Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Bezpečnost ICT – risk management a incident response

Michal Vajdl

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Michal Vajdl

Informatika

Název práce

Bezpečnost ICT – risk management a incident response

Název anglicky

Computer security – risk management a incident response

Cíle práce

Cílem bakalářské práce je analyza rizik hrozící ICT ve vybraném podniku.
Dílčí cíle práce:
- stanovení aktuálních bezpečnostních hrozeb
- nastavení procesů, které mají za účel předcházení rizik a postupů pro řešení vzniklých incidentů

Metodika

Metodika práce je založena na studiu odborné a vědecké literatury a dále pak na konzultacích s oddělením IT a právním oddělením vybraného podniku.

Následně bude provedena analýza rizik a stanovena opatření pro předcházení vybraným rizikům. Na základě zjištěných poznatků bude formulován závěr práce.

Doporučený rozsah práce

Bezpečnost ICT – risk management a incident response

Klíčová slova

počítačová bezpečnost, bezpečnostní rizika, incident response, bezpečnost IT

Doporučené zdroje informací

Broad, J. Risk Management Framework. Syngress, 2013. ISBN: 9780124047235.

Hathaway, M. Best Practices in Computer Network Defense: Incident Detection and Response. Ios Press, 2014. ISBN 9781614993728.

JOHNSON, L R. Computer Incident Response and Forensics Team Management. Syngress, 2014. ISBN: 9780124047259

Loske, A. IT Security Risk Management in the Context of Cloud Computing. Gabler, 2015. ISBN: 9783658113407.

Refsdal, A; Solhaug, B; Stølen, K. Cyber-Risk Management. Springer Verlag, 2015. ISBN: 9783319235707

Předběžný termín obhajoby

2019/20 ZS – PEF (únor 2020)

Vedoucí práce

Ing. Alexandr Vasilenko, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 12. 11. 2018

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 21. 11. 2018

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 25. 11. 2019

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci „Bezpečnost ICT – risk management a incident response“ jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne _____

Poděkování

Rád bych touto cestou poděkoval panu Ing. Alexandru Vasilenkovi, Ph.D., za věcné rady a konzultace při tvorbě práce. Také bych chtěl poděkovat své rodině, za podporu při studiu na vysoké škole.

Bezpečnost ICT – risk management a incident response

Abstrakt

Tato práce je studií, která zkoumá nastavení procesů risk managementu a incident response ve středně velkém podniku v oboru reklamy. V úvodu práce jsou popsány základní požadavky kladené na podniky, metodiky a procesy pro zajištění bezpečnosti jejich informací, aplikací a infrastruktury v souladu s normami z řad ČSN ISO 27000 a ČSN ISO 31000. V analytické části se práce zabývá současnou situací počítačové bezpečnosti v podniku a hodnotí nastavená opatření a jejich dostatečnost. V závěrečné části se věnuje navržení opatření pro minimalizaci rizik hrozících ICT v podniku a nastavení vhodných postupů incident response pro případ vzniku událostí.

Klíčová slova: počítačová bezpečnost, bezpečnostní rizika, risk management, incident response, bezpečnost IT, ISO 27000, ISO 31000

Computer security – risk management a incident response

Abstract

This thesis is a study that investigates the settings of risk management and incident response processes in a medium-sized advertising business. The introduction describes the basic requirements for enterprises, methodologies and the processes to ensure the security of their information, applications and infrastructure in accordance with standards of ISO 27000 and ISO 31000. The analytical portion of this thesis deals with the current situation of computer security in the enterprise and evaluates set measures and their sufficiency. The final part is devoted to proposing measures to minimize the risks of ICT in the company and setting up appropriate incident response procedures in the case these events occur.

Keywords: Computer security, security risks, risk management, incident response, IT security, ISO 27000, ISO 31000

Obsah

Seznam obrázků

Seznam tabulek

Seznam použitých zkratek

- IT – informační technologie (Information technology)
- ICT – informační a komunikační technologie (Information and communication technology)
- ISMS – Systém řízení bezpečnosti informací (Information security management systems)
- BIOS – Basic input/output system
- SCCM – System Center Configuration Manager
- MFA – Multifactor authentification – dvoufázové ověření
- GDPR – Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

1 Úvod

Využívání informačních a komunikačních technologií je v dnešní době běžnou součástí mnoha podniků. Čím dál tím více narůstá ve firmách množství zdrojů, mezi něž řadíme například laptopy, mobilní telefony, síťové prvky a další. Některé podniky by již nemohly bez výpočetní techniky existovat. Dobré fungování informačních technologií je však spojeno s mnoha riziky, kterým se podniky snaží předcházet nastavením kvalitního risk managementu, jenž spočívá v redukci, podstoupení, přenosu rizika a vyhnutí se riziku. (1, str. 21). Nepředvídatelnost a proměnlivost trhu ještě zvyšuje potřebnost takovýchto opatření, jelikož změny trhu s sebou přinášejí i nová potenciální rizika.

V případě omezení nebo dokonce ohrožení informačních systémů využívaných podniky může dojít k závažným potížím v mnoha oblastech od zásobování přes zdravotní péči až po energetiku ap. V zájmu firmy je tedy nepodceňovat zabezpečení IT, které spočívá v identifikaci, analýze a řízení rizik. Tuto agendu má obvykle na starosti IT manažer nebo jiný pověřený pracovník.

Z výše uvedených důvodů jsem se rozhodl zaměřit se ve své bakalářské práci na risk management a incident response ve středně velkém podniku v oboru reklamy, kde jsem momentálně zaměstnán. Dalším důvodem, který mě vedl k výběru tohoto tématu, je silná nedostatečnost opatření ve zmíněném podniku. V neposlední řadě mě tato oblast velmi zajímá a rád bych se v tomto směru dále profesně rozvíjel.

Předmětný podnik, na který se v této práci zaměřuji, je mediální agentura založená v roce 2009. V roce 2016 byla zakoupena globální agenturou. Nyní je součástí celosvětové organizace s 35 tisíci zaměstnanci působících ve 145 zemích a s ročním obratem 200 miliard korun. Před akvizicí nebyla bezpečnost ICT v podniku nijak centrálně řízena. Po akvizici však vznikla potřeba tuto situaci řešit kvůli nařízení nadřízené organizace. Osobně jsem byl v roce 2017 podnikem najat na pozici IT support. Díky tomu mám možnost konzultovat své návrhy s IT specialisty a právním oddělením podniku.

Při tvorbě své práce jsem kromě praktických poznatků a zkušeností získaných ze situace v popisovaném podniku teoreticky vycházel především z norem ČSN a z odborné literatury.

2 Cíl práce a metodika

Hlavním cílem je analýza rizik hrozící počítačové síti modelového podniku.
Dílčí cíle práce:
– stanovení aktuálních bezpečnostních hrozeb;
– nastavení procesů, které mají za účel předcházení rizik, a postupů pro řešení vzniklých incidentů.
Pro firmu budou výsledky analýzy přínosem, neboť je bude moci implementovat do svých procesů. Práce a jí doporučená opatření mohou být použita též v podobných podnicích, pokud jim budou hrozit obdobná rizika.
Metodicky je práce založena na analýze odborné literatury, která byla použita k získání informací pro použití v této práci. Vytěžení literatury prohlubuje pochopení studovaného oboru před začátkem samotného výzkumu. Jako modelový podnik byla použita středně velká firma podnikající v oboru reklamy. Metody použité při zpracování práce se opíraly o normy z řady ČSN ISO/IEC 27000, jež se věnují bezpečnosti informací a souvisejícím metodikám, a o normy z řady ČSN ISO/IEC 31000, které se věnují problematice managementu rizik a souvisejícím metodikám. Pro tvorbu registru rizik a návrhů opatření byla využita Delfská (expertní) metoda.

Názvosloví

- Hacking – neautorizovaný přístup nebo kontrola nad počítačem
- Hung state – stav, ve kterém zařízení nereaguje
- Core switch – switch komunikující na L3 vrstvě
- L2 switch – switch propojující koncová zařízení
- Troubleshooting – řešení problémů

3 Přehled řešené problematiky

Vzhledem k nárůstu množství zařízení připojených do počítačové sítě podniku a závislosti podniků na jejich funkčnosti je zvládnutí rizik hrozících těmto zařízením kruciální pro úspěšný a bezpečný chod podniku. Policie České republiky zaznamenala nárůst kybernetické kriminality z 1502 trestných činů v roce 2011 na 6815 trestných činů zaznamenaných v roce 2018. (2) Podle výzkumu podniknutého společností Microsoft je střední doba odhalení narušení sítě 146 dní, přičemž průměrné náklady poškozené společnosti činí 3,8 milionu dolarů. (3)

Organizace proto musí určit opatření, která zabrání výskytu nesouladu s požadavky ISMS. Preventivní opatření musí být v souladu s těmito požadavky přiměřená závažnosti možných problémů. Zdokumentovaný postup aplikace preventivních činností musí definovat požadavky na:

a) identifikaci potenciálních nesouladů a jejich příčin;

b) vyhodnocení potřeby provedení činností k zamezení opětovného výskytu nesouladu;

c) určení a zavedení potřebných preventivních opatření;

d) zaznamenání výsledků podniknutých opatření;

e) přezkoumání provedených preventivních opatření.

Organizace musí identifikovat změny rizik a požadavky na opatření k nápravě, zejména pak u těch rizik, jejichž změna byla významná. Priority opatření k nápravě budou určeny na základě výsledků vyhodnocení rizik. (4, str. 17)

3.1 Bezpečnost

Pojem bezpečnosti odkazuje na stav, kdy se člověk necítí být ohrožený. Podle studie amerického psychologa Abrahama Harolda Maslowa se jedná o jednu ze základních lidských potřeb pro well–being člověka. (5, str. 370-396)

Obrázek 1Maslowova pyramida potřeb

Zdroj: https://cs.wikipedia.org/

Bezpečnost je i jedním ze základních kamenů pro dobré fungování a rozvoj podniku. Může být definována jako stav, kdy organizaci neohrožují nekontrolované, nepředvídatelné nebo neočekávané události, které mohou vyústit ve ztrátu, rizika jsou na akceptovatelné úrovni a jejich eliminace je efektivní. Součástí zabezpečení podniku je i ochrana zaměstnanců, aktiv, aktivit a reputace podniku. Účelem je zajištění dosažení cílů bez narušení nebo zdržení. Toho je dosahováno pomocí metodologie a strategií. Bezpečnostní metodologie slouží jako podklad pro implementaci bezpečnostních strategií. Zahrnuje metody, teorie a koncepty. Bezpečnostní strategie jsou odvozené od metodologie a odkazují na aplikaci různých aspektů bezpečnosti, jako je fyzická bezpečnost nebo kybernetická bezpečnost. Mezi strategie řadíme odstrašování, klam, detekci, zpoždění, odmítnutí, zmírnění a odpověď. (6, str. 10-11) Risk management je základem korporátní bezpečnosti, rozhodnutí ohledně bezpečnosti by tudíž měla být založena na důkladné analýze rizik.
Posuzování bezpečnostních rizik ve zkoumané společnosti je výrazně zaměřeno na kybernetickou bezpečnost. Jejími základními principy jsou důvěrnost, integrita a dostupnost (v angličtině confidentiality, integrity, and availability), díky čemuž je často nazývána CIA triádou. Cílem důvěrnosti je zajistit dostatečnou úroveň utajení a zamezit neautorizovanému zveřejnění. Integrita je zaměřena na přesnost a důvěryhodnost dat a

předcházení neautorizovaným modifikacím. Účelem dostupnosti je garance toho, aby autorizovaní uživatelé měli přístup k datům a zdrojům ve chvíli, kdy je budou potřebovat. Kontroly minimalizace kybernetických bezpečnostních hrozeb mohou být administrativní, technické a fyzické, jako například školení zaměstnanců, firewall a uzamčení serverovny. Postup, při němž bylo použito více druhů kontrol, se nazývá defense-in-depth. Mechanismy kybernetické bezpečnosti jsou preventivní, detektivní, opravné, odrazující, zotavující a kompenzující. (7, str. 3-10)

3.2 Definice rizika

Existuje mnoho různých definic rizika podle oboru, kde se dané riziko objevuje, mezi jinými i definice podle ISO 31000 o řízení rizik vymezující riziko jako účinek nejistoty na dosažení cílů. Účinek je odchylka od očekávaného – kladná a/nebo záporná. (8, str. 11) Organizace ISO (International Standards Organisation) vytváří dokumenty, které obsahují požadavky, návody, specifikace i charakteristiky, jež mohou být použity pro zajištění toho, aby interní materiály, procesy a služby byly způsobilé jejich účelu. (9)

3.3 Rizika podniku

Rizika ovlivňující podnik mohou mít mnoho různých příčin. Typickými riziky jsou rizika politická, environmentální, plánovací, tržní, ekonomická, finanční, přírodní, projektová, technická, regulační, lidská, trestní, bezpečnostní a právní. ICT zkoumaného podniku hrozí zejména rizika technická, lidská, bezpečnostní, právní a projektová. Zdrojem rizika tedy může být cokoliv, co má vliv na bezpečný chod podniku. Riziko vzniká, pokud je tento vliv nejistý a může ohrozit podnik. (10, str. 16-17)

Existují různé způsoby klasifikace rizik. Rizika mohou být klasifikována jako dynamická, či statická, čistá, nebo spekulativní, celková, či dílčí.

Dynamická rizika, např. politická či finanční, jsou ovlivněna situačními faktory a mohou mít negativní i pozitivní dopady. Podnik ohrožující rizika jsou zejména dynamická. Statická rizika mají pouze negativní dopady, ale na rozdíl od dynamických jsou snáze předvídatelná. Statická rizika jsou taková, která nejsou ovlivněna prostředím podniku. (12, str. 9)

Hopkin rozděluje rizika do čtyř skupin: rizika dodržování předpisů a povinností, nebezpečí a čistá rizika, rizika kontroly a nejistoty a spekulativní rizika a příležitosti.

Rizika dodržování předpisů jsou na základě známých rizik minimalizována, nebezpečí vymýcena, rizika kontroly organizována a rizika příležitostí přijata. Riziko příležitostí je příklad rizika, které může mít pozitivní dopad na podnik. (13, str. 17)

Moeller uvádí čtyři kategorie rizik ohrožujících podnik: rizika strategická, operační, finanční a informační. Strategická rizika zahrnují vnější faktory, jako jsou ekonomická rizika, a interní faktory, jako rizika hrozící reputaci. Operační rizika sestávají z rizik procesních, lidských a rizik vyplývajících z dodržování povinností. Rizika úvěrová, obchodní a správy pokladny jsou finančními riziky. Informační rizika jsou finanční, operační a technologická. (14, str. 25)

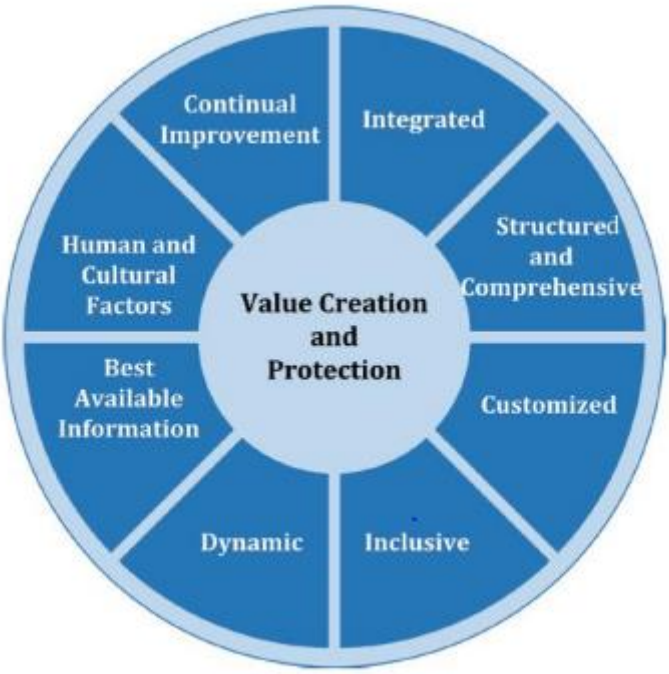
3.4 Risk management

Risk management je proces, který dle ČSN EN 31010:2018 obsahuje 4 hlavní fáze:

- identifikaci rizik;
- zhodnocení rizik;
- ošetření rizik;
- monitoring.

Risk management zahrnuje aktivity, jejichž cílem je řídit a kontrolovat přístup organizace k rizikům. Pokud je dobře zaveden a udržován podle výše uvedené mezinárodní normy, umožňuje organizacím zvýšit pravděpodobnou možnost dosažení cílů, zlepšovat identifikování příležitostí a hrozeb, být v souladu s příslušnými požadavky zákonů, předpisů a mezinárodních norem, zlepšit řízení, účinně rozmístit a využívat zdroje pro ošetření rizik, zlepšit prevenci ztrát a management incidentů a minimalizovat ztráty. Principy dobrého risk managementu, jak je popsán v normě ISO 31000, jsou znázorněny na obrázku níže. Management rizik by měl být integrovaný, strukturovaný a zevrubný, přizpůsobený a dynamický, měl by využívat nejlepší dostupné informace, brát v potaz lidské a kulturní faktory a být neustále zlepšován (8, str. 6–8).

Obrázek 2Principy managementu rizik



Zdroj: ISO 31000:2018, str. 9

Proces managementu rizik organizace je běžně založený na standardech. Standardy managementu rizik popisují proces managementu rizik a doporučený rámec. (13, str. 72) Nejběžnějšími standardy jsou ISO 31000, IRM 2002, ISO/IEC 31010, COSO a OCEG „Red Book“ 2009. (15) Všechny tyto standardy mají obdobnou základní strukturu a skládají se z následujících částí: 1) nastavení zaměření managementu rizik, 2) identifikace rizik a příležitostí, 3) hodnocení rizik, 4) plánování a implementace opatření, 5) reporting a komunikace, 6) pravidelné vyhodnocování kvality a úspěšnosti managementu rizik.
ISO 31000 poskytuje návrh rámce managementu rizik (viz. obrázek 3). Podle toho je management rizik neustále se opakující proces, kdy úkolem organizace je: měřit výkonnost managementu rizik pomocí indikátorů, které jsou periodicky přezkoumávány z hlediska jejich vhodnosti; pravidelně měřit pokrok vzhledem k plánu managementu rizik a odchylky od něj; pravidelně přezkoumávat, zda rámec, politika a plán managementu rizik jsou stále vhodné s ohledem na vnější a vnitřní kontext organizace; podávat hlášení o rizicích, pokroku v rámci plánu managementu rizik, a jak se daří dodržovat politiku managementu rizik; přezkoumávat efektivnost rámce managementu rizik (8, str. 25).

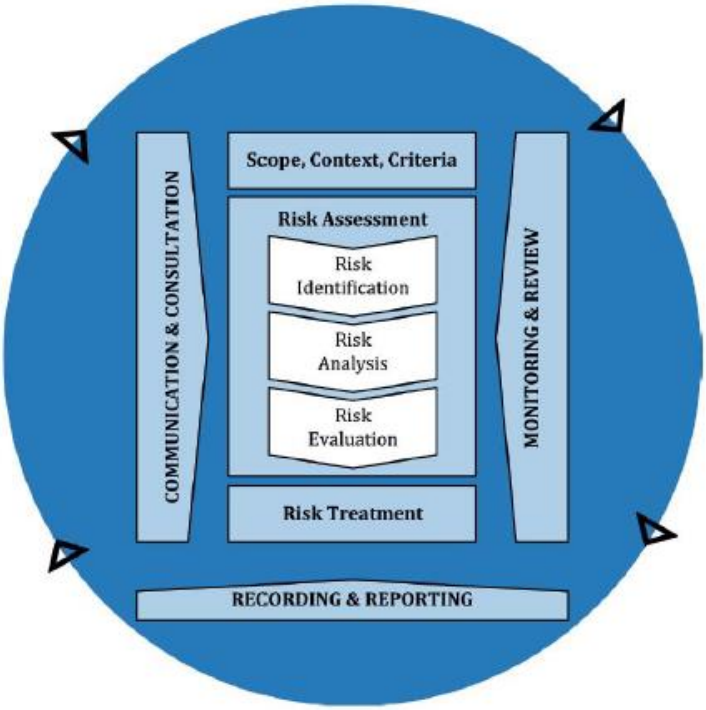
.

Obrázek 3Rámec risk managementu

Zdroj ISO 31000:2018, str. 9

Na obrázku číslo 4 je zobrazen typický proces managementu rizik podle normy ISO 31000. Ten začíná volbou zaměření, kontextu a kritérií. V další fázi, kterou se zabývá tato práce, je posuzování rizik, jež obsahuje identifikaci, analýzu a hodnocení rizik. Po ní následuje fáze ošetření rizik, která zahrnuje výběr a implementaci vhodného plánu ošetření rizik. Celý proces je podporován komunikací a konzultacemi se zainteresovanými vnějšími i vnitřními stranami, monitoringem a přezkoumáváním rámce. (8, str. 13-19)

Obrázek 4Proces managementu rizik



Zdroj ISO 31000:2018, str. 9

Prvním krokem procesu managementu rizik je nastavení zaměření a úkony zajišťující, aby se komunikace o něm dostala ke všem zainteresovaným stranám. Proces může být aplikován na úrovni strategie podniku nebo pouze jako jednotlivý projekt. Při stanovení zaměření může být zohledněno následující: cíle a strategie, očekávané výsledky, čas, lokace, zahrnutí a vyloučení, dostupné nástroje a techniky, zdroje, odpovědnosti, záznamy a vztahy s jinými procesy a činnostmi. (8, str. 14)

Musí být stanoven interní i externí kontext, které mají potenciál ovlivnit dosažení cílů společnosti. To je zásadní krok, jenž má vliv na následné posuzování rizik. Externí kontext může být rozdělen do 3 skupin: 1) mezinárodní, národní a lokální sociální, kulturní, politické, právní, regulační, finanční, technické, přírodní a konkurenční prostředí, 2) klíčové zdroje rizik a trendů ovlivňujících podnik, 3) externí zúčastněné strany. Interní kontext zahrnuje organizační strukturu, firemní kulturu, role, zodpovědnosti, kapacity, schopnosti zaměstnanců, interní systémy a zainteresované strany. Nastavený kontext je zaznamenán v psané formě, schválen managementem a použit pro monitorování a kontrolu. (16, str. 39-42)

Kritéria zohledňují cíle a hodnoty podniku, jeho zdroje, právní a regulační povinnosti a musí být slučitelné s firemními zásadami. Pomáhají určit závažnost rizik a srovnávat jejich úrovně. Mohou obsahovat: 1) povahu a druh příčin a následků a způsoby jejich měření, 2) vymezení postupů při definování pravděpodobnosti, 3) časový rámec pravděpodobnosti a následků, 4) postupy pro výpočet úrovně rizika, 5) názory podílníků, 6) úroveň akceptovatelného rizika, 7) způsoby posuzování kombinace rizik. (16, str. 47-49)

3.5 Posuzování rizik

Posuzování rizik je komplexní proces identifikace rizika, jeho analýzy a hodnocení. Má několik cílů. Je to proces, který pomáhá podniku dělat efektivní a nákladově rentabilní rozhodnutí k řízení a správě rizik. Posuzování rizik je komplexní proces identifikace rizika, jeho analýzy a hodnocení. Je to proces, který pomáhá organizaci dělat efektivní a nákladově rentabilní rozhodnutí k řízení, kontrole a správě rizik. Poskytuje metody pro zkoumání hrozeb, zranitelností a jejich dopadu. Proces posuzování rizik přináší povědomí o rizicích mezi zaměstnance a vede je k tomu, aby se svým dílem snažili přispívat ke kontrole rizik. (17, str. 17) Posuzování rizik má typicky tři fáze: identifikaci rizik, analýzu rizik a vyhodnocení.

Obrázek 5Posuzování rizik

Zdroj: vlastní tvorba

Během identifikace rizik jsou identifikována a popsána významná rizika. Významná rizika jsou ta, u nichž lze s jistou mírou pravděpodobnosti předpokládat, že během určité doby

ovlivní podnik. Efektivním postupem je zapojení zaměstnanců všech úrovní a kategorií napříč organizací, aby pomohli identifikovat a posoudit rizika hrozící jejich oddělením. Model COSO ERM navrhuje brainstorming jako vhodný začátek fáze identifikace rizik. (14, str. 23-24)

Komplexnost identifikace rizik je stěžejní, protože rizika, která nejsou identifikována v tomto stadiu, nebudou zařazena do další analýzy. Identifikace má zahrnout veškerá rizika, ať už jejich zdroje jsou, nebo nejsou řízeny organizací, a to i v případě, že zdroje nebo příčiny rizik nejsou prokazatelné. (8, str. 30) Zásadní podmínkou dosažení platných a spolehlivých výsledků je mít k dispozici aktuální informace. Je tedy třeba dodat dostatečné informace ke každému riziku, jakmile je toto identifikováno. Těmito informacemi jsou cíle, které mohou být rizikem ovlivněny, kontext, zdroj nebo podmínky vzniku, možné následky a současná opatření pro kontrolu rizika.(16, str. 50-52)

Identifikovaná rizika jsou typicky prezentována v registru rizik. Ten zároveň může obsahovat současná opatření a doporučená budoucí opatření pro kontrolu rizika. Možnou nevýhodou této metody je to, že jsou posuzovány pouze hrozby zapsané v registru a proces managementu rizik přestává být dynamický. Registr rizik by tudíž měl být brán spíše jako akční plán popisující současnou situaci managementu rizik a potřebných opatření. (13, str. 88-92)

Obrázek 6Registr rizik

ID	Date raised	Risk description	Likelihood	Impact	Severity	Owner	Mitigating action	Contingent action	Progress on actions	Status
1	12/12/15	There is a risk that assets may not be completed in time to meet production schedules.	Low	High	Amber	S Scott	Agree writing days in advance, reallocate writer's other work. Agree to stagger delivery of chapters so that editing can start earlier.	Increase duration of Printing schedules & move from 4 col to 2 col.	Update 13/12/2015 mitigation actions implemented	Open

Zdroj: https://www.stakeholdermap.com

Druhým krokem procesu posuzování rizik je analýza identifikovaných rizik. Ta zahrnuje zvažování příčin a zdrojů rizik, jejich kladné a záporné následky a možnost výskytu těchto následků. Faktory, které ovlivňují následky a možnosti jejich výskytu, mají být identifikovány. Faktory jako odlišnost názorů mezi experty, nejistota, dostupnost, kvalita, množství a aktuální vhodnost informací nebo omezení při modelování mají být uvedeny a mohou být zdůrazněny.(8, str. 31)

Závěrečným krokem posuzování rizik je jejich hodnocení. Účelem hodnocení rizik je napomoci při rozhodování založeném na výstupech z analýzy rizik o tom, která rizika mají být ošetřena a jaké je stanovení priorit pro implementování řešení. Hodnocení zahrnuje

porovnání úrovně rizik zjištěné v průběhu procesu analýzy se stanovenými kritérii při zohlednění kontextu. Na základě tohoto porovnání může být zvážena potřeba řešení. (8, str. 31)

Rozlišujeme různé typy hrozeb podle původu: záměrné, náhodné nebo přírodní. Hrozby mají dle interních směrnic pět úrovní určených na základě pravděpodobnosti, s jakou nastanou: vzácná (1), nepravděpodobná (2), pravděpodobná (3), očekávaná (4) a téměř jistá (5).

Tabulka 1 Úrovně pravděpodobnosti

	Pravděpodobnost vzniku	Pravděpodobnost	Popis
5	téměř jistá	>80%	běžně se vyskytuje v rámci podniku
4	očekávaná	61–80%	mnohokrát se přihodila v rámci podniku
3	pravděpodobná	31–60%	několikrát se přihodila v rámci podniku
2	nepravděpodobná	11–30%	v malém množství případů se přihodila v rámci podniku
1	vzácná	<10%	přihodila se v rámci podniku jednou/nikdy

Zdroj: interní směrnice

Dále se u hrozeb určuje úroveň zranitelnosti podniku podle efektivity v současnosti zavedených bezpečnostních kontrol a doba, po kterou se podniku bude zotavovat z incidentu. Úrovně zranitelnosti jsou: velmi nízká (1), nízká (2), významná (3), velmi významná (4), kritická (5).

Dopad rizik pro podnik může být přímý i nepřímý. Následky ukazuje následující tabulka.

Tabulka 2 Úrovně dopadů rizik

Úroveň dopadu		Finanční	Reputační	Operační
5	kritická	více než 100 milionů Kč	• dlouhodobé (déle než 1 měsíc trvající) extenzivní negativní pokrytí způsobující závažnou ztrátu důvěry zainteresovaných stran; • ztráta více klíčových klientů	• okamžitý dopad přímo na služby klientům
4	velmi významná	51–100 milionů Kč	• krátkodobé extenzivní negativní mediální pokrytí • ztráta klíčového klienta	• krátkodobý dopad přímo na služby klientům; • dlouhodobý dopad na poskytování služeb zaměstnancům
3	významná	26–50 milionů Kč	• dlouhodobé negativní mediální pokrytí; • ztráta více klientů	• dlouhodobý dopad přímo na služby klientům v rámci bussiness unit; • střednědobý dopad na poskytování služeb zaměstnancům
2	nízká	11–25 milionů Kč	• krátkodobé negativní mediální pokrytí; • ztráta klienta	• krátkodobý dopad přímo na služby klientům v rámci bussiness unit; • krátkodobý dopad na poskytování služeb zaměstnancům
1	velmi nízká	2–10 milionů Kč	• krátkodobé negativní mediální pokrytí	• krátkodobý dopad na poskytování služeb zaměstnancům mimo klíčová oddělení

Zdroj: interní směrnice

Rychlost rizika je odhad, jak rychle dopad rizika ovlivní společnost. Rychlost rizika nemá vliv na úroveň rizika jako takového, ale pomáhá při plánování a určování priorit zmírňování rizik. Rychlost rizika má tři stupně: vysokou (méně než 3 měsíce), střední (3–12 měsíců) a nízkou (více než 12 měsíců). Většina rizik ovlivňuje podnik s vysokou rychlostí.

Závažnost rizika se vypočítává za pomoci údajů o úrovni dopadu na podnik a pravděpodobnosti vzniku události – čím vyšší je hodnota rizika, tím je riziko závažnější.

Tabulka 3 Tabulka závažnosti rizik

Dopad	kritický	5	10	15	20	25
	velmi významný	4	8	12	16	20
	významný	3	6	9	12	15
	nízký	2	4	6	8	10
	velmi nízký	1	2	3	4	5
		nepravděpodobná	nejistá	pravděpodobná	očekávaná	jistá
		Pravděpodobnost				

Zdroj: interní směrnice

3.6 Ošetření rizik a monitoring

Ošetření rizik zahrnuje výběr jedné nebo více možností pro změnu (modifikování) rizik a jejich zavedení do podniku. Jakmile jsou zavedeny, ošetření poskytnou nebo změní opatření.

Cyklický proces ošetření rizik zahrnuje:

- posuzování ošetření rizika;
- rozhodování, zda úroveň zbytkového rizika je tolerovatelná;
- vygenerování nového ošetření, pokud tolerovatelná není;
- vyhodnocování efektivnosti ošetření.

Možnosti pro ošetření rizik se nemusí navzájem vylučovat a zároveň jednotlivé možnosti nemusí být vhodné za všech okolností. Možnosti mohou obsahovat:

- vyvarování se rizika rozhodnutím nezačínat nebo nepokračovat s činnostmi, které dávají vzniknout riziku;
- přijetí nebo zvýšení rizika za účelem dosáhnout příležitosti;
- odstranění zdroje rizika;
- změnu možnosti výskytu rizika;
- změnu následků rizika;

- sdílení rizika s jinou stranou nebo stranami (včetně smluv a financování rizika);
- zachování rizika na základě informovaného rozhodnutí (8, str. 32).

Procesy monitorování a přezkoumávání v organizaci mají zahrnovat všechny aspekty procesu managementu rizik pro účely:

- zjištění, že opatření jsou efektivní a účinná jak v návrhu, tak ve vlastním provozu;
- získání dalších informací pro zlepšení posouzení rizik;
- analyzování událostí (včetně skoronehod), změn, trendů, úspěchů a chyb a poučení se z nich;
- rozpoznání změn ve vnějším i vnitřním kontextu, včetně změn kritérií rizik a rizik samotných, které mohou vyžadovat revizi ošetření rizik a priorit;
- identifikování nově se objevujících rizik.

Výsledky monitorování a přezkoumávání mají být zaznamenány a externě i interně hlášeny vhodným způsobem a rovněž mají sloužit jako vstup pro přezkoumání rámce managementu rizik.

3.6.1 Vyhnutí se riziku

je jednou ze strategií kontroly rizik. Strategie předcházení rizik zahrnuje situace, kde určité vystavení riziku není přijato nebo existující vystavení riziku je opuštěno. Například ztrátám způsobeným záplavami lze předejít tím, že nová pobočka podniku nebude postavena v záplavové zóně. (18, str. 44) Jinými slovy, pokud je předpokládaný risk vyšší než tolerance rizika, není důvod, proč ho podstupovat. Pokud je to možné, je preferováno jiné řešení, například v uvedeném příkladu postavit onu novou pobočku na pozemku sice dražším, ale mimo záplavovou zónu.

Ačkoliv výhody předcházení rizik jsou jasně viditelné, má tato strategie i své nevýhody: není vždy možné předpokládat nebo kontrolovat všechna rizika (například smrt člena vrcholného managementu) nebo některá vnější rizika, která nelze eliminovat, jelikož jsou součástí obchodních operací (možnost krachu hlavního odběratele, která způsobí přerušení obchodního řetězce, apod.). (18, str. 45)

Přenášení rizik jsou způsoby, jak přenést zodpovědnost za případné škody mimo společnost na třetí osobu. (19, str. 51-52) Existují tři druhy přenášení rizik. Prvním jsou finanční instituce nesoucí riziko, jako jsou pojišťovny, které pokrývají předem smluvně

dohodnutá rizika za pravidelný poplatek od společnosti. Druhým jsou smluvní převody, kdy například za škody na zboží od okamžiku jeho expedice do předání v cílové destinaci je zodpovědný přepravce. Třetím způsobem je převod s omezenou odpovědností, kdy podnik neposkytuje záruky nebo neručí svým majetkem za případný bankrot, pokud se k tomu explicitně nezaváže.

3.6.2 Modifikace rizika

odkazuje na opatření, která sníží závažnost ztráty poté, co tato nastane. (18, str. 46) Tato strategie může být použita například po ztrátě nebo zcizení kreditní karty zablokováním transakcí s použitím této karty. Pokud bude po zablokování provedena nějaká transakce, náhrada škody půjde za společností provozující tuto kartu, respektive za pojišťovací společností, která ji kryje.

3.6.3 Podstoupení rizika

Podstoupení rizika se přijímá zejména u malých a nevýznamných rizik, která se objevují vzácně nebo málo a mají nízký dopad na podnik. Takovým rizikem může být například souběžná nemoc obou specialistů malého oddělení podniku tvořeného pouze těmito dvěma zaměstnanci. Pravděpodobnost, že tato možnost nastane, je nízká a náklady na třetího zaměstnance pracujícího z domova by byly vyšší než případné najmutí dočasné výpomoci.

4 Vlastní práce

Nadřízená organizace nedávno provedla akvizici modelového podniku, aby rozšířila svůj podíl na českém trhu. Modelový podnik v rámci zařazení do struktury nadřízené organizace přejal její nastavení bezpečnostní politiky. To dle interních materiálů dělí bezpečnostní rizika do 4 oblastí:

1) ochrana citlivých dat;
2) ochrana kritické podnikové infrastruktury;
3) ochrana fyzických zařízení;
4) ochrana lidských zdrojů.

Politika nadřízené organizace doporučuje a určuje:

1) použít běžná řešení užívaná v organizaci;
2) IT manažer je zodpovědný za IT řešení;
3) jednotlivé společnosti organizace odpovídají za svá rizika a činnosti konané k jejich zmírnění;
4) přizpůsobení v podniku jsou prováděna podle trendů a identifikovaných rizik.

Do první výše jmenované oblasti spadá vybavení, média, krádež nebo ztráta dokumentů, lidská chyba, hacking, sabotáž systému nebo jeho narušení, hrozba zevnitř, malware, odposlouchávání nebo úprava komunikace a sociální inženýrství.
Do druhé oblasti patří lidská chyba, hacking, sabotáž systému nebo jeho narušení, hrozba zevnitř, malware, útok odepřením služby, nefunkčnost infrastruktury nebo aplikace, kriminální hrozby a násilí, fyzická rizika a hrozby a přírodní neštěstí.
Třetí oblast zahrnuje kriminální hrozby a násilí, fyzická rizika a hrozby a přírodní neštěstí.
Do čtvrté oblasti jsou začleněny kriminální hrozby a násilí, fyzická rizika a hrozby, přírodní neštěstí a zdravotní potíže.

4.1 Analýza současného stavu

V této podkapitole uvádím úplnou analýzu současného stavu podniku. Výsledky této analýzy budou následně použity k tvorbě návrhu opatření pro minimalizaci rizik v podniku.
Firma má okolo 190 zaměstnanců (v podniku je poměrně vysoká fluktuace a počet zaměstnanců se v průběhu psaní práce průběžně měnil) a roční obrat zhruba 1100 milionů

Kč. Sídlo firmy leží v pronajatých prostorách v Praze. S centrálou nadřízené společnosti, kde jsou umístěny servery, je spojeno pomocí internetu. Toto spojení bylo firmě nařízeno po akvizici nadřízenou společností. Kanceláře firmy se nacházejí v přízemí a v 1. patře kancelářské budovy a zabírají plochu zhruba 2000 metrů čtverečních. Přístup do nich je možný přes recepci kanceláře nebo zadním vchodem. Recepce je zajišťována pronajímatelem prostor v časovém rozmezí 8:00–18:00 během pracovních dní a je společná i pro firmu sousedící ve vedlejším prostoru. Recepční nevyžadují od návštěvníků identifikaci a nevedou žádný seznam návštěv. Osoba tvářící se jako zaměstnanec tudíž bez problémů projde do prostor firmy. U vstupu do budovy je recepce budovy společná pro všechny nájemce, recepční však pouze směrují návštěvníky do správných prostor. Kontrola, zda je osoba přicházející do prostoru kanceláří zaměstnancem podniku, neprobíhá. Přístup zadním vchodem je zabezpečen kováním typu koule a odemykáním na čipovou kartu. Čipové karty jsou vydávány konkrétním zaměstnancům. Plánuje se stěhování do nových prostor ve 4. a 5. nadzemním podlaží kancelářské budovy.
Laptopy mají mix operačních systémů Windows 7 Home (2 zařízení), Windows 7 Professional (52 zařízení) a Windows 10 Professional (88 zařízení). Macbooky mají mix operačních systémů OS X 10.10 Yosemite (1 zařízení), OS X 10.11 El Capitan (4 zařízení), macOS 10.12 Sierra (27 zařízení) a macOS 10.13 High Sierra (21 zařízení). Všechny uživatelské účty jsou lokální a mají administrátorská práva, což znamená, že každý uživatel může stahovat a instalovat libovolný software. E-mailové služby a sdílený disk poskytuje společnost Google v rámci produktu Google Suite, který se zároveň stará i o ochranu proti spamu pomocí umisťování e-mailových adres generujících spamové e-maily na seznam (blacklist). V kancelářských prostorách je dostupná WiFi síť pro bezdrátové připojení k internetu. Tato síť je zabezpečena technologií WPA2 (Wi–Fi Protected Access 2), heslo je sdílené pro všechny zaměstnance. WiFi připojení zajišťuje čtveřice zařízení Aruba IAP–225RW, které s minimálním přesahem pokrývají prostory firmy.
Hardwarové vybavení tvoří mix zařízení pořízených před akvizicí a po ní nadřízenou společností. Zařízení pořízená před akvizicí u retailových prodejců jsou: Hewlett–Packard ProBook 430 3. a 4. generace, Hewlett–Packard ProBook 450 3. generace, Hewlett–Packard ProBook 455 4. generace, Lenovo ThinkPad X240, Asus ZenBook UX305C, MacBook Air 13“ verze Mid 2013, Early 2014 a Early 2015, MacBook Pro 13“ Retina verze Early 2013, Late 2013 a Early 2015, MacBook Pro 15“ Retina verze Early 2013 a Mid 2015 a iMac 27“ verze Late 2013. Zařízení s operačním systémem Windows,

pořizovaná po akvizici, jsou zakoupena přímo od společnosti Dell. Zařízení s operačním systémem macOS jsou i po akvizici pořizována u retailových prodejců. Zařízení nakupovaná po akvizici jsou: Dell Latitude 3460, 3480, 7290, 7480, 7490 a 5300 a stolní počítače Dell Optiplex 7080.
V prostorách kanceláří není umístěn žádný server, ten je umístěn v evropské centrále nadřízené společnosti v Londýně. České kanceláře jsou s ní spojeny pomocí VPN tunelu. Na pobočce se nacházejí 3 zařízení QNAP TS–212 pro lokální ukládání dat projektů a kampaní. O bezpečnost připojení k internetu se starají hardwarové firewally Juniper SRX210 a SRX240, switche HP ProCurve 1410–24G, HP ProCurve 1810G–24, D–Link DGS–1016D a D–Link DGS–1210–48 a jsou umístěny v uzamčeném racku v prostoru kuchyňky dostupné všem zaměstnancům firmy, kabeláž je přístupná.
Softwarové vybavení tvoří kancelářské balíky Microsoft Office verzí 2010, 2013 a 2016 Professional, programy Adwind Kite, Median Media Office a Buying.
Software pro zařízení s operačním systémem macOS Pages, Numbers, Adobe Creative Cloud, Slack.

4.2 Současný stav risk managementu

Před akvizicí nadřízenou organizací nebyl risk management v podniku nijak centrálně řízen. Po akvizici vyvstala potřeba dosáhnout standardů organizace. Budova není vybavena protipožárním systémem. Není zajištěno napájení síťových zařízení v případě výpadku dodávky elektrického proudu. Fyzický přístup k síťovým zařízením má každý zaměstnanec nebo návštěvník prostor firmy. Firewall je pouze jeden a switche mají minimální rezervu volných portů. Překryv pokrytí signálem WiFi sítě je minimální a v případě výpadku jednoho routeru není možnost distribuce signálu WiFi ke všem uživatelům v nezhoršené kvalitě. Náhradní router není zařízen.
Centrální monitoring zdrojů podniku není řádně zaveden. Pro jejich evidenci slouží sdílená excelová tabulka, která neobsahuje veškeré zdroje ani aktuální data. Tabulka je spravována oddělením office managementu.
Dedikované IT oddělení nebylo součástí podniku. Stanice nejsou zařazeny v doméně a veškeré účty jsou lokální. Každý uživatel má na své pracovní stanici práva administrátora. Antivirová ochrana zařízení s Windows je řešena nativní aplikací Windows Defender. Antivirová ochrana zařízení s macOS není řešena. V případě poruchy pracovní stanice je

zaměstnanec odkázán na použití vlastního zařízení, než je jemu přidělené firemní zařízení opraveno v servisu.
Přístupová práva k souborům na sdílených discích jsou udělována jednotlivým uživatelům, při jejich odchodu nejsou rušena, počítá se s rušením e-mailového účtu. E-mailové účty jsou zakládány a mazány office managementem na žádost manažerů jednotlivých oddělení. Žádost nemusí být písemná. Při kontrole bylo zjištěno, že některé e-mailové účty zůstaly aktivní více než rok po odchodu zaměstnance z firmy.
Není nastavena žádná politika určující obtížnost hesla do pracovních stanic nebo do emailových účtů. Hesla mají neomezenou platnost. Na pracovních stanicích není použito žádné šifrování disku. Není nastaven proces pro ochranu firemních dat v případě krádeže nebo ztráty pracovní stanice či mobilního telefonu. Ochrana proti phishingu a spamu je řešena na úrovni Google Suite.

4.3 Návrh opatření

Pro vytvoření registru rizik bylo osloveno 11 expertů působících na pozicích IT manažer nebo IT ředitel ve středně velkých podnicích. Těmto osobám byl zaslán dotazník na rizika, která podle nich hrozí předmětnému podniku. Z došlých odpovědí byl vytvořen seznam rizik, jenž jim byl poté znovu odeslán na ohodnocení závažnosti, dopadu a pravděpodobnosti výskytu. Z výsledných tabulek byl vytvořen samotný registr rizik. Vybraný podnik se chystá na stěhování a níže uvedené návrhy řešení risk managementu proto pracují s přípravou nových kancelářských prostor v souladu s normami a interními směrnicemi nadřízené organizace místo vylepšování stavu v současných prostorách.

4.3.1 Přírodní neštěstí

Požár

Příčina: Cílený nebo náhodný vznik požáru (například z důvodu zkratu elektrického vedení).
Dopad: Poškození nebo zničení zdrojů, elektroinstalace a síťového vybavení.
Ošetření: Kancelářská budova vybraná pro stěhování je vybavena hlásiči kouře, protipožárními zástěnami a požárními rozprašovači. Kancelářské prostory jsou vybaveny přenosnými hasicími přístroji pro hašení lokálních ohnisek požáru. Serverovna je stavebně oddělena protipožární vložkou od zbytku kancelářských prostor. Veškerá elektroinstalace do serverovny prochází protipožárními kabelovými průchodkami. Pro pokrytí případných škod vzniklých požárem bude podnik pojištěn.
Reakce: Office manager v součinnosti s finančním a IT oddělením provede kontrolu vzniklých škod a kontaktuje zástupce pojišťovny. Ředitel IT zajistí externí spolupracovníky pro uvedení všech poškozených zdrojů do funkčního stavu.

4.3.2 Systémové hrozby

Přerušení dodávek elektrického proudu

Příčina: Přerušení vedení elektrického proudu či narušení přenosové soustavy přírodními nebo lidskými silami.
Dopad: Nedostupnost serverů, nedostupnost síťových úložišť, nefunkčnost síťového připojení, nefunkčnost pracovních stanic

Ošetření: Vybavení serverovny zdroji nepřerušovaného napájení (UPS) (20, str. 1) pro klíčová zařízení na 30 minut.
Reakce: Office manager v případě výpadku kontaktuje správce kancelářské budovy s žádostí o nápravu stavu. Pokud Office manager není přítomen, kontakt provádí Reception Chief, pokud není přítomen ani ten, kontakt provádí recepce.

Ochrana proti přepětí

Příčina: Elektrické napětí vyšší než nejvyšší povolené provozní napětí (tj. nejvyšší napětí pro zařízení). (21)
Dopad: Poškození síťových prvků, nefunkčnost síťového připojení.
Ošetření: Vybavení serverovny zdroji nepřerušovaného napájení (UPS) (20, str. 1) s ochranou proti přepětí.
Reakce: Ředitel IT zajistí výměnu nefunkčních zařízení, právní oddělení kontaktuje výrobce UPS s žádostí o náhradu škody kvůli nefunkčnosti zařízení.

Přerušení síťového připojení

Příčina: Nefunkčnost síťového připojení na trase od dodavatele síťových připojení (Internet Service Provider – ISP) k firewallu z důvodu fyzického přerušení linky vedení nebo jiných obtíží na straně dodavatele.
Dopad: Nefunkčnost síťového připojení.
Ošetření: Zajištění primární a sekundární linky internetového připojení. Každá linka bude zajištěna jiným dodavatelem internetového připojení pro případ kompletního výpadku poskytovaných služeb od dodavatele. Sekundární linka bude vedena bezdrátově. Nastavení síťových prvků pro automatické přepnutí na sekundární linku v případě výpadku primární linky.
Reakce: Ředitel IT se spojí s kontaktní osobou ISP a zajistí obnovení služeb. V případě nepřítomnosti ředitele IT provede kontaktování ISP IT support.

Disfunkce firewallu

Příčina: Poškození vlivem přepětí, poškození opotřebením, zamrznutí zařízení v „hung state“, změna konfigurace.
Dopad: Nefunkčnost síťového připojení.

Ošetření: Nákup firewallů Cisko Meraki MX250, zdvojení firewallu, seznámení oddělení IT s možnostmi restartování zařízení, komunikace všech změn na zařízení s celým IT oddělením, provádění změn mimo pracovní dobu zaměstnanců společnosti, vybavení všech zaměstnanců laptopy (z důvodu interní směrnice vyjma finančního oddělení).

Reakce: V případě poruchy zařízení ředitel IT kontaktuje zástupce dodavatele a zajistí dodání náhradního kusu. Pokud není přítomen, IT support kontaktuje IT manažera clusteru nadřízené společnosti, který zajistí výměnu. V případě zamrznutí provede člen IT oddělení, který si stavu všimne, restart zařízení. Pokud se projeví nefunkčnost po změně konfigurace v průběhu pracovní doby a není vyřešena do 30 minut od nahlášení, je konfigurace změněna na poslední známou funkční verzi.

Disfunkce core switche

Příčina: Poškození vlivem přepětí, poškození opotřebením, poškození převodníku optického signálu (Small form–factor pluggable transceiver – SFP), zamrznutí zařízení v „hung state“, změna konfigurace.

Dopad: Nefunkčnost síťového připojení, nefunkčnost zařízení napájených způsobem PoE.

Ošetření: Nákup switchů Cisko Meraki MS250–24P, zdvojení switche, seznámení oddělení IT s možnostmi restartování zařízení, komunikace všech změn na zařízení s celým IT oddělením, provádění změn mimo pracovní dobu zaměstnanců společnosti, vybavení všech zaměstnanců (z důvodu interní směrnice vyjma finančního oddělení) laptopy.

Reakce: V případě poruchy zařízení nebo převodníku ředitel IT kontaktuje zástupce dodavatele a zajistí dodání náhradního kusu. Pokud není přítomen, IT support kontaktuje IT manažera clusteru nadřízené společnosti, který zajistí výměnu. V případě zamrznutí provede člen IT oddělení, který si stavu všimne, restart zařízení. Pokud se projeví nefunkčnost po změně konfigurace v průběhu pracovní doby a není vyřešena do 30 minut od nahlášení, je konfigurace změněna na poslední známou funkční verzi. IT support provede přepojení počítačů finančního oddělení do funkčního switche.

Disfunkce L2 switche

Příčina: Poškození vlivem přepětí, poškození opotřebením, zamrznutí zařízení v „hung state“, změna konfigurace.

Dopad: Nefunkčnost síťového připojení pro část zaměstnanců.

Ošetření: Naddimenzování počtu switchů, aby bylo možné pokrýt výpadek jednoho switche přepojením síťových kabelů do ostatních zařízení, seznámení oddělení IT

s možnostmi restartování zařízení, komunikace všech změn na zařízeních s celým IT oddělením, provádění změn mimo pracovní dobu zaměstnanců společnosti, vybavení všech zaměstnanců laptopy (z důvodu interní směrnice vyjma finančního oddělení).

Reakce: V případě poruchy zařízení ředitel IT kontaktuje zástupce dodavatele a zajistí dodání náhradního kusu. Pokud není přítomen, IT support kontaktuje IT manažera clusteru nadřízené společnosti, který zajistí výměnu. V případě zamrznutí provede člen IT oddělení, který si stavu všimne, restart zařízení. IT support provede přepojení počítačů finančního oddělení do funkčních zařízení.

Disfunkce síťového úložiště

Příčina: Poškození vlivem přepětí, poškození opotřebením, nárůst množství nefunkčních sektorů na disku, disfunkce připojení k síti, zamrznutí zařízení v „hung state“, změna konfigurace.

Dopad: Nedostupnost síťových disků pro zaměstnance.

Ošetření: Pořízení zařízení Synology DS1517+ (nařízení nadřízené organizace) s dvěma konektory RJ45, zapojení ethernetových kabelů ze zařízení do rozdílných core switchů, zdvojení síťového úložiště, nastavení RAID 5 na každém z nich, nastavení clusteru z obou zařízení, seznámení oddělení IT s možnostmi restartování zařízení/uvolnění z hung state, komunikace všech změn na zařízeních s celým IT oddělením, provádění změn mimo pracovní dobu zaměstnanců společnosti, pořízení rezervního disku.

Reakce: V případě poruchy zařízení ředitel IT kontaktuje zástupce dodavatele a zajistí dodání náhradního kusu. Pokud není přítomen, IT support kontaktuje IT manažera clusteru nadřízené společnosti, který zajistí výměnu. V případě zamrznutí provede člen IT oddělení, který si stavu všimne, přepnutí aktivního zařízení na sekundární v clusteru a následně restart postiženého zařízení. V případě poškození disku provede IT support výměnu za rezervní kus.

Disfunkce LAN sítě

Příčina: Poškození opotřebením, fyzické poškození.

Dopad: Nedostupnost síťového připojení pro konkrétního uživatele.

Ošetření: Zdvojení ethernetové linky ke každému pracovnímu místu, vybavení všech zaměstnanců laptopy (z důvodu interní směrnice vyjma finančního oddělení).

Reakce: IT support provede kontrolu měřákem, zda se nejedná o poruchu v prostoru switch–panel nebo zástrčka–zařízení. V případě zjištění závady provede dle zjištění výměnu kabelu nebo postupuje podle bodů disfunkce switche / pracovní stanice. Při

nezjištění závady kontaktuje office manager správu budovy a zajistí opravu nebo výměnu poškozeného kabelu.

Disfunkce WiFi sítě

Příčina: Poškození přívodního ethernetového kabelu, přerušení napájení PoE, zamrznutí v „hung state“, změna konfigurace.

Dopad: Nedostupnost WiFi sítě pro zaměstnance.

Ošetření: Rozmístění přístupových bodů pro vytvoření překrývajících se polí signálu, jejich zapojení střídavě do obou core switchů.

Reakce: IT support provede dle stavu restart příslušného přístupového bodu nebo kontrolu ethernetového kabelu a napájení způsobem PoE. V případě závady na těchto součástech sítě provede postup dle bodů disfunkce LAN sítě / core switche. V případě závady na přístupovém bodu kontaktuje IT manager dodavatele zařízení a zajistí výměnu. V jeho nepřítomnosti kontakt provede IT support.

Disfunkce pracovní stanice

Příčina: Poškození zařízení opotřebením, chyba operačního systému, chyba softwaru.

Dopad: Znemožnění práce zaměstnance, ztráta dat uložených na zařízení.

Ošetření: Nákup pracovních stanic s prodlouženou zárukou a službou Next bussines day on–site Pro support od společnosti Dell (výměna poškozené součástky následující pracovní den po nahlášení závady na kontaktní linku, pouze pro zařízení značky Dell), postup dle interní směrnice nařizující ukládání pracovních dat na síťové úložiště, dostupná náhradní pracovní stanice v IT oddělení.

Reakce: IT support poskytne uživateli náhradní zařízení a provede diagnostiku stanice. Při zjištění hardwarového problému zkontroluje platnost záruky a kontaktuje hotline služby NBD Pro support v případě zařízení Dell, v případě zařízení Apple domluví s asistentem managementu odvoz do autorizovaného servisu na provedení záruční opravy. V případě propadlé záruky IT support zjistí odhadovanou cenu opravy, kterou předloží IT řediteli ke schválení. V případě schválení zajistí IT support opravu. Pokud by tato byla nerentabilní, objedná IT ředitel novou pracovní stanici. Není-li zjištěna hardwarová chyba, provede IT support aktualizaci firmwaru a ovladačů. Jestliže chyba zůstává i nadále, vytvoří IT support zálohu uživatelských dat a reinstaluje stanici. Pokud je chyba na nainstalovaném softwaru, podnikne IT support kroky troubleshootingu, respektive reinstalaci softwaru.

Disfunkce telefonní ústředny

Příčina: Změna konfigurace, zamrznutí v „hung state“.

Dopad: Ztráta telefonního spojení.

Ošetření: Seznámení všech členů IT oddělení s možnostmi restartování zařízení, komunikace všech plánovaných změn a jejich provádění mimo pracovní dobu uživatelů.

Reakce: Člen IT oddělení, který nefunkčnost zařízení zjistí, zkontroluje stav zařízení, a pokud je to nutné, provede jeho restart. V případě poruchy zařízení objedná IT ředitel u dodavatele výměnu. V době jeho nepřítomnosti IT support kontaktuje IT manažera clusteru, který zajistí výměnu.

Disfunkce SQL serveru

Příčina: Poškození vlivem přepětí, poškození opotřebením, zamrznutí v „hung state“, poškození databáze.

Dopad: Nedostupnost některých služeb pro uživatele.

Ošetření: Seznámení všech členů IT oddělení s možnostmi restartování zařízení, nastavení zálohování databáze na síťové úložiště, náhradní desktopová stanice k dispozici v IT oddělení (SQL server běží na desktopu).

Reakce: Člen IT, který disfunkci zaznamená, provede restart / výměnu zařízení nebo obnovení databáze ze zálohy dle zjištěné závady, následně odešle komunikaci k postiženým uživatelům ohledně verze obnovené databáze.

Porucha silového rozvodu

Příčina: Přerušení silového rozvodu fyzickým poškozením, přerušení silového rozvodu opotřebením.

Dopad: Přerušení dodávky elektrického proudu k pracovnímu místu zaměstnance / k jinému zařízení.

Ošetření: Zdvojení vedení silového rozvodu ke každému pracovnímu místu / výklenku pro tiskárny a skartovacímu stroji.

Reakce: Office manažer kontaktuje správu budovy a zajistí výměnu poškozeného vedení. V době nepřítomnosti Office manažera kontakt provádí vrchní recepční.

Poškození pracovní stanice

Příčina: Poškození nevhodnou manipulací ze strany uživatele (pád zařízení, vylomení displeje, poškození klávesnice apod.), poškození neopatrnými aktivitami v okolí zařízení (převržení sklenice s vodou, upuštění předmětu na zařízení apod.), smazání systémového souboru uživatelem.

Dopad: Znemožnění práce zaměstnance, ztráta dat uložených na zařízení.

Ošetření: Interní směrnice nařizující ukládání pracovních dat na síťové úložiště, náhradní pracovní stanice dostupná v IT oddělení, doporučení zaměstnancům pro zřízení pojištění odpovědnosti, uživatelské účty nemají přidělena oprávnění administrátora.
Reakce: IT support poskytne uživateli náhradní zařízení a provede diagnostiku stanice. IT support zjistí odhadovanou cenu opravy, kterou předloží IT řediteli ke schválení. Při schválení zajistí IT support provedení opravy. Pokud by tato byla nerentabilní, objedná IT ředitel novou pracovní stanici. Finanční oddělení vyčíslí škodu požadovanou po zaměstnanci. Manažer oddělení domluví se zaměstnancem způsob náhrady způsobené škody. Není-li zjištěno hardwarové poškození, provede IT support zálohu uživatelských dat, pokud to stav zařízení dovoluje, a reinstalaci stanice. Je-li chyba na nainstalovaném softwaru, podnikne IT support kroky troubleshootingu, respektive reinstalaci softwaru.

Ztráta pracovní stanice

Příčina: Ztráta pracovní stanice chybou zaměstnance.
Dopad: Znemožnění práce zaměstnance, ztráta dat na zařízení.
Ošetření: Šifrování interního disku, použití hesla pro přístup do BIOS, správa pracovních stanic pomocí SCCM, interní směrnice nařizující ukládání pracovních dat na síťové nebo cloudové úložiště, náhradní pracovní stanice dostupná v IT oddělení, doporučení zaměstnancům pro zřízení pojištění odpovědnosti, školení zaměstnanců o nutnosti okamžitého nahlášení ztráty zařízení.
Reakce: IT support vymaže data ze stanice pomocí SCCM a poskytne uživateli náhradní zařízení. IT ředitel objedná novou pracovní stanici. Finanční oddělení vyčíslí škodu požadovanou po zaměstnanci. Manažer oddělení dohodne se zaměstnancem náhradu způsobené škody.

Ztráta mobilního telefonu

Příčina: Ztráta mobilního telefonu chybou zaměstnance.
Dopad: Ztížení práce zaměstnance, ztráta dat a kontaktů uložených na zařízení.
Ošetření: Povinná instalace aplikace Microsoft Intune do zařízení pro možnost nastavení firemního e-mailu na telefon, povinné nastavení zámku obrazovky, školení zaměstnanců o nutnosti okamžitého nahlášení ztráty zařízení.
Reakce: IT support vymaže data z telefonu pomocí správcovského rozhraní Intune. Při ztrátě firemního telefonu poskytne IT support zaměstnanci náhradní zařízení a finanční oddělení vyčíslí náhradu škody. Manažer oddělení dohodne se zaměstnancem náhradu způsobené škody. IT ředitel objedná nové zařízení a náhradní SIM kartu. IT support

vyresetuje dvoufázové ověření a asistuje zaměstnanci při spárování nového mobilního telefonu s MFA.

Náhodné smazání souboru

Příčina: Neúmyslné smazání souboru/složky uživatelem.
Dopad: Ztráta pracovních dat, nedodržení termínů, ohrožení služeb klientům.
Ošetření: Interní směrnice nařizující ukládání pracovních dat na síťové nebo cloudové úložiště, zálohování síťového uložiště Synology do cloudového úložiště Microsoft Azure pomocí nástroje Hyper Backup.
Reakce: IT support provede obnovení souboru/složky ze zálohy.

Odeslání dat nesprávnému příjemci

Příčina: Neúmyslné odeslání citlivých informací nesprávnému příjemci.
Dopad: Poškození reputace podniku, finanční škody.
Ošetření: Implementace nástroje Mimecast Content Control and Data Leak Prevention, školení zaměstnanců ohledně kontroly odesílaných e-mailů, zakázky pro konkurenční klienty musí zpracovávat různé týmy.
Reakce: Při odeslání citlivých dat, které nástroj Mimecast nezachytí, uživatel neprodleně kontaktuje příjemce s žádostí o smazání přijaté zprávy. V případě splnění podmínek v článku č. 33 nařízení o GDPR provede právní oddělení do 72 hodin od nahlášení kontaktování dozorového úřadu – Úřadu pro ochranu osobních údajů. (22)

Špatné nastavení přístupových práv

Příčina: Přístupnost neoprávněných uživatelů k citlivým datům či datům konkurenčního klienta.
Dopad: Získání neoprávněné výhody pro konkurenčního klienta, kompromitace interních dokumentů.
Ošetření: Vytvoření šablony nového uživatele v Active Directory s přístupy pouze k všeobecně sdíleným souborům, přidělování dalších přístupů pouze po písemném potvrzení od nadřízeného, team leader při předávání klientů informuje IT oddělení s žádostí o odebrání přístupů stávajícímu týmu.

Reakce: IT support provede odebrání přístupů. V případě splnění podmínek v článku č. 33 nařízení o GDPR provede právní oddělení do 72 hodin od nahlášení kontaktování dozorového úřadu – Úřadu pro ochranu osobních údajů.

4.3.3 Podvratná činnost

Krádež dat zaměstnancem

Příčina: Krádež dat a informací zaměstnancem podniku
Dopad: Poškození reputace podniku, finanční škody
Ošetření: HR oddělení se snaží o vytváření příjemného pracovního prostředí, zajištění dostatečného platového ohodnocení a vhodných benefitů pro zaměstnance, IT oddělení se stará o přidělení minimálních potřebných přístupových práv zaměstnancům. IT oddělení nastaví v group policies automatické uzamčení uživatelského účtu po 5 minutách nečinnosti.
Reakce: CEO napíše omluvný dopis klientům a dodavatelům. Právní oddělení podá trestní oznámení Policii ČR a v případě splnění podmínek v článku č. 33 nařízení o GDPR provede právní oddělení do 72 hodin od nahlášení kontaktování dozorového úřadu – Úřadu pro ochranu osobních údajů. Při zjištění viníka na něj podá žalobu o náhradu vzniklé škody. HR oddělení připraví výpověď zaměstnance pro hrubé porušení pracovní kázně.

Krádež pracovní stanice / mobilního telefonu cizí osobou

Příčina: Krádež pracovní stanice nebo z prostor kanceláří cizí osobou.
Dopad: Znemožnění práce zaměstnance, ztráta dat na zařízení, možnost úniku citlivých dat.
Ošetření: Šifrování interního disku, použití hesla pro přístup do BIOS, správa pracovních stanic pomocí SCCM, interní směrnice nařizující ukládání pracovních dat na síťové nebo cloudové úložiště, interní směrnice nařizující ukládání zařízení do uzamykatelného šuplíku nebo uzamčení fyzickým zámkem, náhradní pracovní stanice dostupná v IT oddělení, školení zaměstnanců o nutnosti okamžitého nahlášení zcizení zařízení, vybavení vstupů do kanceláří kováním typu koule a přístupem na čipovou kartu, evidence čipových karet zaměstnanců v oddělení office managementu, evidence návštěvníků na recepci, vybavení kancelářských prostor kamerovým systémem se záznamem a detekcí pohybu.
Reakce: IT support vymaže data ze stanice pomocí SCCM a poskytne uživateli náhradní zařízení. IT ředitel objedná novou pracovní stanici. Finanční oddělení vyčíslí škodu. Při

krádeži z prostor kanceláří office manažer s liniovým nadřízeným zkontroluje, zda bylo zařízení zabezpečeno v souladu se směrnicí a zjistí časové rozmezí, kdy proběhla krádež. IT support prohledá záznamy z kamer. Při identifikaci podezřelých předá záznamy právnímu oddělení. Právní oddělení podá trestní oznámení na neznámého pachatele a předá kamerové záznamy Policii ČR. Při nedodržení směrnic o zabezpečení zařízení dohodne manažer oddělení se zaměstnancem náhradu způsobené škody

Krádež pracovní stanice / mobilního telefonu zaměstnancem

Příčina: Krádež zařízení zaměstnancem z prostor kanceláří nebo nenavrácení zařízení při ukončení pracovního poměru.
Dopad: Znemožnění práce postiženého zaměstnance, ztráta dat na zařízení, možnost úniku citlivých informací.
Ošetření: Šifrování interního disku, použití hesla pro přístup do BIOS, správa pracovních stanic pomocí SCCM, interní směrnice nařizující ukládání pracovních dat na síťové nebo cloudové úložiště, interní směrnice nařizující ukládání zařízení do uzamykatelného šuplíku nebo uzamčení fyzickým zámkem, náhradní pracovní stanice dostupná v IT oddělení, školení zaměstnanců o nutnosti okamžitého nahlášení zcizení zařízení, vybavení kancelářských prostor kamerovým systémem se záznamem a detekcí pohybu, IT support při onboardingu podepisuje s novým zaměstnancem předávací protokol, při každé změně IT support a zaměstnanec podepisují dodatek k předávacímu protokolu. Při ukončení pracovního poměru obdrží zaměstnanec v HR oddělení dokumenty, které IT support potvrdí při převzetí zařízení vydaných zaměstnanci (proběhne kontrola oproti předávacímu protokolu).
Reakce: IT support vymaže data ze stanice pomocí SCCM a poskytne uživateli náhradní zařízení. IT ředitel objedná novou pracovní stanici. Finanční oddělení vyčíslí škodu. Při krádeži z prostor kanceláří office manažer s liniovým nadřízeným zkontroluje, zda bylo zařízení zabezpečeno v souladu se směrnicí a zjistí časové rozmezí, kdy proběhla krádež. Office manažer dodá IT oddělení výpis použití přístupových karet. IT support prohledá záznamy z kamer. Při identifikaci podezřelého předá záznamy právnímu oddělení. Právní oddělení v součinnosti s HR oddělením kontaktuje podezřelého s žádostí o podání vysvětlení. Pokud se podezřelý nepřizná a nevrátí ukradená zařízení, kontaktuje právní oddělení Policii ČR. HR oddělení připraví listiny pro ukončení pracovního poměru z důvodu hrubého porušení pracovní kázně. Při nedodržení směrnic o zabezpečení zařízení

dohodne manažer oddělení se zaměstnancem náhradu způsobené škody. Nepředá-li odcházející zaměstnanec mzdové účetní potvrzený dokument o navrácení zapůjčených zařízení, nejsou mu vydány výstupní listiny a HR oddělení ho kontaktuje kvůli nápravě. Pokud na toto nereaguje, právní oddělení ho kontaktuje s předžalobní výzvou. Když přesto zaměstnanec nevrátí zařízení, podává právní oddělení trestní oznámení Policii ČR.

Cracking

Příčina: Prolomení hesla uživatele.
Dopad: Přístup neoprávněné osoby do systému, zcizení firemních dat, ztráta uložených dat, instalace podvodného softwaru do zařízení.
Ošetření: Uživatelé nemají přidělena administrátorská oprávnění, uživatelé mají nastavena minimální přístupová práva. Je nastavena doba platnosti hesla, jsou určeny podmínky zadání hesla (minimální počet znaků, minimální počet skupin znaků, jsou zakázána nejčastěji používaná hesla, použití jména a příjmení).
Reakce: IT support provede změnu hesla uživatele a obnoví data smazaná ze síťového úložiště. CEO napíše omluvný dopis klientům a dodavatelům. Právní oddělení podá trestní oznámení Policii ČR a v případě splnění podmínek v článku č. 33 nařízení o GDPR provede právní oddělení do 72 hodin od nahlášení kontaktování dozorového úřadu – Úřadu pro ochranu osobních údajů. Při zjištění viníka na něj podá žalobu o náhradu vzniklé škody.

Malware

Příčina: Instalace podvodného softwaru do zařízení
Dopad: Zpomalení zařízení, kompromitace či ztráta dat, kompromitace přihlašovacích údajů, ohrožení ostatních zařízení v síti.
Ošetření: Aktualizace operačních systémů pracovních stanic na aktuální verzi, vynucení automatických aktualizací operačního systému, ovladačů zařízení a antivirového softwaru (Windows Defender pro zařízení s operačním systémem Windows a Eset Endpoint security pro zařízení s operačním systémem macOS) v Group Policies. Implementace nástroje Cisco Umbrella a doplňku Microsoft Outlook Junk Reporting. IT oddělení připraví školení pro zaměstnance, jak rozpoznat rizikový e-mail, pokus o phishing a spam a jak reagovat, pokud taková zpráva dorazí. IT oddělení provádí pravidelné skeny pracovních stanic.

Reakce: Uživatel odpojí pracovní stanici od LAN. IT support neprodleně spustí antimalware kontrolu a následně kompletní scan počítače antivirovým programem. IT oddělení přikáže uživateli počítače změnu hesla. Při poškození systémových souborů provede reinstalaci.

Phishing

Příčina: Krádež citlivých údajů pomocí sociálního inženýrství.
Dopad: Kompromitace citlivých údajů, jako jsou přihlašovací jména, hesla nebo údaje k bankovním účtům.
Ošetření: Implementace nástroje Mimecast Content Control and Data Leak Prevention. IT oddělení připraví školení pro zaměstnance, jak rozpoznat rizikový e-mail, pokus o phishing a spam a jak reagovat, pokud taková zpráva dorazí, a implementuje do GPO instalaci doplňku Microsoft Oultook Junk Reporting. Při školení je apelováno na zaměstnance, aby raději nahlásili vše byť jen mírně podezřelé. Nově nastupující zaměstnanci dostanou školení o phishingu během onboardingové prezentace. IT oddělení bude pravidelně provádět testování reakcí uživatelů pomocí simulovaných phishingových e-mailů a dedikuje pracovní stanici (nezařazenou do domény) pro testování potenciálně nebezpečných zpráv. V GPO je nařízena změna hesla po uplynutí určité lhůty.
Reakce: IT support informuje zaměstnance o probíhajícím phishingovém útoku a nahraje do nástroje Mimecast předmětnou zprávu. Při nahlášení podezřelé zprávy provede IT support kontrolu pomocí nástroje Office 365 Advanced Threat Protection. Uživatelské účty, u nichž je podezření kompromitace, jsou dočasně uzamčeny a uživatelům je vynucena změna přihlašovacího hesla.

Krádež dat cizí osobou

Příčina: Krádež dat a/nebo informací při krádeži / ztrátě zařízení či při počítačovém útoku.
Dopad: Poškození reputace podniku, finanční škody.
Ošetření: Opatření vypsaná v kapitolách Krádež / Ztráta zařízení, Malware a Phishing.
Reakce: CEO napíše omluvný dopis klientům a dodavatelům. Právní oddělení podá trestní oznámení Policii ČR a v případě splnění podmínek v článku č. 33 nařízení o GDPR provede právní oddělení do 72 hodin od nahlášení kontaktování dozorového úřadu – Úřadu pro ochranu osobních údajů. Při zjištění viníka na něj podá žalobu o náhradu vzniklé škody.

Spamování

Příčina: Doručování nevyžádané pošty do e-mailové schránky uživatele.
Dopad: Snížení produktivity uživatele, riziko stažení malwaru do zařízení.
Ošetření: Implementace nástroje Mimecast Content Control and Data Leak Prevention. IT oddělení připraví školení pro zaměstnance, jak rozpoznat rizikový e-mail, pokus o phishing a spam a jak reagovat, pokud taková zpráva dorazí, a implementuje do GPO instalaci doplňku Microsoft Oultook Junk Reporting. Nově nastupující zaměstnanci dostanou školení o spamu během onboardingové prezentace.
Reakce: IT support informuje zaměstnance o probíhajících spamových útocích a nahraje do nástroje Mimecast předmětnou zprávu, která pronikla spamovým filtrem. Jestliže některý ze zaměstnanců otevřel spamovou zprávu, spustí IT support komplexní kontrolu v antivirovém programu Microsoft Defender (pro uživatele zařízení s operačním systémem Windows) nebo v programu Eset Endpoint security (pro uživatele zařízení s operačním systémem macOS).

DDoS útok

Příčina: Útok na DNS server podniku jeho zahlcením nepotřebným provozem.
Dopad: Nedostupnost internetového připojení pro uživatele.
Ošetření: ISP v rámci služeb poskytovaných podniku řeší filtraci škodlivého provozu. IT oddělení nakonfiguruje firewall pro blokování nevyužívaných portů. DNS–UDP port je nastaven pro zahození žádostí při UDP záplavě, které nejsou validními DNS dotazy. Systém vyžaduje autentifikaci žádosti pro eliminaci podvržených DNS útoků. Datová linka od ISP je naddimenzována.
Reakce: Při detekovaném útoku je spuštěno vyžadování platné FQDN a nastavení limitu žádostí od FQDN.

Poškození vybavení serverovny

Příčina: Cílené poškození síťových prvků.
Dopad: Nedostupnost internetového připojení, síťových disků, telefonního spojení a nefunkčnost kamerového systému.
Ošetření: Síťové prvky jsou umístěny v samostatné místnosti k tomu určené. Serverovna je vybavena kováním typu koule a zámkem na čipovou kartu. Přístup do serverovny mají pouze zaměstnanci IT oddělení. Serverovna je zabírána kamerou s nonstop záznamem.

Reakce: Právní oddělení kontaktuje Polici ČR a podá trestní oznámení. IT manažer kontaktuje dodavatele poškozených prvků a zajistí jejich výměnu. V případě, že není IT manažer přítomen, kontaktuje IT support IT manažera clusteru nadřízené společnosti, který zajistí kontakt s dodavateli. Po výměně poškozených prvků IT oddělení provede konfiguraci dle dokumentace. IT support provede kontrolu kamerových záznamů. Relevantní záběry předá právnímu oddělení, které je poskytne Polici ČR.

5 Zhodnocení výsledků

Výsledkem této práce je registr rizik hrozících IT zdrojům zkoumaného podniku a návrh opatření pro jejich kontrolu v souladu s interními směrnicemi nadřízené společnosti. Uvedení těchto opatření do praxe je spojeno s jistou mírou zátěže pro firmu. Zavedení řádného risk managementu bude v první řadě vyžadovat investice do vybavení nových kancelářských prostor síťovými prvky a do jejich zabezpečení. Odhadovaná suma by se mohla pohybovat v řádech milionů korun. Výše částky je částečně dána podmínkami na vybavení serverovny určenými nadřízenou společností. Dále bude IT oddělení muset implementovat řadu softwarových nástrojů a aktualizovat všechna zařízení na aktuální stabilní verzi operačních systémů – Windows 10 verze 1903, jde-li o zařízení s operačním zařízením Microsoft Windows, a macOS 10.15 Catalina v případě zařízení od společnosti Apple, což bude znamenat značnou časovou zátěž, jelikož se jedná o zhruba 120 zařízení. Kromě toho bude nutné proškolit všechny zaměstnance v rozpoznávání malwaru, phishingu a spamu a reagování na ně.

Předmětný podnik je kriticky závislý na funkčnosti internetového připojení a počítačové sítě. Investice do jeho ochrany jsou proto vzhledem k množství hrozeb a zranitelnosti zdrojů podniku nutné. Navržená opatření jsou vhodná též pro obdobné podniky, jejichž fungování je silně závislé na informačních a komunikačních technologiích. Pro podniky, u nichž práce přes internet a na počítačích nepředstavuje jediný nebo hlavní zdroj příjmů, je možné použít infrastrukturu méně náročnou na zdroje. IT manažer předmětného podniku s navrženými opatřeními většinou souhlasí, doporučil doplnění Bussiness continuation plánu. Kromě realizace navržených opatření bude pro úspěšné fungování risk managementu v podniku zapotřebí zavést ještě pravidelnou revizi zdrojů, rizik a jejich ošetření.

6 Závěr

Na počátku své práce jsem na základě odborné literatury vymezil pojem riziko, stanovil, jaká rizika rozlišujeme a jakými způsoby je ošetřujeme. Následně jsem provedl průzkum aktuálního stavu risk managementu ve zvoleném středně velkém podniku, který se zabývá reklamou.

Z výsledků výzkumu zaměřeného na risk management a incident response zkoumané firmy je zřejmé, že úroveň v současnosti nastavených opatření k eliminaci a nápravě rizik je zcela nedostatečná, neboť zde neprobíhají žádné procesy risk managementu. Podnik je vážně ohrožen úmyslným i neúmyslným lidským jednáním a selháním systémů, což by vzhledem k jeho kritické závislosti na funkčnosti internetového připojení a počítačové sítě vyústilo ve významné finanční ztráty. Za použití Delfské metody byl proto ve spolupráci s odborníky vytvořen registr rizik hrozících předmětnému podniku a za pomoci rámce ČSN ISO/IEC 27005 na možnosti ošetření rizik byla navržena opatření pro jejich zvládnutí na úroveň uspokojivého řešení. (1, str. 25) Návrh opatření pokrývá rizika přírodního původu, rizika hrozící díky lidským chybám, podvodnému lidskému chování i hrozby vyplývající ze selhání počítačové sítě.

Složitost zkoumané problematiky a neustále se měnící prostředí způsobuje, že nelze pouze jednou nastavit fixní opatření, ale zodpovědné osoby musí průběžně provádět pravidelné revize hrozeb i opatření pro jejich eliminaci.

7 Seznam použitých zdrojů

1. ČSN ISO/IEC 27005 (36 9790). Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací. Praha : Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2019.

2. Kyberkriminalita. *Policie České Republiky.* [Online] Policie České Republiky. [Citace: 3. Únor 2019]. Dostupné z https://www.policie.cz/clanek/kyberkriminalita.aspx.

3. Advanced Threat Analytics. *Microsoft.* [Online] Microsoft. [Citace: 10. Únor 2019.] Dostupné z https://www.microsoft.com/en–us/cloud–platform/advanced–threat–analytics.

4. *ČSN ISO/IEC* 27001 *(36 979).* Informační *technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky*. Praha : Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013.

5. MASLOW, Abraham Harold. A theory of human motivation. *Psychological Review.* 1943, Sv. 4, 50.

6. PURPURA, Philip. *Security: An Introduction.* Boca Raton : CRC Press, 2010. ISBN 14–20092–83–9.

7. HARRIS, Shon a MAYMI, Fernando. *CISSP All–in–One Exam Guide.* New York : McGraw–Hill Education, 2016. ISBN 00–71849–27–0.

8. *ČSN ISO 31000 (01 0351). Management rizik – Směrnice.* Praha : Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2017.

9. ISO – Standards. *ISO – Standards.* [Online] International Organization for Standardization. [Citace: 28. září 2019.] Dostupné z https://www.iso.org/standards.html.

10. MERNA, Tony a AL–THANI, Faisal. *Corporate risk management.* New Jersey : John Wiley & Sons Ltd., 2008. ISBN 04–70518–33–2.

11. LOCH, Christoph H., DEMEYER, Arnoud a PICH, Michael. *Managing the Unknown: A New Approach to Managing High Uncertainty and Risk in Projects.* New Jersey : John Wiley & Sons Ltd., 2006. ISBN 978–04–71–69305–5.

12. MCNEIL, Alexander John. *ResearchGate.* [Online] 17. Květen 1999. [Citace: 3. Říjen 2019.] Dostupné z https://www.researchgate.net/publication/2470539_Extreme_Value_Theory_for_Risk_Managers.

13. HOPKIN, Paul. *Fundamentals of Risk Management.* London : Kogan Page, 2017. ISBN 07–49479–62–0.

14. MOELLER, Robert R. *COSO Enterprise Risk Management: Understanding the New Integrated ERM Framework.* New Jersey : John Wiley & Sons, 2007. ISBN 04–70912–88–X.

15. *Institute of Risk Management.* [Online] [Citace: 4. Únor 2019.] Dostupné z https://www.theirm.org/knowledge–and–resources/risk–management–standards/.

16. LARK, John. *ISO 31000: Risk Management. A practical guide for SMEs.* Geneva : ISO, 2015. ISBN 978–92–67–10645–8.

17. BURNS–HOWELL, Tony, CORDIER, Pierre a ERIKSSON, Therese. *Security Risk Assessment and Control.* London : Palgrave Macmillan, 2003. ISBN 978–18–99–28766–6.

18. REJDA, George E. a MCNAMARA, Michael J. *Principles of Risk Management and Insurance, 13th edition.* London : Pearson Education Limited, 2017. ISBN 978–12–92–15103–8.

19. DORFMAN, Mark S. a CATHER, David. *Instructor's Resource Manual for Introduction to Risk Managment and Insurance.* London : Pearson, 2013. ISBN 978–01–31–39414–8.

20. *ČSN EN 62040–1 (36 9066). Zdroje nepřerušovaného napájení (UPS) – Část 1: Všeobecné a bezpečnostní požadavky pro UPS.* Praha : Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2009.

21. Přepětí – Elektrika.cz. *Elektrika.cz.* [Online] [Citace: 15. Říjen 2019.] Dostupné z https://elektrika.cz/terminolog/eterminologitem.2005–05–23.7953032978.

22. GDPR (Obecné nařízení): Úřad pro ochranu osobních údajů. *Úřad pro ochranu osobních údajů.* [Online] [Citace: 12. Listopad 2019.] Dostupné z https://www.uoou.cz/gdpr/ds–3938/p1=3938.

8 Přílohy

Výsledný registr rizik

Hrozba	Dopad	Pravděpodobnost	Závažnost
Přírodní neštěstí			
Požár			
Systémové hrozby			
Přerušení přívodu elektrického proudu			
Ochrana proti přepětí			
Disfunkce síťového připojení (k ISP)			
Disfunkce firewallu			
Disfunkce core switche			
Disfunkce L2 switche			
Disfunkce síťového úložiště			
Disfunkce LAN sítě			
Disfunkce WiFi sítě			
Disfunkce pracovní stanice			
Disfunkce telefoní ústředny			
Disfunkce SQL serveru			
Porucha silového rozvodu			
Náhodné lidské chyby			
Poškození pracovní stanice			
Ztráta pracovní stanice			
Ztráta mobilního telefonu			
Náhodné smazání souboru			
Odeslání dat nesprávnému příjemci			
Špatné nastavení přístupových práv			
Podvratná činnost			
Krádež dat zaměstnancem			
Krádež pracovní stanice/mobilního telefonu cizí osobou			
Krádež pracovní stanice/mobilního telefonu zaměstnancem			
Cracking			
Malware			
Phishing			
Krádež dat cizí osobou			
Spamování			
DDoS			
Poškození vybavení serverovny			

	Kritický dopad	Jistá událost	Nepřijatelné riziko
	Velmi významný dopad	Očekávaná událost	Značné riziko
	Významný dopad	Pravděpodobná událost	Mírné riziko
	Nízký dopad	Nejistá událost	Přijatelné riziko
	Velmi nízký dopad	Nepravděpodobná událost	Zanedbatelné riziko