyžaduje, měly by bát uchazeči informováni o tom, že budou prověřováni.

A.7.1.2 Podmínky pracovního vztahu – Pracovní smlouvy uzavřené se zaměstnanci a smluvními stranami musí obsahovat ustanovení o jejich odpovědnostech a odpovědnostech organizace za bezpečnost informací.

4.2.2 A.7.2 Během pracovního vztahu

A.7.2.1 Odpovědnosti vedení organizace – Vedení organizace musí po všech zaměstnancích a smluvních stranách požadovat dodržování bezpečnosti informací v souladu s ustavenými politikami a postupy v organizaci.

A.7.2.2 Povědomí, vzdělávání a školení bezpečnosti informací – Všichni zaměstnanci organizace, a je-li to relevantní i smluvní strany, musí s ohledem na svou pracovní náplň dostávat odpovídající vzdělávání a školení pro zvyšování povědomí bezpečnosti informací a musí být pravidelně informováni o změnách v politikách a postupech bezpečnosti informací.

A.7.2.3 Disciplinární řízení – Musí existovat formální proces disciplinárního řízení k přijetí opatření vůči zaměstnancům, kteří se dopustili narušení bezpečnosti informací.

Formální disciplinární řízení by mělo zajistit korektní a spravedlivé zacházení se zaměstnanci podezřelými z narušení bezpečnosti. Disciplinární řízení by nemělo být zahájeno bez předchozího ověření, zda se opravdu o narušení bezpečnosti jedná. Mělo by být vzatu v potaz, zda se jedná o první nebo opakované narušení, zda byl zaměstnanec dostatečně proškolen a měla by být vzata do úvahy i odpovídající legislativa. V závažných případech by měl být narušitel okamžitě zbaven svých povinností, přístupových oprávnění a výsad. Je-li to nutné, měl by být co nejrychleji a v doprovodu vyveden mimo prostory organizace.

Disciplinární řízení by mělo působit jako odstrašující prostředek odrazující zaměstnance od porušení bezpečnostních politik, směrnic a od narušení bezpečnosti.

4.2.3 A.7.3 Ukončení a změna pracovního vztahu

A.7.3.1 Odpovědnosti při ukončení nebo změně pracovního vztahu – Odpovědnosti a povinnosti v oblasti bezpečnosti informací, které zůstávají platné po ukončení nebo změně pracovního vztahu, musí být definovány, komunikovány se zaměstnanci nebo smluvními stranami a prosazovány.

Celý proces ukončení pracovního vztahu by měl být formalizovaný a měl by zahrnovat navrácení poskytnutého programového vybavení, dokumentů a vybavení, které jsou majetkem organizace. Opomenuty by neměly být také další předměty, jako například mobilní výpočetní zařízení, kreditní karty, přístupové karty, čipy, programová dokumentace a informace uložené na elektronických médiích.

4.3 Administrátoři

Opatření, která mohou být učiněna ze strany správců ICT pro snížení pravděpodobnosti neúmyslné chybné činnosti ze strany nevzdělaných uživatelů nebo i pro ztížení činnosti zvídavých a škodících uživatelů.

4.3.1 Uživatelské účty a oprávnění

přístup do registrů operačního systému, možnost instalovat software, vyprázdnění %temp% při odhlášení ze systému, zajistit oprávnění pro přístup k jednotlivým aplikacím a datům a pro čtení dat, pro zápis dat a změnu oprávnění.

4.3.2 Aktualizace

Neustále omílané doporučení, kdy se radí pravidelně aktualizovat operační systém, antivir, prohlížeče, kancelářské balíky a další zranitelný software. Praktickým příkladem může být vydání záplaty pro podporované operační systémy Microsoftu na zranitelnost v protokolu SMBv1. Tato aktualizace byla Microsoftem uvolněna v rámci běžného Microsoft Security Bulletinu v březnu tohoto roku (každé druhé úterý v měsíci). Shodou okolností se jedná o uniklý exploit EternalBlue z dílny NSA, kterou zveřejnila hackerská skupina Shadow Brokers ale až v polovině dubna. Podle neověřených informací, které aktuálně kolují na internetu, tedy NSA při podezření na únik těchto informací předala detailní informace o způsobu zneužití protokolu SMB Microsoftu, který byl schopen ještě před zveřejněním zdrojového kódu exploitu tuto zranitelnost záplatovat.

Častým argumentem odpůrců aktualizování jsou nepovedené aktualizace, kdy operační systém po nainstalování oficiální záplaty uvízl v nekonečné smičce restartů (17), antivirový software „požírající sám sebe“ (18) nebo například chybnou aktualizace antiviru, která téměř každý web označovala jako nebezpečný a znemožnila tak přístup na internet. (19)

V sítích s heterogenními systémy je hromadné aktualizování značně ztížené, ale je dobré záplaty nepodceňovat, což nedávno ukázalo masové rozšíření síťového ransomwaru WannaCryptor.

Doporučuji tedy pravidelně aktualizovat veškerý zranitelný software, ale nejlépe prvně na jednom až několika testovacích strojích a až následně nabízené aktualizace aplikovat i na zbytek počítačů v organizaci.

4.3.3 Office makra

Office makra jsou obvykle krátké kódy napsané ve Visual Basicu (VBA), které primárně zjednodušují a automatizují opakující se činnost. Samy o sobě jsou velice užitečná, ale nezřídka jsou zneužívány autory malwaru pro infikování počítače.

Makro (nebo souhrn maker), které je schopno zkopírovat sebe sama z jednoho dokumentu do druhého (a to opakovaně), je nazýváno makrovirem. Je zřejmé, že úspěšné šíření viru vyžaduje několik podmínek. Používaná aplikace musí být široce používána a musí docházet k výměně dat včetně maker mezi jednotlivými uživateli a počítači. Všechny tyto podmínky dnes splňují hlavně programy Microsoft Word a Microsoft Excel, a proto jsou zdaleka nejrozšířenější právě makroviry pro tyto dva programy (oba jsou součástí kancelářského balíku MS Office). Programy z MS Office neukládají makra do zvláštního souboru, ale do stejného, ve kterém jsou uložena vlastní data. V takovém případě se tedy nejedná o čistě datové soubory, ale svým způsobem o programy. To zásadně mění přístup k takovým souborům z hlediska bezpečnosti. (20)

Pro ukládání údajů do souboru používá Microsoft svůj vlastní formát, nazývaný Compound Storage File, který je součástí OLE2 (Object Linking and Embedding). Takový soubor obsahuje svůj vlastní souborový systém, včetně tabulek FAT, adresářů, podadresářů, souborů. (20)

Autoři malwaru používají techniky, kterými malwarovým analystům znepříjemňují a ztěžují práci jako jsou anti-sandboxing techniky, časový interval před spuštěním škodlivého kódu,

šifrování maker, obfuskování kódu apod. Existuje sice několik volně dostupných nástrojů (olevba, olefile od autora decalage nebo oledump.py od bezpečnostního analytika a Microsft MVP Didiera Stevense – všechny zmiňované nástroje jsou napsány v pythonu), které umí makra extrahovat, ale tyto nástroje jsou spíše vhodné pro systémové administrátory než pro běžné uživatele.

Doporučeným návrhem je zákaz automatického spouštění maker u souborů, které makra mohou obsahovat. Problematika maker a hrozeb z nich vyplývajících z pohledu uživatelů je součástí prezentace ke školení zaměstnanců KII a VIS, která se nachází v závěrečné části této práce.

4.3.4 Spouštění spustitelných souborů z proměnných prostředí

Dalším návrhem, který jsem ze sledování činnosti malwaru v operačních systémech vypozoroval, a který má hodně malwaru společný, je zakáz spouštění souborů (zejména .exe) z několika nejběžnějších umístění prostřednictvím Group Policy Objects (GPO) jako jsou:

- %temp%
- %localappdata%
- %appdata%
- %userprofile%

Malware má tato umístění v oblibě, protože jsou využívána i legitimními programy a aplikacemi. Proto se na restriktivní opatření podobného charakteru lze dívat různě.

První, velice restriktivní, politikou je zákaz spouštění softwaru ze všech výše zmíněných umístění včetně podsložek a vytvoření výjimek pro legitimní aplikace (whitelisting jednotlivých aplikací - souborů). Tento přístup je vhodný pro některé pracovní stanice, kde uživatel pracuje výhradně s aplikacemi již předinstalovanými firemním administrátorem.

Druhým, méně restriktivním, návrhem je zákaz spouštění souborů ze všech zmíněných proměnných prostředí, ale bez podsložek. Omezení tedy platí pouze pro soubory v umístění např. „%appdata%*.*" . Hodně druhů malwaru si své části stahuje/extrahuje právě do %temp%, kde tato restrikce může z hlediska informační bezpečnosti výrazně pomoci. Nejde o tak rozsáhlé omezení jako v prvním případě, ale například spuštění spustitelného souboru, který je zkomprimovaný v archivu (zip, rar, ...), stále nebude možné – soubor je nutné nejprve extrahovat a až následně spustit.

Oba tyto návrhy je vhodné zkombinovat, upravit, ale hlavně otestovat před finálním nasazením do ostrého provozu, protože mohou způsobit i nezamýšlené problémy.

4.3.5 DRP

Zálohování, zpracování Disaster Recovery Planu (DRP), který je součástí Business Continuity Managementu (BCM) a pravidelná kontrola jejich funkčností. V rámci tohoto plánu je nutné určit další věci jako jsou:

- zabezpečení proti ztrátě dat z důvodu vady pevného disku – RAID,
- použití přepěťové ochrany,
- UPS - zdroj napájení zajišťující souvislou dodávku el. energie pro kritická zařízení v případě krátkodobého výpadku,
- způsob zálohování – zálohy na lokální disk, pásku a následný transport na jinou lokalitu, cloudové řešení,
- aktivní prvky a jejich konfigurace v recovery prostředí,
- pořadí spouštění systémů v disaster recovery.

Při řízení kontinuity činností by měla být stanovena strategie, která se stará o naplnění následujících cílů:

- minimální úrovně poskytovaných služeb, která je přijatelná pro užívání, provoz a správu IS KII, komunikačního systému KII nebo VIS,

- doby obnovení chodu, během které bude po kybernetickém bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb IS KII, komunikačního systému KII nebo VIS, a
- dobu obnovení dat jako termínu, ke kterému budou obnovena data po kybernetickém bezpečnostním incidentu.

Nesmí se zapomínat na pravidelné testování korektní funkčnosti zpracovaného plánu.

4.3.6 Password management

- zrušení požadavků typu: heslo musí obsahovat alespoň jedno velké písmeno, alespoň jednu číslici a speciální znak. Tyto požadavky často vedou k tomu, že heslo není silné, ale zároveň je pro uživatele těžko zapamatovatelné.
- zrušení periodické expirace platnosti hesel. Je-li heslo silné, nutnost takové heslo změnit v konečném důsledku spíše uškodí než pomůže. Za tohoto předpokladu je nutné sledovat nezdařené pokusy o přihlášení a po několikátém chybně zadaném hesle v dalších pokusech na jistou dobu přihlášení zakázat. Heslo musí být změněno při důvodném podezření, že byl účet kompromitován nebo na vlastní žádost vlastníka účtu.
- zrušení nápověd při zapomenutém hesle a kontrolních otázek. Tato možnost je dobrá pro uživatele, ale ještě více si jí cení útočníci. Pokud uživatel navíc stejnou kontrolní otázku používá pro více služeb, což není vyjímka, útočník má silnou motivaci této slabiny zneužít.
- blacklist nejčastěji používaných hesel. Zadá-li uživatel při registraci heslo, které je předpřipravenou databází vyhodnoceno jako slabé (podobné databázím, které používají crackeři a penetrační testeři při slovníkových útocích), je uživatel vyzván k zadání hesla silnějšího.
- podpora všech tisknutelných ASCII znaků v heslech, dále i UNICODE znaků a mezer.

- délka hesla alespoň 8 znaků. Délka hesla je klíčovým parametrem při určování síly hesla. Čím méně znaků heslo obsahuje (například jen množina malých písmen), tím delší heslo musí být. Maximální přípustná délka hesla by měla být **až 64 znaků**.
- hesla by měla být uchována v hashované podobě s příměsí soli. Pro tyto účely je možné použít např. hashovací funkci PBKDF2. Sůl by měla být náhodná hodnota o délce nejméně 32 bitů a generována spolehlivým generátorem náhodných čísel (deterministic random bit generator – DRBG). (9) Při generování soleného hashe by mělo být provedeno alespoň 10.000 iterací. Správné použití tohoto postupu rapidně ztíží prolamování těchto hesel, protože musí prolamovat každý hash zvlášť – ne jako u běžných hashovacích funkcí typu MD5, SHA256.
- dvoufaktorová (2FA) nebo vícefaktorová (MFA) autentizace všude, kde je to důležité, ale vynechat SMS. Cíl vícefaktorové autentizace je v tom, aby byl přístup ke službě umožněn jen a pouze osobě, která je k tomu oprávněna. Jinými slovy je nutné, aby dotyčný dokázal tím, co ví (loginem, heslem, PINem), co má (bezpečnostní token, mobilní telefon, čipová karta) nebo čím je (biometrické údaje, čtečka otisků prstů, identifikace obličeje), že je osobou, za kterou se vydává. Poslední bezpečnostní incidenty nedoporučují SMS zprávu za vhodný způsob dvoufaktorové autentizace. V případě mobilního telefonu je lepší použít přístroj jako one-time password generátor (OTP) za využití zabezpečené aplikace. Nebo použít jednoúčelový generátor těchto hesel. Jedním z důvodů nepoužívání autentizace pomocí SMS může být již několik let známá zranitelnost prokolu Signalling System No. 7 (SS7). Těžko opravitelné zranitelnosti tohoto protokolu umožňují:
    - získání informací o uživateli jako jsou jedinečný identifikátor (IMSI), uživatelova lokace a další.
    - odposlouchávání přenosu s možností úpravy nebo nedoručení příchozích textových zpráv. Tyto man-in-the-middle útoky lze provádět bez toho, aby měl koncový uživatel o právě probíhajícím útoku nejmenší tušení,
    - finanční krádeže, kdy značná část bank na území ČR poskytuje jako ověřovací mechanismus právě SMS. Zjistí-li útočník i logovací údaje pro přístup do internetového bankovnictví např. pomocí phishingových mailů nebo pokud

finanční instituce pro reset hesla používá SMS, nic mu nebrání k převodu libovolné finanční hotovosti [10]

Oprava zneužitelných děr v komunikační technologii SS7, kterou pro komunikaci mezi sebou používají telefonní operátoři po celém světě, není jednoduchá, neboť není nejnovější (byla vyvinuta v 70. letech minulého století), upgrady probíhají jen pozvolna a tudíž oprava i dlouho zveřejněných zranitelností zkrátka trvá.

4.3.7 Automatické spouštění obsahu externích médií

Autorun.inf je textový konfigurační soubor umístěný v kořenovém adresáři disku a externího média, který je používán k automatickému přehrávání či spouštění obsahu externích médií (zahájení instalace po vložení CD/DVD, automatické přehrávání filmu apod.) jako jsou CD, DVD, USB flash disky, externí disky aj. Jedná se o mechanismus operačních systémů Microsoft Windows, kterou operační systémy Microsoftu disponují již od verze Windows 95. Autoři malwaru však této funkce dokáží elegantně zneužít. Příkladem mohou být červi šířící se bez vědomí uživatelů, jakými v minulosti byli např. Conficker, INF/Autorun, či stále se v knihovnách a veřejných počítačích vyskytující Win32/Kryptik. Poslední zmiňovaný sbírá informace o napadeném stroji, na flashce z existujících souborů a složek vytvoří zástupce (původní data stále na flash disku jsou, ale skrytá), zajistí si spouštění při každém startu počítače a komunikuje s C&C (command and control), kterým zasílá nashromážděné informace. Kryptik funguje jako backdoor, kdy má útočník nad takto napadeným strojem velkou kontrolu v podobě dalšího, cíleného infikování. Pro všechny počítače ve firemní síti, na kterých běží operační systém Microsoft Windows, proto doporučuji zakázat funkci automatického spouštění a přehrávání (AutoRun a AutoPlay) z důvodu zamezení šíření červů pomocí externích zařízení.

4.3.8 Mail filter

Důležitou roli hraje důsledné nastavení pravidel pro doručování e-mailů. Jedním z možnosti nastavení je filtrování (nedoručení, přesun do karantény) e-mailů, pokud obsahují přílohu například s jedním z těchto typů souborů: .ade, .adp, .bat, .chm, .cmd, .com, .cpl, .exe, .hta, .ins, .isp, .jar, .js, .jse, .lib, .lnk, .mde, .msc, .msi, .msp, .mst, .nsh .pif, .scr, .sct, .shb, .sys, .vb, .vbe, .vbs, .vxd, .wsc, .wsf, .wsh.

Další možná nastavení:

- ověření odesílatele - kontrola, zda mail nepřišel z jiného mailserveru
- monitorování odchozího spamu
- konfigurace MTA (mail transfer agenta)

4.3.9 Nástroj pro ochranu před škodlivým kódem

Odpovědná osoba pro ochranu IS používá nástroj pro ochranu před škodlivým kódem, který zajistí ověření a stálou kontrolu

- komunikace mezi vnitřní a vnější sítí,
- serverů a sdílených datových úložišť,
- pracovních stanic.

Samozřejmostí je provádění pravidelných aktualizací tohoto nástroje, jeho definic a signatur pro účinnější detekci.

4.3.10 Přípony souborů

Názvy souborů v prostředí MS Windows se skládají ze dvou částí – název souboru a přípona (typ souboru). Například soubor faktury.xlsx byl vytvořen kancelářským balíkem MS Office, což systém pozná právě díky příponě .xlsx. Windows z důvodu zjednodušení defaultně skrývá přípony známých souborů (jen jednu poslední). Toho hlavně dříve zneužívali útočníci. Pokud byl vytvořen soubor malware.pdf.exe, a byl samozřejmě opatřen ikonou

napodobující pdf, Windows poslední příponu skryl a pro nepozorného uživatele tak soubor vypadal jako běžný pdf dokument (malware.pdf), který může bez obav otevřít, čímž si do počítače pustil nezvaného návštěvníka. Z tohoto důvodu je lepší povolit zobrazování známých přípon souborů.

4.3.11 Logování, monitorování a log management

Logování, bezpečná archivace logů a pravidelné přezkoumávání logů zaznamenávající aktivity uživatelů, výjimky, selhání a události bezpečnosti informací, aby v případě zjištění incidentu mohla proběhnout důsledná analýza průniku do systému a činnosti útočníka. Útočník nemusí přicházet pouze zvenku, proto je důležité logovat a monitorovat činnost zaměstnanců, včetně administrátorů a správců takovým způsobem, aby dotyční neměli možnost tyto výstupy jakkoliv modifikovat a zametat tak po sobě nebo jiném neoprávněném přístupu stopy – zajistit bezpečnost a integritu log záznamů. Pro tyto účely je velmi důležitá časová synchronizace všech kontrolních mechanismů a jednotný časový formát, které jsou při analýzách klíčové. Pro KII podle ZoKB platí: (3) Orgán a osoba uvedená v § 3 písm. c) a d) zákona záznamy činností zaznamenané podle odstavce 2 uchovává nejméně po dobu 3 měsíců. V případě KII platí doporučení zasílat logy do log managementu nejpozději každých 5 minut. U VIS je doporučení volnější a interval pravidelného zasílání je v rozmezí 15-60 minut. Logy by měly být dostupné i při poruchách systému (zálohování). Analýzy by měly probíhat v pravidelných intervalech, nejlépe s automatizovaným upozorněním na výskyt abnormalit.

4.3.12 Microsoft EMET

Microsoft vyvinul bezpečnostní freeware nástroj, který slouží jako další vrstva ochrany mezi firewallem a antivirem. Lze jej využít jako ochrana před některými zranitelnostmi nultého dne (0-day vulnerability) či jako Data Execution Prevention (DEP), což je nízkoúrovňová ochrana před spuštěním škodlivého kódu, který využívá výjimek (exception-handling).

Pravidla se nastavují pro každý program zvlášť. Díky pozitivní zpětné vazbě Microsoft prodlužuje oficiální podporu tohoto bezplatného nástroje do konce července 2018.

Enhanced Mitigation Experience Toolkit (EMET) je nástroj, který pomáhá zabránit úspěšnému zneužití chyb zabezpečení v softwaru. Tohoto cíle nástroj EMET dosahuje pomocí technologií pro omezení rizik zabezpečení. Tyto technologie fungují jako zvláštní ochranné prvky a překážky, které musí autoři útoků překonat, aby mohli zneužít chyby zabezpečení v softwaru. Tyto technologie pro omezení rizik zabezpečení nezaručují, že nebude možné zneužít chyby zabezpečení. Jejich úkolem je však zajistit, aby bylo zneužití chyb co nejobtížnější. Nástroj EMET 5.5 rovněž nabízí konfigurovatelnou funkci připnutí certifikátů SSL/TLS nazvanou Certificate Trust (Důvěryhodnost certifikátů). Tato funkce je určena pro detekci útoků prostředníkem (man-in-the-middle attack), které využívají infrastrukturu veřejných klíčů (PKI – public key infrastructure). EMET je určen pro práci s jakýmkoli softwarem, bez ohledu na to, kdy a kým byl napsán. To zahrnuje software vyvinutý společností Microsoft i jinými výrobci. Nicméně je třeba si uvědomit, že některé programy nemusí být s nástrojem EMET kompatibilní. (16)

Po instalaci je nutné nástroj EMET nakonfigurovat tak, aby poskytoval ochranu určitému softwaru. Je třeba zadat název a umístění spustitelného souboru, který chcete chránit. Použijte některou z následujících metod:

- Pomocí funkce Application Configuration (Konfigurace aplikací) grafického rozhraní aplikace
- Pomocí nástroje příkazového řádku

Chcete-li použít funkci Certificate Trust (Důvěryhodnost certifikátů), která byla vydána v nástroji EMET 5.5, je třeba poskytnout seznam webů, které chcete chránit, a pravidla připnutí certifikátů, která se k těmto webům vztahují. K tomuto účelu je třeba využít funkci Certificate Trust Configuration grafického rozhraní aplikace. Další možností je použít nového průvodce

konfigurací. Tento průvodce umožňuje automaticky nakonfigurovat požadované nastavení nástroje EMET. (16)

U aktuální verze nástroje EMET je nejsnazším způsobem nasazení v podniku použití podnikových technologií pro nasazení a konfiguraci. Aktuální verze obsahuje integrovanou podporu zásad skupiny a nástroje System Center Configuration Manager.

K nasazení nástroje EMET můžete rovněž využít nástroje příkazového řádku. Postupujte takto:

1. Nainstalujte soubor MSI do každého z cílových počítačů. Můžete také umístit kopii všech nainstalovaných souborů do sdílené síťové položky.
2. Ve všech cílových počítačích, ve kterých chcete nakonfigurovat nástroj EMET, spusťte nástroj příkazového řádku. (16)

4.3.13 Ochrana mobilních zařízení

Některé zdroje tvrdí, že politika BYOD (Bring Your Own Device) zvyšuje produktivitu, protože zaměstnanec používá systém i zařízení, na které je již zvyklý a nemusí se učit orientovat v novém prostředí. Zavedení politiky, která bezpečnost mobilních zařízení řeší, je nutná, protože pokud taková politika stanovena není, není možné zneužití citlivých dat z takového zařízení trestat.

Po zavedení politiky je nutné, aby byl uživatel seznámen s riziky, která pro něj z používání mobilního zařízení k pracovním účelům plynou jako jsou:

- krádež zařízení a přístup k interním informacím (e-mailům, IS atd.),
- připojování k veřejným a nezabezpečeným Wi-Fi.

V různorodosti tohoto prostředí však vzniká problém, jak mít nad všemi zařízeními kontrolu. Na trhu již existují řešení, která tuto možnost nabízí, alespoň v podobě seznamu zařízení (zda

se jedná o pracovní nebo soukromé), v případě nainstalování aplikace, která vyžaduje nepřiměřená oprávnění a představuje pro firemní data riziko, dojde k omezení přístupu této aplikace ke kontejneru nebo v případě porušení bezpečnostní politiky ke smazání firemního kontejneru. Dalšími možnostmi jsou zálohování a v případě odcizení nebo ztráty přístroje ke smazání obsahu zařízení na dálku.

4.3.14 Šifrování citlivých dat

Při používání e-mailové komunikace v prostředí organizace se doporučuje využít šifrování pomocí PGP nebo S/MIME.

Kanál určený pro distribuce logů do log managementu by měl být šifrovaný (minimálně pro KII a VIS). Samotné zálohy logů by měly být rovněž šifrovány a zabezpečeny proti neoprávněné modifikaci prostřednictvím hashovacích algoritmů a uchráněny tak před neoprávněným přístupem.

4.3.15 Sandboxing a virtualizované prostředí

Pokud je mail server nastaven tak, že v případě spustitelné přílohy přesměruje e-mail do karantény, je velice vhodné mít zařízené izolované, virtualizované prostředí pro účely automatizované dynamické analýzy. Techniky sandboxu jsou užitečné i v případech výskytů kybernetických bezpečnostních událostí a využitelné tak jako podklady pro nahlášení detailů kybernetického bezpečnostního incidentu.

Doporučení virtualizované servery a disky ve dvou geograficky různých umístěních pro případ požáru nebo jiného incidentu (ať už živelního nebo jiného).

4.3.16 Dvě brány do perimetru

Je vhodné počítat s výpadkem spojení na perimetr. Proto není rozumné spoléhat se na komunikaci s perimetrem pouze prostřednictvím jednoho komunikačního kanálu, ale dvou.

Aby v případě výpadku dostupnosti jednoho kanálu nedošlo k ochromení celého perimetru. Proto je doporučení kromě internetového připojení použít i telefony (uložené a připravené kontakty ne odpovědné pracovníky apod.).

4.4 Vzdělávací program

Společnost Check Point zveřejnila zprávu „H2 2016 Global Threat Intelligence Trends“, podle které se počet ransomwarových útoků v druhé polovině roku 2016 zdvojnásobil. V rámci všech celosvětově detekovaných malwarových incidentů v období od července do prosince 2016 se zvýšil podíl ransomwarových útoků z 5,5 % na 10,5 %. Většina těchto útoků je distribuována prostřednictvím e-mailů – buď prostřednictvím spustitelných příloh nebo odkazů.

Národní institut standardů a technologie (National Institute of Standards and Technology, NIST) ve veřejně dostupné normě s označením SP 800-50 **Building an Information Technology Security Awareness and Training Program** pro tvorbu a životní cyklus programu o vzdělávání, zlepšování úrovně bezpečnostního povědomí a bezpečnosti informací popisuje čtyři základní kroky:

- Návrh vzdělávacího programu (sekce 3)
- Tvorba materiálů vzdělávacího programu (sekce 4)
- Implementace programu (sekce 5)
- Post-implementace (sekce 6)

Návrh vzdělávacího programu – nejčastěji má na svědomí bezpečnostní incident uživatel, který jej způsobí svou neznalostí. Proto je prezentace zaměřena na nevzdělané uživatele a zvýšení úrovně základního bezpečnostního povědomí. Základní kostru prezentace tedy tvoří vysvětlení phishingu a sociálního inženýrství, problematika příloh e-mailů, riziko povolení maker v MS Office, ukázka ransomwaru a důležitost hesel.

Tvorba materiálů – cilem prezentace je v co nejpřijatelnější a nejsrozumitelnější formě vysvětlit základy bezpečnostního povědomí. Důležité je používat správné termíny, ale srozumitelnou a odlehčenou formou tak, aby výkladu rozuměl i postarší zaměstnanec, pro kterého je bezpečnost informací cizí slovo. V prezentaci nemá jít jen o výklad politik a směrnic, ale při radách co dělat a co naopak nedělat, je důležité říct, co by se stalo, když pravidla poruším (ransomware). Navíc tyto zvyky určitě uplatní i v soukromí. Prezentace je složena primárně z praktických ukázek. Tato kombinace by měla zaručit vyšší účinnost školení.

Implementace programu – důležitá je součinnost vedení. Pokud se vedení při školení angažuje, bylo prokázáno, že je účinnost školení daleko vyšší. Proto je nutné vedení vysvětlit důležitost školení a jaké bude mít pro organizaci pozitivní důsledky. Dále je nutné vybrat vhodné prostory pro potřeby školení – zda je k dispozici učebna s počítači, jaká je kapacita učebny apod. Samotnou školení může vést administrátor, manažer bezpečnosti nebo outsourcovaný pracovník.

Post-implementace zahrnuje zpětnou vazbu, ale i průběžné a náhodné testování zaměstnanců. Administrátoři a vedení by měli v nepravidelných intervalech využívat nástroje sociálního inženýrství pro testování uživatelů se snahou dostat se k citlivým informacím. Podporované metody jsou phishingové či jinak podvrhnuté e-maily, předstírání identity někoho jiného skrze telefonní hovor a fyzický přístup k počítači v době, kdy u něj dotyčný nesedí apod.

4.5 Ekonomické zhodnocení

Ekonomické zhodnocení zavedených proaktivních opatření, jakými zavedení ISMS a zejména zvyšování bezpečnostního povědomí jsou, lze těžce přesně vyčíslit. Je to velice podobné jako s činností zkušeného administrátora, který ví, co dělá a v ICT dané organizace

má pořádek. Zaměstnavatelé si často mylně myslí, že dotyčný vlastně pro fungování organizace není potřeba, protože nastává pouze minimum incidentů, které stíhá rychle vyřešit a vše bez problému funguje. Nezřídka následně dochází k výměně administrátora, který sice ICT organizace nemá tolik pod kontrolou, ale v očích vedení nestíhá a míní se přetrhnout. Zkušený administrátor totiž aktiva firmy nebo organizace úspěšně chránil před útoky, kterým společnost čelila a proto neznalý a neuvědomělý člověk nabývá dojmu, že dotyčného opravdu nepotřeboval. Úplně totožná je situace při vyčíslování důsledků školení. Pokud jsou zaměstnanci správně proškoleni a úspěšně odolávají méně či více sofistikovaným kybernetickým útokům vedeným proti organizaci, je velice těžké takovou částku vůbec odhadnout.

Jelikož se tato práce nezabývá návrhem ani implementací ISMS, ale slouží jako podpora pro zvyšování bezpečnostního povědomí a zavádění konkrétních opatření pro prvky KII a VIS, pro které je již od 1.1.2015 ZKB v platnosti, předpokládám, že všechna technická zařízení, která v práci zmiňuji, již v organizaci jsou. Zavedení všech organizačních opatření v návrhové části jsou tedy bez dalších nákladů. Jediná činnost, na kterou bude nutné vyhradit prostředky v řádu tisíců Kč, je přítomnost lektora, který bude zaměstnance organizace školit za účelem zvyšování bezpečnostního povědomí.

ZÁVĚR

Problematika bezpečnosti informací mne zajímá již delší dobu s ohledem na malware, který pro mě představuje nekonečnou studnici informací. Bylo tedy velmi zajímavé řešit problematiku bezpečnosti ICT z pohledu uživatelské bezpečnosti a rozšířit si tak obzor.

Žádné bezpečnostní opatření není 100% a ani žádná kombinace těchto opatření nezajistí 100% ochranu před nežádoucím vstupem. Cílem této práce je útočníkům a jiným potenciálním škoditelům co nejvíce znesnadnit jejich činnost a v případě úspěšného průniku do systému takový incident detekovat, analyzovat, učinit vůči němu přiměřené opatření a nahlásit potřebné detaily příslušné autoritě. Dle veřejných průzkumů je většina bezpečnostních incidentů způsobena nedbalostí a neznalostí uživatelů, proto je budování bezpečnostní povědomí nedílnou součástí a velice důležitým aspektem celkové informační bezpečnosti.

Pro potřeby práce jsem pročítal normy řady 27k, ZKB a s ním související vyhlášky a desítky článků zabývajících se informační bezpečností. Na základě takto nabytých a křížově ověřovaných informací jsem sestavil návrhy, které mohou administrátoři ve svých sítích aplikovat a snížit tak možnosti neznalému uživateli způsobit bezpečnostní incident. Po aplikování těchto doporučení jsem přistoupil k návrhu školení určeného uživatelům za účelem zvýšení bezpečnostního povědomí.

ZDROJE

[1] ČESKO. Zákon č. 181/2014 sb., zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Dostupný také z: https://www.nbu.cz/download/pravni-predpisy/container-nodeid-1347/zkb-181-2014-sb.pdf.

[2] NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*. Maryland. Dostupný také z: *http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf*

[3] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

[4] ČESKO. Vyhláška č. 315/2014 Sb. - Nařízení vlády, kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury

[5] MLÝNEK, Jaroslav. *Zabezpečení obchodních informací*. Brno: Computer Press, 2007. ISBN 978-80-251-1511-4.

[6] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.

[7] MITNICK, Kevin D. a William L. SIMON. *Umění klamu*. Gliwice: Helion, 2003. ISBN 83-7361-210-6.

[8] Kybernetický zákon. *Kybernetický zákon* [online]. Copyright © 2014 AutoCont CZ a.s. Všechna práva vyhrazena [cit. 23.05.2017]. Dostupné z: http://www.kybernetickyzakon.cz/#pojmy

[9] NIST SP 800-90C, *Recommendation for Random Bit Generator (RBG) Constructions*. Maryland. Dostupný také z: http://csrc.nist.gov/publications/drafts/800-90/sp800_90c_second_draft.pdf

[10] SONUS. *Sonus* [online]. [cit. 26.5.2017]. Dostupný na WWW: https://www.sonus.net/download/ss7-vulnerabilities

[11] ČESKO. Vyhláška č. 316/2014 Sb., Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)

[12] ČESKO. Vyhláška č. 317/2014 Sb. Vyhláška o významných informačních systémech a jejich určujících kritériích. 2014. Dostupný také z: *http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z&id=27583*

[14] ČSN ISO/IEC 27001, Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky. Praha: Český normalizační institut, 2014.

[15] NÁDENÍČEK, Petr. *SystemOnLine* [online]. [cit. 15.5.2017]. Dostupný na WWW: https://www.systemonline.cz/it-security/uzivatel-jako-zdroj-rizik-a-pristupy-k-jejich-zvladani-1.htm

[16] TECHNET. *Microsoft* [online]. [cit. 26.5.2017]. Dostupný na WWW: https://technet.microsoft.com/en-us/security/jj653751

[17] HRUSKA, Joel. *ExtremeTech* [online]. [cit. 20.5.2017]. Dostupný na WWW: https://www.extremetech.com/computing/237117-windows-10-update-traps-some-systems-in-a-boot-loop-microsoft-promises-fix

[18] IONUT, Ilascu. *SoftPedia* [online]. [cit. 26.5.2017]. Dostupný na WWW: http://news.softpedia.com/news/Self-Destruct-Update-from-Panda-Security-Gets-Manual-Fix-475591.shtml

[19] SCHROTT, Urban. *ESET* [online]. [cit. 26.5.2017]. Dostupný na WWW: https://blog.eset.ie/2016/02/29/eset-releases-and-quickly-fixes-a-faulty-update/

[20] HÁK, Igor. *viry.cz* [online]. [cit. 26.5.2017]. Dostupný na WWW: http://www.fce.vutbr.cz/aiu/vojkuvka.m/u3v/vyuka/Kniha-o-virech.pdf

[21] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 4., aktualiz. a rozš. vyd. Praha: Grada, 2013. Expert (Grada). ISBN 978-80-247-4644-9.

[22] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7.

[23] STORM, Darlene. *ComputerWorld* [online]. [cit. 26.5.2017]. Dostupný na WWW: http://www.computerworld.com/article/2896408/gamers-targeted-by-teslacrypt-ransomware-1-000-to-decrypt-games-mods-steam.html

[24] ČERMÁK, Miroslav. *Clever And Smart* [online]. [cit. 26.5.2017]. Dostupný na WWW: http://www.cleverandsmart.cz/zakladni-bezpecnostni-pravidla-pro-zamestnance/

[25] ČERMÁK, Miroslav. *Clever And Smart* [online]. [cit. 26.5.2017]. Dostupný na WWW: http://www.cleverandsmart.cz/punycode-a-phishing-na-ktery-se-pry-nachytaji-i-bezpecnostni-experti/

[26] ČSN ISO/IEC 27002, Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Soubor postupů. Praha: Český normalizační institut, 2014.

[27] NCKB. *Národní centrum kybernetické bezpečnosti* [online]. [cit. 26.5.2017]. Dostupný na WWW: https://www.govcert.cz/cs/informacni-servis/doporuceni/2486-socialni-inzenyrstvi/

[28] ITIL 2011. *Best Practice* [online]. [cit. 26.5.2017]. Dostupný na WWW: https://www.bestpractice.cz/Files/Documents/itil_2011_summary_of_updates.pdf

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH