VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
FACULTY OF INFORMATION TECHNOLOGY

ÚSTAV INTELIGENTNÍCH SYSTÉMŮ
DEPARTMENT OF INTELLIGENT SYSTEMS

ŘÍZENÍ BEZPEČNOSTI V MALÝCH A STŘEDNÍCH PODNICÍCH

ITSM IN SMALL AND MEDIUM-SIZED ENTERPRISES

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE **VOJTĚCH OLEJ**
AUTHOR

VEDOUCÍ PRÁCE **Mgr. KAMIL MALINKA, Ph.D.**
SUPERVISOR

BRNO 2021

Vysoké učení technické v Brně
Fakulta informačních technologií

Ústav inteligentních systémů (UITS) Akademický rok 2021/2022

Zadání bakalářské práce

Student: **Olej Vojtěch**
Program: Informační technologie
Název: **Řízení bezpečnosti v malých a středních podnicích**
ITSM in Small and Medium-Sized Enterprises
Kategorie: Bezpečnost

Zadání:

1. Nastudujte relevantní standardy pro řízení IT bezpečnosti (rodina standardů ISO 27001, rodina NIST SP 800 a další).
2. Nastudujte zákonné povinnosti, které firma má v souvislosti s IT.
3. Seznamte se s problematikou naplňování těchto povinností malými a středními podniky.
4. Navrhněte obecné postupy, které lze uplatnit při řízení bezpečnosti s ohledem na potřeby malých a středních podniků. Při sestavování postupů mějte na paměti i náklady, aby tyto postupy byly i cenově dostupné, ale zároveň naplňovaly požadovanou úroveň bezpečnosti.
5. Navržené postupy aplikujte ve vybraném v malém až středním podniku.
6. Zhodnoťte výsledek analýzy a kvalitu postupů.

Literatura:

- https://gcatoolkit.org/smallbusiness/

Pro udělení zápočtu za první semestr je požadováno:

- Body 1 až 3

Podrobné závazné pokyny pro vypracování práce viz https://www.fit.vut.cz/study/theses/

Vedoucí práce: **Malinka Kamil, Mgr., Ph.D.**
Vedoucí ústavu: Hanáček Petr, doc. Dr. Ing.
Datum zadání: 1. listopadu 2021
Datum odevzdání: 11. května 2022
Datum schválení: 3. listopadu 2021

Abstrakt

Bakalářská práce se zabývá sestavením vlastní metodiky pro řízení rizik na základě již existujících standardů, uplatnitelné v malých a středních podnicích v České republice. V teoretické části jsou analyzovány zákonné povinnosti, existující standardy a současná situace. Do praktické části se řadí návrh metodiky, nasazení ve vybrané firmě a zhodnocení použitelnosti.

Abstract

This bachelor thesis deals with the compilation of own methodology for risk management, which is based on existing standards, applicable in small and medium-sized enterprises in the Czech Republic. The theoretical part analyzes the legal obligations, existing standards and the current situation. The practical part includes the design of the methodology, deployment in the selected company and usability evaluation.

Klíčová slova

Analýza rizik, řízení rizik, bezpečnost IT, ISO 27001, IT bezpečnost

Keywords

Risk analysis, risk management, IT security, ISO 27001, IT security

Citace

OLEJ, Vojtěch. *Řízení bezpečnosti v malých a středních podnicích*. Brno, 2021. Bakalářská práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce Mgr. Kamil Malinka, Ph.D.

Řízení bezpečnosti v malých a středních podnicích

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně pod vedením Mgr.Kamila Malinky, Ph. D. Další informace mi poskytl Ing. Tomáš Nedbal. Uvedl jsem všechny literární prameny, publikace a další zdroje, ze kterých jsem čerpal.

.....
Vojtěch Olej
10. května 2022

Poděkování

Rád bych poděkoval Mgr. Kamilu Malinkovi, Ph.D. za jeho ochotu a čas na konzultace. Taktéž bych chtěl poděkovat panu Ing. Tomáši Nedbalovi za cenné rady.

Obsah

Kapitola 1

Úvod

Hlavním cílem této bakalářské práce je vytvoření jednoduché, přehledné, jasné a stručné metodiky řízení rizik IT pro malé a střední podniky v Česku. Metodika by měla obsahovat základní informace potřebné k zavedení řízení rizik v malém a středním podniku. Z osobní zkušenosti mi přijde řízení rizik jako důležitý prvek, obzvlášť pak co se IT týče, neboť jsem v praxi poznal, jaké dopady může mít riziko, které nebylo včas zjištěno a nebyly provedeny žádné akce ke snížení pravděpodobnosti přechodu v incident a zmírnění dopadů incidentu. Zároveň je však řízení rizik procesem, který by neměl ležet na bedrech pouze správce IT, ale i vedení podniku, a taktéž by při něm měli spolupracovat všechny dotčené strany.

Samotná bakalářská práce je členěna na dvě hlavní části. Úkolem první je především analyzovat současnou situaci z teoretického hlediska. První kapitolou této sekce je přehled povinností pro firmy v rámci IT, které vyplývají ze zákona. V druhé kapitole popisuji standardy a návody pro řízení rizik. Největší pozornosti se dostalo návodu Queenslandské vlády a dokumentům Mozilla Foundation, které považuji za přehledné, ucelené a zároveň v dosti ohledech jednoduché, aby se částečně v nějaké podobě daly uplatnit v rámci malých a středních firem v Česku. Poslední kapitolou této části je analýza současné situace v malých a středních podnicích, tedy úrovně bezpečnosti IT, přístupu k řízení rizik a naplňování zákonných povinností.

Na základě první části pak vznikala část druhá, která již přináší vlastní návrh metodiky procesu řízení rizik. Při návrhu příručky jsem vycházel z nastudovaných materiálů a z praktické znalosti a součástí je i například motivační část, která slouží k vysvětlení důležitosti procesu řízení rizik spojeného s IT ve firmě. Poslední kapitolou práce je popis procesu praktického nasazení ve vybrané firmě a vyhodnocení kvality metodiky a postupů.

Kapitola 2

Zákonné povinnosti

Pro správné pochopení situace je třeba si prvně stanovit povinnosti v oblasti bezpečnost IT infrastruktury, které pro firmy působící v České republice vyplývají ze zákona.

2.1 Zákon o kybernetické bezpečnosti

V roce 2014 přijala Česká republika zákon o kybernetické bezpečnosti na základě předpisů Evropské unie.[17] Srozumitelně jej popisuje sekce FAQ (často kladených otázek) na webu Národního úřadu pro kybernetickou bezpečnost. [13] Tento zákon se však nevztahuje na všechny občany a instituce v České republice, nýbrž pouze na subjekty, které jsou stanoveny v § 3.

U subjektů, které tyto kritéria splňují, pak dojde k jejich určení na základě jednání s Národním úřadem pro kybernetickou a informační bezpečnost (dále jen Úřadem). Za jejich identifikaci odpovídají správci těchto systémů. Vzhledem k tomu, že zákon přímo stanovuje povinné subjekty, týká se nejen státní správy, nýbrž i soukromých společností, které splňují podmínky uvedené v § 3.

Ze zákona pro subjekty jím dotčené plynou povinnosti, jako například nahlásit Úřadu kontaktní údaje podle § 16, aplikovat bezpečnostní opatření podle § 4 odst. 1 a v souladu s vyhláškou č. 82/2018 Sb. vést o těchto opatřeních dokumentaci. Dále tyto subjekty musí úřadu hlásit bezpečnostní incidenty podle § 8 a provádět opatření podle § 11, jsou-li vydána.

Ačkoliv tedy ze znění vyplývá, že tento zákon nedopadá na všechny firmy a pravděpodobně se většiny malých a středních firem týkat nebude, je třeba jej brát v potaz, neboť firmy dotčené tímto zákonem jsou povinny zavést bezpečnostní opatření minimálně v zákonem a vyhláškou stanoveném rozsahu.

2.2 Směrnice GDPR

Obecné nařízení o ochraně osobních údajů, známé spíše pod anglickou zkratkou GDPR (General Data Protection Regulation), je rámec právní ochrany osobních údajů platný pro všechny subjekty, které shromažďují nebo zpracovávají osobní údaje Evropanů, a to včetně společností působících mimo Evropskou Unii, které působí na evropském trhu. [3]

Součástí směrnice je stanovení několika důležitých pojmů. Správce osobních údajů je subjekt, který určuje způsob a účel zpracování osobních údajů. Dále je odpovědný za jejich shromažďování, zpracování a uchovávání. Zpracovatelem je myšlen subjekt, který zpracovává

údaje pro správce osobních údajů. Posledním důležitým pojmem je pak subjekt údajů, což je fyzická osoba, jejíž údaje jsou zpracovávány.

Osobní údaje definuje GDPR jako veškeré informace vztahující se k identifikované nebo identifikovatelné osobě. Mezi obecné osobní údaje patří jméno a příjmení, pohlaví, věk a datum narození, osobní stav, IP adresa a fotografický záznam. Dále se k obecným osobním údajům řadí e-mailová adresa, telefonní číslo a různé identifikační údaje vydané státem.

Kategorie zvláštních osobních údajů zahrnuje například údaje o rasovém či etnickém původu, politických názorech, náboženském vyznání, zdravotním stavu či trestním rejstříku. Dále pak stanovuje kategorie genetických údajů (genetické znaky, které vyplývají např. z analýzy biologického vzorku), údaje o zdravotním stavu a biometrické údaje (otisky prstů, snímky obličeje nebo podpis).

Veškeré osobní údaje jsou správce a zpracovatel osobních údajů povinni chránit před neoprávněným přístupem. Výjimku tvoří údaje anonymizované, údaje zesnulých a údaje získané v rámci činnosti čistě osobní povahy, které nemají obchodní či institucionální charakter.

V rámci analýzy je tedy třeba umět správně identifikovat osobní údaje ukládané a zpracovávané v rámci IT a v součinnosti s firmou zajistit, aby se k nim dostaly pouze povolané osoby. Z GDPR dále vyplývá, že je vhodné data šifrovat jako ochranu v případě úniku dat.

2.3 Legálnost software

Ačkoliv legálnost software spadá spíše do kategorie správy softwarových aktiv (software asset management), je třeba mít alespoň základní povědomí o tom, co je legální a co nelegální využití software, neboť možnost nelegálního použití software může být jedním z rizik. Navíc je třeba počítat s tím, že obecný postup navržený v další části této práce je určen pro malé a střední podniky a tedy že analýzu rizik bude nejspíš vykonávat stejná osoba, jako správu IT a správu softwarových aktiv.

Účelem autorského zákona [16] je především poskytnout ochranu výsledkům jedinečné, tvůrčí činnosti autora. Dle § 65, odst. 1 tohoto zákona je počítačový program, bez ohledu na formu jeho vyjádření, chráněn jako literární dílo.

Ze znění zákona vyplývá, že nelegální software je nejen takový, který nebyl nabyt legální cestou, ale i software, který je použit v nesouladu s licenční smlouvou. Příkladem takového porušení může být například zakoupení licence programu pro použití na jedné stanici a jeho následné využití na vícero počítačích.

Rizika, která z použití nelegálního software plynou, jsou poměrně závažná. Krom toho, že se může autor programu bránit soudní cestou, hrozí i riziko postihu ze strany finančního úřadu, neboť se může jednat o daňový únik, protože dle finanční správy se náklady na hardware bez legálního software stávají daňově neuznatelnými [6].

Kapitola 3

Standardy a návody pro řízení rizik

V dnešní době existuje množství různých návodů, manuálů a standardů pro řízení rizik, a to nejen v IT. Cílem této kapitoly je seznámit se s těmito již hotovými postupy a zjistit, v jaké míře jsou aplikovatelné na malé a střední podniky.

3.1 Business Queensland Risk Management

Jedním ze zdrojů, ze kterých lze čerpat, je přehledný návod Queenslandské vlády v oblasti řízení rizik pro firmy. [4] Řízení rizik v IT je pouze jednou kapitolou tohoto materiálu, nicméně jde o ucelený a přehledný návod, jak postupovat.

3.1.1 Definice hrozeb

Na začátku je třeba si definovat obecné IT hrozby, jako například selhání hardware nebo software (výpadek energie, poškození dat), počítačové viry, spam, podvody a phishing (postup, při kterém jsou získány citlivá data od uživatelů na základě jejich důvěry) a lidskou chybu (špatné zpracování dat, neopatrné smazání dat, otevření infikované přílohy mailu).

Další kategorií hrozeb jsou kriminální IT hrozby, mezi které spadají hackeři (lidé nelegálně se vloupající do systému), podvodníci (používají počítače k úpravě dat za účelem vlastního zisku), DoS útok (z anglického „denial of services“, neboli nedostupnost služby), narušení bezpečnosti (online i fyzické vloupání) a neupřímnost zaměstnanců (krádež dat nebo vynesení citlivých informací).

Poslední definovanou hrozbou jsou přírodní katastrofy, jako například povodně, požáry, bouře aj., které taktéž mohou poškodit hardware a vést ke ztrátě nebo poškození dat.

3.1.2 Řízení rizik

Analýza rizik je sérií strukturovaných kroků, které vedou k jejich identifikování, posouzení, zmírnění, vytvoření reakčních plánů a přezkoumání postupů jejich řízení. Dále se pak dočteme, že správce, který má řídit rizika v IT, by měl mít povědomí o aktuálních zákonech a vyhláškách.

Na stránkách je zmíněn i tzv. „Business continuity planning“, neboli plánování kontinuity podnikání, což je postup vytváření praktických plánů, jak se může podnik připravit na jednotlivé problémy a jak pokračovat v práci i přes nastalou krizi. Postup zahrnuje identifikaci a redukování rizik, přípravu na rizika, která nelze ovládat a plánování postupu na obnovení chodu v případě incidentu nebo problému.

Mezi řízení rizik se řadí například i stanovení a dodržování zásad IT, které by měly zaměstnancům vysvětlovat důležitost řízení rizik v IT a zapojit je do něj. Mezi zásady IT patří například bezpečné používání mailové komunikace, nastavení procesů na běžné úlohy, řízení změn v IT systémech a reakce na IT incidenty. Správně sepsaný kodex chování by měl zaměstnancům stanovit jasný směr a definovat přípustné chování ve vztahu k IT problémům a určit postupy pro krizové situace.

3.1.3 Snižování rizik

Pro zvýšení ochrany IT systémů a dat návod uvádí kroky, jako například zabezpečení počítačů, serverů a bezdrátových sítí, použití antiviru a firewallu, aktualizace software, zálohování dat na vzdálené úložiště, zabezpečení hesel, školení personálu v otázce zásad IT a pochopení zákonných povinností v případě online podniků.

Pokud se například podnik prezentuje i v online světě, mělo by dojít k zabezpečení webových stránek, mailových účtů, internetového bankovnictví a profilů na sociálních sítích, například použitím šifrovaného spojení pomocí technologie SSL.

Návod dále uvádí sjednání pojištění jako jednu z možností, jak snížit dopady případných problémů, neboť není možné se všem rizikům vyhnout. Je třeba pravidelně přezkoumávat smlouvu o pojištění a zajistit si změnu v případě vyvstání nových rizik, jako například používání osobních mobilních telefonů pro pracovní aktivity.

3.1.4 Reakce na incident

Správná odpověď na incidenty určuje, jak dobře a rychle se podnik zotaví a taktéž ovlivňuje názory zákazníků na spolehlivost podniku. Mezi incidenty může patřit například DoS útok, ale také i výpadek sítě v souvislosti s živelnou pohromou. Z tohoto důvodu by měl existovat plán řízení rizik a plán kontinuity podnikání obsahující plány pro reakci na IT incident, plány krizové reakce a plány obnovy.

Plán reakcí pro IT incidenty slouží k identifikaci rizik v IT a kroků ke snížení účinků nebo škod. Mohou zahrnovat například odpovědné osoby, které by měly být v případě problému kontaktovány, prioritní akce, komunikační plány, seznam kontaktů a záznam událostí k zápisu vykonaných akcí.

IT incident může být způsoben větším problémem, například požárem, explozí nebo povodní. V každém případě by měla být prioritní bezpečnost zaměstnanců a veřejnosti. Plán reakcí pro IT incidenty by měl být součástí plánu krizové reakce.

Plán obnovy by měl vést k efektivní reakci na IT incident nebo krizi, která podnik ovlivňuje. Správné stanovení tohoto plánu snižuje čas, potřebný pro obnovení chodu firmy, a také ztráty. Měl by obsahovat strategii na obnovení chodu firmy v nejkratším čase, popis klíčových zdrojů, vybavení a zaměstnanců, které jsou potřeba pro obnovení chodu a časové cíle.

3.1.5 Shrnutí

Ačkoliv je web přehledný a poskytuje spoustu užitečných informací, ať už o řízení rizik v IT nebo o řízení rizik obecně, je psaný v angličtině, a tedy může být pro část správců IT v ČR nedostupný. Navíc je do značné míry třeba jej brát obecně, protože v legislativní části se může značně lišit a je třeba si dohledat další zdroje. Dle mého názoru je však možné z něj ve spoustě věcí vycházet a může se jednat o dobrý výchozí bod pro vytvoření obecného postupu řízení rizik pro malé a střední podniky. V závěru části o řízení rizik IT

navíc obsahuje zajímavý kontrolní seznam, který čtenáři přehledně pomáhá se zorientovat v tom, které kroky by měl ve firmě aplikovat.

3.2 Standard ČSN ISO

Mezinárodní organizace pro normalizaci, známější spíše pod názvem ISO (International Organization for Standardization), je světová federace národních normalizačních organizací. Jejím cílem je tvorba mezinárodních norem. Jednou z těchto norem je i řada norem ISO 27000 (v české verzi ČSN EN ISO/IEC 27000) zabývajících se systémy řízení bezpečnosti informací.

3.2.1 ISO 27000

Vzhledem ke složitosti problematiky je třeba si na začátku správně definovat termíny a vymezit pojmy. K tomu v případě výše uvedené řady norem slouží norma ISO 27000[15]. Ta, vyjma slovníku pojmů, obsahuje i definici „systému řízení bezpečnosti rizik“.

Obecně norma uvádí, že každá organizace bez ohledu na velikost a typ shromažďuje informace a pracuje s nimi. Dále říká, že informace a vše s nimi související jsou aktiva důležitá k dosažení cílů a taktéž že všechny organizace čelí řadě rizik, která mohou ovlivnit fungování aktiv.

Důležitou informací je, že krom útoků jsou informace ohroženy například chybou či přírodními vlivy a taktéž jsou vystaveny zranitelnostem, které vznikají při jejich používání. Termín bezpečnost informací je postaven na informacích majících hodnotu, kterou je třeba chránit. Dle normy je důležitým prvkem činnosti organizace dostupnost přesných a úplných informací pro oprávněné pracovníky v požadovaném čase.

Jak norma uvádí, rizika bezpečnosti informací a účinnost opatření se s časem mění a je třeba neustále hledat možná nová rizika, vyhodnocovat aktuální bezpečnostní opatření a zavádět nová opatření. Aby celý proces probíhal koordinovaně a nevznikal chaos, je třeba, aby si organizace stanovila postupy, politiky a cíle k dosažení bezpečnosti informací a dosahovala jich pomocí systému řízení.

Dále norma zmiňuje existenci ISMS, neboli systému řízení bezpečnosti informací, který definuje jako sestavu politik, postupů, směrnic, příslušných zdrojů a činností řídící organizaci k zajištění ochrany informačních aktiv. Základem ISMS je posuzování rizik a jejich řízení. K úspěšné implementaci je mj. třeba mít povědomí o potřebě bezpečnosti informací, určit odpovědnost za tuto bezpečnost, aktivně předcházet incidentům a detekovat je a neustále vyhodnocovat bezpečnost informací a modifikovat procesy a opatření.

V závěru normy jsou pak přehledně uvedeny vztahy mezi normami ISMS. Mezi nejdůležitější patří norma ISO/IEC 27001, která popisuje požadavky ISMS bez ohledu na typ nebo velikost organizace.

3.2.2 ISO 27001

Jedná se o mezinárodní normu, jejímž cílem je poskytnutí požadavků na ustavení, implementaci, udržování a zlepšování systému řízení bezpečnosti informací.[14]

Dle normy je pro správnou implementaci standardu třeba porozumět organizaci a jejímu kontextu, potřebám a očekáváním zainteresovaných stran a stanovit rozsah systému řízení bezpečnosti informací, přičemž rozsah řízení bezpečnosti informací musí být dostupný jako dokumentovaná informace.

Do řízení bezpečnosti informací je dle standardu zapojena celá organizace. Úkolem vrcholového vedení je například zajistit stanovení politiky bezpečnosti informací, integraci požadavků systému řízení bezpečnosti do procesů organizace a podpora ostatních relevantních řídících rolí. Dále musí zajistit stanovení politiky bezpečnosti informace, která je přiměřená záměrům organizace a která musí být dostupná jako dokumentovaná informace, komunikovaná v rámci organizace a přiměřeně dostupná zainteresovaným stranám.

Dalším z hlavních bodů je plánování. Organizace musí jednak plánovat opatření zaměřená na řízení rizik, jednak je i integrovat a implementovat do procesů systému řízení bezpečnosti informací a vyhodnocovat jejich efektivitu. Taktéž musí mít definovaný a aplikovaný proces posuzování rizik bezpečnosti informací, který stanovuje kritéria akceptace rizik a kritéria pro provádění posuzování rizik bezpečnosti informace, přičemž opakované posuzování rizik musí produkovat konzistentní, opodstatněné a porovnatelné výsledky. Analýza rizika nejen identifikuje, ale posuzuje i potenciální následky, pokud by došlo k jejich realizaci, a pravděpodobnost jejich výskytu.

Organizace je pro splnění standardu povinna definovat a používat proces ošetření rizik bezpečnosti informace s ohledem na výsledky analýzy rizik a porovnávat je s opatřeními v příloze normy, aby zajistila, že žádné nezbytné opatření nebylo vynecháno. K ošetření rizik taktéž potřebuje mít souhlas vlastníků rizik a případně přijmout zbytková rizika bezpečnosti informací.

Pro řízení rizik dle normy je taktéž třeba, aby organizace zajistila potřebné zdroje, stanovila kompetence osob (do které se řadí i odpovídající vzdělání, školení nebo zkušenosti), zajistila povědomí o politice bezpečnosti informací, přínosů a výhod zlepšené výkonnosti bezpečnosti informací a důsledků nepřizpůsobení se požadavkům systému řízení bezpečnosti informací.

Dále je třeba ve vztahu k systému řízení bezpečnosti stanovit komunikační procesy (kdo, kdy, o čem a s kým má komunikovat) a procesy, kterými musí být komunikace realizována, přičemž se nejedná pouze o komunikaci interní (mezi zaměstnanci), ale i externí (s partnery, dodavateli, technickou podporou, atd.).

Kromě již uvedeného monitorování, analýzy a vyhodnocování si norma klade jako další požadavek i interní audity, které by měly být prováděny v pravidelných intervalech a kontrolovat, zda systém řízení vyhovuje požadavkům organizace i normy a je efektivně implementován a udržován. Auditoři, kteří jej provádí, musí být objektivní a nestranní. Je nutno výsledky auditu dokumentovat a předat vedoucím pracovníkům. Vedení organizace pak i na základě těchto auditů musí přezkoumávat systém řízení bezpečnosti informací s ohledem na změny, které se udály, a hledat příležitosti neustálého zlepšování.

Poslední uvedenou povinností organizace je tedy výše zmíněné zlepšování. Do této kategorie se řadí přijetí nápravných opatření při neshodě, přičemž je třeba, aby byla neshoda přezkoumána a určena příčina neshody a možnosti výskytu podobné neshody. Neshody je třeba dokumentovat, včetně informací o přijetí opatření a jeho výsledcích.

3.2.3 Shrnutí

Norma ISO poskytuje kvalitní, robustní nástroj k řízení rizik informací ve firmách. Krom toho, že klade důraz na tvorbu plánů a analýz a jejich dokumentaci, tak staví na předpokladu, že do řízení rizik informací se zapojuje celá organizace a nikoliv jen IT oddělení nebo jeden správce IT. Díky své robustnosti a obecnosti je však dle mého v případě malých a středních firem příliš komplikovaná. Její komplexnost s sebou nese časovou složitost na porozumění a taktéž vyžaduje jistou dávku odbornosti pro její správnou implementaci. Myslím

si, že pro splnění cíle této bakalářské práce je tento standard dobrým studijním základem a materiálem, ze kterého lze čerpat, nicméně pro použití jako podkladu pro průměrného správce IT v malé až střední firmě je nevhodný. Je třeba najít cestu, která sice nebude tak robustní, ale bude jednodušší, pochopitelnější a snáze uplatnitelná pro průměrného správce IT v malé nebo střední firmě.

3.3 Mozilla Security Assurance and Security Operations

Mozilla Foundation je nezisková organizace známá veřejnosti především díky prohlížeči Mozilla Firefox nebo mailovému klientovi Mozilla Thunderbird. Krom této činnosti však provozuje i webovou stránku Infosec, která je zaměřena na poskytování informací o bezpečnosti pro „Mozziliany“ (členy komunity) k zajištění ochrany dat napříč organizací. Pro příklad lze uvést články „AWS Security“, zabývající se nejlepšími postupy pro bezpečné ovládání prostředí Amazon Web Services, či „Phishing“, poskytující návod pro uživatele k identifikaci phishingové zprávy a adekvátní reakci. Dále pak web obsahuje i informace k určování a řízení rizik.

3.3.1 Assessing Security Risk

Cílem těchto dokumentů je pomoc s pochopením, jak je využíván bezpečnostní rámec Security týmu Mozilly a taktéž k sestavení vlastního bezpečnostního rámce v případě, že oficiální standardy nejsou dostatečně felxibilní nebo jsou příliš složité na implementaci. Větší část rámce používaného Mozillou je inspirována standardy ISO 31000 (standard pro celkové řízení rizik) a ISO 27001.[7]

Dle článku je riziko běžně definováno jakou součin pravděpodobnosti, že nějaká situace nastane, a jejího důsledku v tom nejhorším případě. Určení dopadu je relativně přímočará činnost. Můžeme určit, kolik peněz můžeme ztratit, jak moc bude poškozena naše reputace, nakolik bude chod firmy ochromen aj. Dopady se většinou s časem příliš výrazně nemění, pokud nedojde k závratným změnám ve struktuře firmy nebo v její činnosti (např. nové stroje, rozšíření provozu, změna lokace). Při určování nejhorších dopadů je však třeba myslet realisticky a brát v potaz pouze rizika, která jsou reálná a smysluplná.

Pravděpodobnost je v článku definována jako frekvence (četnost), s jakou se mohou tyto dopady projevit. Oproti určování dopadů může být určení pravděpodobnosti složitější, neboť nelze přesně určit, jak často se někdo pokusí například zvenku zaútočit na infrastrukturu pomocí známých zranitelností. Navíc je pravděpodobnost značně proměnlivá a v čase se může měnit rychle. Denně jsou nalézány nové zranitelnosti a prostředí, ve kterých běží IT služby se taktéž vyvíjí a dochází ke změnám nastavení. Z tohoto důvodu existuje několik metod s různými stupni přesnosti. Určení pravděpodobnosti s vhodně zvolenou přesností je však klíčové pro určení rizik.

3.3.2 Likehood Indicators

Cílem tohoto dokumentu je popsat metodologii pro určení dopadu, jaký by mělo chybějící zabezpečení, na komponent pravděpodobnosti definovaný dříve. [8]

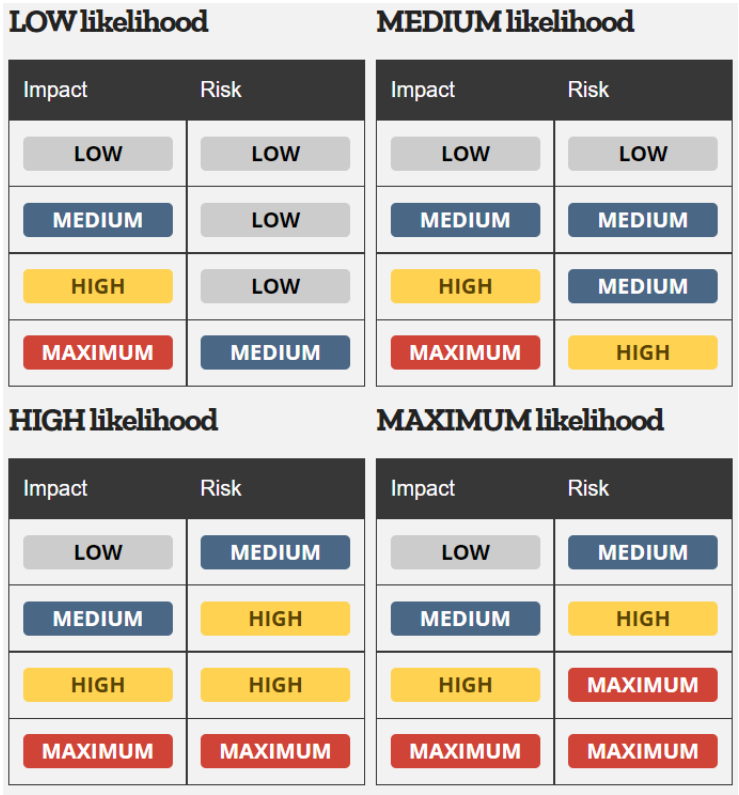
Pravděpodobnost se řídí primárně kvalitou či absencí zabezpečení, na rozdíl od rizika, které se řídí převážně zdroji, které mohou být ohroženy. Rámec Mozilly k pravděpodobnosti přistupuje jako k ukazateli šance, že některá ze zranitelností bude kvůli absenci zabezpečení

zneužita během jednoho kalendářního roku. S využitím Standard Levels [12] je lze rozdělit do několika úrovní podle pravděpodobnosti projevení se v případě absence zabezpečení:

- **Nízká pravděpodobnost**: riziko se pravděpodobně neprojeví. Může způsobit zhoršení nebo zpomalení reakce na bezpečnostní incident.
- **Střední pravděpodobnost**: riziko se může projevit během následujícího roku. Zabezpečení je důležité, nicméně v případě zavedení podpůrných zabezpečení není vyžadováno.
- **Vysoká pravděpodobnost**: riziko se pravděpodobně projeví během následujícího roku. Zabezpečení je důležité a může být zanedbáno pouze u služeb s nízkou prioritou.
- **Maximální pravděpodobnost**: riziko se projeví během následujícího roku. Zabezpečení je vyžadováno.

Při určování pravděpodobnostního ukazatele je třeba brát v potaz, jak snadno lze odhalit zranitelnost, absenci jejího zabezpečení a v případě jeho absence i obtížnost zneužití. Taktéž je třeba zhodnotit, jak moc chybějící zabezpečení usnadňuje odhalení zranitelnosti ve službě, jestli aktuálně probíhají útoky na tuto chráněnou službu a případně jak často služba trpěla na útoky tohoto typu v minulosti.

Na závěr článek uvádí přehlednou tabulku dopadů a míry rizika pro každou z uvedených pravděpodobností (na obrázku níže).



Obrázek 3.1: Vliv pravděpodobnosti a dopadu na velikost rizika[8]

3.3.3 Mozilla Rapid Risk Assessment

Základní myšlenkou dokumentu je, že běžně používáme vyhodnocování rizika při běžném denním rozhodování bez toho, abychom o tom nějak hluboce přemýšleli. Tento dokument má za cíl dát rámec tomuto rozhodování a zajistit opakovatelnost a konzistenci procesu a taktéž snadnou komunikaci výsledků.[10]

Dle dokumentu trvá typické rychlé vyhodnocení rizik (Rapid Risk Analysis / Assessment) zhruba 30 minut. Nejedná se však o podrobnější analýzu nebo audit, nicméně ty lze na základě tohoto vyhodnocení stavět. Hlavním cílem je porozumět významu služeb, jejich hodnotě a vlivu, ať už na reputaci, finance nebo produktivitu, přičemž v této části vůbec neřešíme procesy nebo zabezpečení jako takové.

Dále dokument zmiňuje informaci, že data jsou nejdůležitějším subjektem analýzy rizik. Všichni pracují s daty, ať už jde o uživatele, webové stránky, software, sítě. Ti všichni data zpracovávají, uchovávají a vyměňují. Na základě této myšlenky pak stanovuje několik klíčových vlastností tohoto postupu, jako například rychlost (30-60 minut), absence detailů (ty se dají vybudovat postupem času na základě rychlé analýzy), čitelnost a jednoduchost. Na základě tohoto postupu a vzniklé analýzy si lze pak klást další otázky, jako například zda je nastavené zabezpečení dostačující, zda není třeba akutně něco opravit, na kterou část se blíže zaměřit a jestli neexistuje slepé místo, které jsme přehlédli.

Dle autorů je doporučené spolupracovat na prvním rychlém vyhodnocení rizik daného projektu se zkušeným analytikem rizik a taktéž jej vytvořit již v návrhové fázi služby. Pro vytvoření analýzy je taktéž dobré mít k dispozici informace o zodpovědných osobách, datech a datových tocích, klasifikaci dat (veřejné, soukromé a důvěrné) a jiných důležitých aspektech služby. Klíčová je taktéž dobrá znalost způsobu, jakým služba funguje.

V dokumentu je uvedeno taktéž několik situací, při kterých není vhodné pracovat s rychlým vyhodnocením rizik. Prvním případem je, pokud jej chceme použít na cokoliv jiného, než službu, např. máme otázky k nové vlastnosti nebo funkci, kterou chceme přidat. V takovém případě je vhodné pracovat přímo se službou, na kterou se vlastnost nebo funkce váže či s již hotovou analýzou nebo rychlým vyhodnocením rizik této služby. Dále pak není vhodné používat tento postup na velké služby kvůli jejich komplikovanosti. Pokud je možné takovou službu rozdělit na menší služby nebo podslužby, které spravují specifická data, mají menší sadu funkcí a jsou za ně případně odpovědné různé týmy. Pokud velkou, komplexní službu nelze rozdělit na menší části, je vhodné uvažovat o přepracování návrhu této služby.

V rámci rychlého vyhodnocení rizik je třeba se zaměřit na hodnotu, kterou služba má pro jejího vlastníka, data se kterými pracuje, dopady nejhoršího možného scénáře a které typy útoku nebo pohrom byly brány v potaz. Je třeba zanedbat bezpečnostní opatření a jejich efektivitu, neboť jde o informace, jejichž získání je časově náročné a je možné jej provést později v rámci hlubší analýzy. Stejně tak musíme z velké části zanedbat i pravděpodobnost, neboť její určení je opět časově náročné a Mozilla Foundation poskytuje jiné procesy pro její určení.

Před samotným zahájením rychlého vyhodnocení rizik je třeba několik kroků. Prvním je ujištění se, že neexistuje žádná předchozí zpráva o rychlé analýze rizik. Pokud existuje, nebudeme vytvářet novou, ale vylepšovat původní. Druhým je vytvoření kopie standardizované šablony výsledného dokumentu. Třetím krokem je pozvat jednoho až dva členy, kteří jsou se službou spojeni (majitel, správce, aj.) a kteří mají alespoň trochu odborných znalostí o službě a kteří s sebou přinesou informace o datech spojených se službou. Posledním krokem je ujistit se, že všichni účastníci znají cíle a postupy rychlého vyhodnocení rizik a jaké jsou její kroky.

Podstatnou dovedností potřebnou k správnému vedení rychlého vyhodnocení rizik je organizace času. Je třeba být asertivní, zkrátit diskuzi na minimum a vyhnout se tendenci debatovat o bezpečnostních opatřeních. Není třeba, aby diskuze zabíhala příliš do detailu. Dokument zmiňuje jeden dobrý tip, a to vyhradit si na rychlé vyhodnocení rizik 60 minut, ale chovat se tak, jako bych si vyhradil pouze polovinu času. Dále je dobré mít přehled o čase.

Během první minuty by měly být vyplněny informace o službě, jako je její název, vlastník (zodpovědná osoba; pokud není určena, jedná se o osobu, která by řešila případný incident) a nadřízeného zodpovědné osoby. Dalších zhruba pět minut je vyhrazeno na popis služby, konkrétně k čemu slouží a jak funguje. Je třeba se ujistit, že jsme pochopili tyto informace správně, nejlépe tím, že je přeformulujeme a necháme si je potvrdit vlastníkem služby.

Následující část by měla trvat pět až deset minut a jejím cílem je se zaměřit na datový slovník, což jsou veškeré informace o datech, které služba zpracovává a ukládá. Zde je třeba uvést hlavně klasifikaci dat, tzn. pro koho jsou data určena. Předposlední částí o časovém okně mezi pěti a deseti minutami je stanovení scénářů, při kterých by data uvedená v datovém slovníku byla ohrožena, přičemž bereme v potaz hlavně nejhorší scénáře, a taktéž dopady těchto scénářů. Je třeba myslet hlavně na tři body, a to:

- Důvěrnost - co se stane, když data uniknou mezi veřejnost?
- Integrita - co se stane, když data budou zavádějící, nesprávná nebo bude jinak ovlivněna jejich integrita?
- Dostupnost - co se stane, když data budou nedostupná nebo smazaná?

Dokument přímo uvádí příručku, jak stanovit velikost dopadu ve třech hlavních kategoriích (reputace, produktivita a finanční stránka) od nízkého až po nejvyšší. Posledním krokem je stanovit cirka v 5 minutách doporučení, které sestávají z dalších kroků, jako například kontrola a nastavení záznamů o přístupu, práv přístupu, plánů reakce na incident, kontroly zda služba splňuje bezpečností politiku firmy aj.

Osobně si myslím, že principy rychlého vyhodnocení rizik by mohly být základem, na kterém bych rád stavěl svůj návrh analýzy rizik, neboť se jedná o rychlý a účinný způsob, jak získat základní přehled o službách a datech, se kterými pracují, přičemž tento základ lze pak dále rozvíjet a stavět na něm komplexní analýzu s návrhem řešení. Navíc se dle mého názoru jedná o vhodný přístup pro malé a střední firmy z hlediska poměru ceny (časové i finanční) a výkonu.

3.3.4 Scoring and other levels

Cílem tohoto dokumentu je zajistit konzistenci mezi dalšími bezpečnostními dokumenty Mozilla Foundations [11]. Jako první definuje úrovně doporučení, konkrétně „volitelné“ (je možné provést nebo ignorovat), „mělo by být“ (musí být provedeno, výjimky jsou možné pouze po diskuzi) a „musí být“ (musí být bez výjimky provedeno).

Dále jsou stanoveny tři úrovně stavu konfigurace. První z nich je „moderní“, tedy správně provedený z pohledu bezpečnosti, vhodný pro služby citlivé na bezpečnost, což ale může vést k menší kompatibilitě s klienty nebo servery. Druhá je „střední“, která je Mozilla Foundation doporučována jako výchozí, pokrývá největší množství klientů a ačoliv pár klientů či serverů může být nekompatibilních, jedná se o menší množství, než u „moderní“ konfigurace. Poslední možností je pak „zastaralá“ konfigurace, která by měla být použita

pouze v nejhorším případě, kdy není technická možnost uplatnit jinou konfiguraci. Je relativně bezpečná, ale musí být co nejdřívě předělána na „střední“ konfiguraci. Podporuje největší množství serverů a klientů.

Další částí je popis stavových kódu dokumentů, jejich vysvětlení a stavy testů, nicméně se jedná spíše o interní popisy, které nejsou pro téma této bakalářské práce důležité. Jako poslední věc pak dokument popisuje úrovně hodnocení, ke kterému používá stupnici A až F (s vynechaným písmenem E) a taktéž znaménka plus a mínus jako mezistupně. Toto známkování je stejné jako školní, tedy A značí nejlepší známku a F nejhorší. Jeho využití není pouze pro hodnocení rizik, ale spíše pro hodnocení celkového cíle nebo úkolu.

Myslím si, že ačkoliv jde o poměrně krátký dokument a část z něj se přímo netýká řízení rizik, je důležitým základem, na kterém staví následující dokument týkající se přímo standardních úrovní. Jeho znalost mi poskytla náhled do způsobů definování pojmů včetně toho, proč je třeba některé pojmy přímo definovat.

3.3.5 Standard levels

Jedná se o další z řady dokumentů, které Mozilla Foundation používá k ustanovení a udržení konzistence mezi svými dokumenty [12]. Základní myšlenkou je stanovení konvencí v označování úrovní barvou a názvem, a taktéž stanovení očekávání od určitých úrovní. V případě standardních úrovní rizika se jedná o zjednodušení ISO 31000, přičemž toto zjednodušení standard nenaplňuje. Celkem se rizika dělí do pěti kategorií.

První z nich je maximální riziko (označeno červenou barvou), tedy riziko s nejvyšší úrovní důležitosti. Toto riziko vyžaduje plnou pozornost všech zúčastněných stran a veškeré dostupné zdroje, má velké nebo maximální dopady a téměř nikdy nemůže být akceptováno jako zbytkové riziko. Doporučeno je okamžité zahájení práce na vyřešení.

Druhé je vysoké riziko (označeno žlutou barvou). Taktéž vyžaduje plnou pozornost všech zúčastněných stran, nicméně v tomto případě již není potřeba všech dostupných zdrojů, nýbrž jen části. Má střední, vysoké nebo maximální dopady a lze jej akceptovat jako zbytkové riziko pouze po diskuzi a mělo by dojít ke snížení rizika. Doporučené je zahájení práce na vyřešení do sedmi dnů.

Třetí je střední riziko (označeno modrou barvou), které vyžaduje pozornost všech zúčastněných stran (ne však plnou) a ačkoliv vyžaduje zdroje na vyřešení, nejedná se již o klíčové zdroje. Dopady tohoto rizika mohou být malé, střední nebo velké. Opět by toto riziko mělo být přijato jako zbytkové pouze po diskuzi a měla by být vyvinuta snaha o jeho snížení. Doporučené je zahájení práce do 90 dnů.

Předposledním rizikem je nízké (označeno šedou barvou), u kterého je pozornost očekávána, ale nikoliv vyžadována. Jeho dopady mohou být nízké nebo střední a je často přijatelné jako zbytkové riziko. Nemá žádný očekávaný čas zahájení práce.

Posledním rizikem je neznámé riziko (označeno bílou barvou), u kterého chybí dostatek dat. V tomto případě se očekává hlubší průzkum a přeřazení do jedné z výše uvedených kategorií. Konceptuálně se jedná o přístup „důvěruj, ale prověřuj“, tedy že nálepka neznámého rizika nezdiskredituje službu nebo uživatele, nicméně poukáže na to, že je třeba hlubšího průzkumu.

Dále v závěru dokumentu následují čtyři praktické příklady použití včetně ukázky dočasného řešení situace a přijetí zbytkového rizika.

Z mého pohledu je takovéto přehledné a čisté určení kategorií, časů a priorit, velice důležité. Umožňuje jasně sdělit, kde leží priorita při řízení rizik a co je třeba řešit před-

nostně, přičemž navíc i ukazuje praktický přístup k sníženi rizika. Tento dokument mě velice inspiroval a pomohl mi ujasnit si, co dalšího by má finální práce měla obsahovat.

3.3.6 Phishing

Ačkoliv tento dokument přímo nespadá do kategorie řízení bezpečnosti, poskytuje jasný a přesný návod, jak postupovat v případě pocitu, že se osoba stala cílem phishingu a ukazuje jeden z důvodů, proč je pro správné zabezpečení IT potřeba taktéž neustálého školení uživatelů.[9] V prvé řadě je třeba si uvést, co to vlastně phishing je. Dle dokumentu se jedná o útok na uživatele, jehož cílem je donutit jej provést akci, kterou by za normálních okolností nevykonal (například kliknout na odkaz, přihlásit se, provést platbu nebo otevřít přílohu). Důsledkem takového jednání může být například ovládnutí počítače, zaplacení za neposkytnuté služby nebo získání přístupových údajů k uživatelskému účtu.

Dokument uvádí, že nejlepší obranou proti tomuto typu útoku je vlastní intuice. Pokud se email zdá podezřelý, neočekávaný nebo vyžaduje podezřelou akci, je třeba se zastavit a zamyslet. Dále nabízí několik možností, jak útok odhalit. První z nich jsou emailové hlavičky. Uvedený návod se však vztahuje pouze na Gmail od Google, stále však přehledně uvádí, jak lze využít podvrhnutí odesilatele v hlavičce.

Další, podstatně podrobněji popsanou možností, je prozkoumat odkazy a být obezřetný. HTML dokumenty mohou obsahovat odkazy i na emailové adresy, které je taktéž třeba před odesláním zprávy kontrolovat. Většina emailových klientů umožňuje při přejetí myší nad odkazem zobrazit jeho adresu. Další běžnou taktikou útočníka je použití adresy s doménou, která na první pohled připomíná jinou, důvěryhodnou doménu, ale ve skutečnosti využívá záměny znaků nebo změny jejich pořadí, například náhradou písmene „O“ za číslici nula.

Doporučenými způsoby, jak se bránit, je neklikat na odkazy ve zprávě, ale otevírat stránku ručně zadáním adresy nebo přes záložky v prohlížeči. Další možností, která brání pouze proti krádeži přihlašovacích údajů, je používání správce hesel s podporou automatického vyplňování formulářů vázaného na doménu. V případě útoku sice může uživatel stále vyplnit přihlašovací údaje ručně, nicméně samotný fakt, že automatické vyplnění nefungovalo, by mělo sloužit jako varování.

Poslední uváděnou možností, jak útok odhalit, je obezřetnost při otevírání přiložených souborů. Prvním krokem je ověření původu zprávy, například pomocí výše zmíněné hlavičky a obsahu zprávy. Dle dokumentu existují tři typy příloh, které jsou více nebezpečné, než ostatní. Patří mezi ně PDF dokumenty (mohou obsahovat počítačové viry), MS Word nebo Excel dokumenty (obzvlášť v případě, že je pro jejich správnou funkci nutno povolit spuštění Makre) a Bash nebo EXE soubory.

Dokument taktéž doporučuje v případě podezření na Phishing kontaktovat firemní bezpečnostní tým (pokud existuje) případně jinou zodpovědnou osobu. Dále, jak již bylo zmíněno, doporučuje používání správce hesel, který dokáže odhalit drobné rozdíly v doménovém jménu, čímž může uživatele varovat, že je něco v nepořádku.

Ačkoliv tento dokument přímo nespadá pod řízení rizik, dle mého názoru skvěle zpracovává tématiku Phishingu, která, jak je všeobecně známo, je poslední dobou na vzestupu. Osobně mi tam trochu chybí ukázky častých taktik, jako například pojmenování EXE souboru tak, aby jeho jméno evokovalo, že se jedná o obrázek nebo fakturu. Nejdůležitějším poznatkem, který si lze z tohoto dokumentu odnést, je myšlenka toho, že jakákoliv bezpečnostní politika ve firmě je prakticky bezzubá za předpokladu, že nepočítá s pravidelným školením zaměstnanců v oblasti Phishingu a jejich obezřetností.

3.4 Shrnutí

Pro větší přehlednost jsem se rozhodl poznatky získané studiem těchto standardů a návodů shrnout do několika bodů.

- Řízení bezpečnosti je proces, kterého se účastní celý podnik (i když někteří zaměstnanci pouze okrajově nebo vůbec). Je nutné, aby si vedení podniku bylo vědomo, co jim přinese řízení rizik v oblasti IT a mělo motivaci vyhradit nezbytné prostředky. Je třeba, aby každý zaměstnanec znal svou roli v procesu řízení rizik a aby celý proces podporoval, nikoliv sabotoval.
- Řízení bezpečnosti vyžaduje vedení dokumentace, která nemusí být rozsáhlá, jak požaduje například standard ISO, ale musí obsahovat všechny potřebné informace.
- Proces řízení rizik ve firmě je možné (a do jisté míry nutné) postupem času vylepšovat s tím, jak zainteresované osoby postupně získávají zkušenosti.
- Pro správné vyhodnocení rizik a nastavení opatření je třeba alespoň jednoho pracovníka, který se v dané problematice vyzná, a v ideálním případě se i neustále vzdělává (např. s pomocí kurzů nebo samostudiem).

Kapitola 4

Analýza aktuální situace

Jedním z důležitých faktorů při návrhu metodiky je správně motivovat podniky a srozumitelně jim vysvětlit, proč je řízení bezpečnosti důležité. Je třeba, aby si byly vědomy, proti čemu stojí, jaké jsou rizika a případné následky.

4.1 Zpráva NÚKIB

Každý rok Národní úřad pro kybernetickou bezpečnost vydává svou zprávu o kybernetické bezpečnosti. Dle nejnovější z nich, která shrnuje rok 2020, se mezi nejčastější typy útoků patřil spam, phishing a skenování vnějších sítí organizací[2]. Pouze jednotky respondentů čelily skenování vnitřní sítě nebo nelegální těžbě kryptoměn. Do kategorie nejzávažnějších útoků pak zařadili ransomware (virus šifrující data a požadující výkupné), DoS/DDoS útoky (znepřístupnění služby) spear-phishingové emaily (cílené phishingové útoky) a pokusy o zneužití zranitelností.

Více než polovina respondentů sdělila, že byli vystaveni alespoň jednomu útoku, avšak u téměř tří čtvrtin z nich tento útok nevedl k bezpečnostnímu incidentu. Ačkoliv největší počet bezpečnostních incidentů detekovaly instituce veřejné správy a zdravotnická zařízení, neznamená to, že k nim nedochází i v ostatních institucích, neboť tato statistika může být ovlivněna schopností odhalit útoky mířící na integritu a důvěrnost dat, jejichž detekce vyžaduje odborný personál a pokročilé detekční technologie.

Ačkoliv v roce 2019 docházelo většinou ke zvyšování rozpočtu na kybernetickou bezpečnost, v roce 2020 došlo ve 43 % případů k jeho snížení. Podíl vynaložených nákladů se stále pohybuje v rozmezí mezi nula až pěti procenty, což hodnotí více než polovina organizací jako nedostatečnou. Zajímavostí je, že 62 % respondentů alokuje pouze 0-2 % svého rozpočtu na bezpečnost.

Dalším z problémů je nedostatek odborných pracovníků a fakt, že 68 % organizací uvedlo, že nízké finanční ohodnocení vedlo k odrazení nových pracovníků v oblasti kybernetické bezpečnosti již při samotném náboru. Nejčastějším způsobem, jak se vyrovnat s nedostatkem odborníků je pak outsorcingem a nebo pomocí benefitů, např. ve formě dalšího vzdělávání.

Pozitivní zprávou je, že se 86 % organizací snažilo útokům předcházet s pomocí školení svých uživatelů. I přesto, že polovina dotázaných nemá vyhrazené specifické finanční prostředky na školení uživatelů, u více než poloviny z nich proběhlo školení jednou za rok nebo častěji. Téměř čtvrtina organizací pak prováděla simulované phishingové kampaně nebo své uživatele testovala v rámci penetračního testování.

Mezi nejčastější typy útoků, které byly Národnímu úřadu pro kybernetickou bezepčnost hlášeny, patří hlavně škodlivý kód (virus, trojský kůň, spyware aj.), útok na dostupnost (DoS / DDoS útoky, sabotáž) a průnik (úspěšné získání přístupu k uživatelskému účtu nebo aplikaci). Méně častý pak byl podvod nebo phishing, sběr informací a administrativní nebo technický bezpečnostní incident (způsobený vlastní chybou).

Největší hrozbu dle zprávy představuje kybernetická kriminalita. Největším vývojem v rámci kyberkriminální aktivity prošly ransomware útoky, které v roce 2020 nejvíce zasáhly sektor zdravotnictví, například Fakultní nemocnici Brno nebo Psychiatrickou nemocnici Kosmonosy. Postupně tak částečně dochází k odklonu od nízkonákladových, nezacílených útoků na masy lidí s rychlým ziskem směrem k cíleným útokům na konkrétní organizace. Tyto útoky jsou pečlivě plánovány a výkupné je stanovováno na základě průzkumu napadeného systému, analýzy souborů a stanovení jejich potencionální hodnoty pro napadenou instituci.

V oblasti ransomware se ve světě objevil i trend tzv. dvojitého vydírání, kdy útočník odcizí citlivá data a poté vydírá oběť skrze jejich zveřejnění. Ačkoliv v Česku k tomuto typu útoku dle NÚKIB v roce 2020 stále nedošlo, uvádí s pravděpodobnosti 25 až 50 %, že k němu v budoucnu dojde.

NÚKIB dle zprávy doporučuje napadeným subjektům neplatit za dešifrování dat, neboť neexistuje záruka, že tak útočník skutečně učiní a může být získáním výkupného motivován k dalším útokům. Nejdůležitější je v tomto případě prevence v podobě rozdělení sítě na menší části (segmentace), aktualizací softwarového vybavení a vytváření offline záloh, minimálně u kritických systémů. Dle odpovědí respondentů celkem 89 % z nich tvoří offline zálohy, nicméně 33 % z celkového počtu netestuje jejich obnovitelnost. Osobně si však myslím, že zaplacení může být jednou z možností jak data získat zpět, neboť v případě nedešifrování dat by mohla utrpět jejich reputace a další oběti by nebyly ochotny zaplatit.

Myslím si, že vzhledem k tomu, že se z velké části jedná o statistiky získané na základě dotazníkového šetření, může docházet k velkému zkreslení. Navíc i zpráva samotná uvádí, že některé útoky je obtížné detekovat. Z osobní zkušenosti většinou (hlavně u malých a středních podniků) dochází k detekci útoku až zpětně ve chvíli, kdy vyústí v bezpečnostní incident.

4.2 Zkušenost z praxe

S ohledem na ochranu obchodního tajemství jsem se rozhodl v této části vynechat konkrétní označení a detaily, které nejsou podstatné pro srovnání subjektů a uvést pouze informace obecné povahy.

4.2.1 Příspěvková organizace

V rámci praxe jsem se setkal s několika subjekty, ve kterých jsem prováděl správu IT a snažil se pracovat s analýzou rizik. První z nich byla příspěvková organizace zřizovaná krajem se zhruba 30 klientskými stanicemi (počítače a notebooky) a dvěma servery s operačním systémem Windows Server 2013 a 2016. Původně celou síť spravoval interní zaměstnanec, nicméně po bezpečnostním incidentu s ransomwarem, který vyústil v zašifrování hlavního serveru a NAS, se vedení rozhodlo tohoto zaměstnance propustit a na správu IT si najmout externí firmu.

Z analýzy, kterou provedl kolega vyplynulo několik závažných problémů. Prvním problémem, který souvisel se zákonnými povinnostmi, bylo užití nelegálního software, především

operačního systému Windows 7. Druhým výrazným problémem bylo ignorování rizik souvisejících se zastaralým softwarem a hardwarem, jakožto i chybějící antivirovou ochranou a otevřenými porty služeb, jako je například Remote Desktop Protocol. Dalším výrazným prvkem bylo nedostatečné proškolení zaměstnanců, kteří si na pracovních počítačích vyřizovali soukromé emaily. Posledním problémem, se kterým jsme bojovali, bylo omezení přístupů, neboť každý zaměstnanec měl práva Administrátora na svém PC a přístupy na sdílený disk bez omezení.

Z těchto informací lze usuzovat, že bezpečnostní incident s ransomwarem nebyl přímým důsledkem jednoho chybného kroku, ale spíše vyústěním dlouhodobé situace, do které se organizace dostala. Důsledky tohoto incidentu paralyzovaly velkou část organizace, neboť trvalo několik měsíců, než se specializované firmě povedlo data dešifrovat a obnovit, přičemž cena za obnovení značně převyšovala roční náklady na externí správu IT. Z rozhovorů se zaměstnanci pak vyplynulo, že zaměstnanec, který měl správu IT na starosti, si nebyl většiny rizik vědom a pokud na ně byl upozorněn zaměstnanci, buď je vědomě ignoroval nebo bagatelizoval.

Z výše uvedeného lze tedy usuzovat, že samotné řízení rizik v IT by organizaci s nejvyšší pravděpodobností nepomohlo vyhnout se tomuto bezpečnostnímu incidentu a ani by nevedlo k nápravě zmíněných nedostatků. Problém totiž nebyla pouze absence standardizovaného procesu, ale i nedostatečné znalosti a zkušenosti správce IT a jeho osobní přístup. Je navíc nepravděpodobné, že by si organizace mohla dovolit zaplatit experta v oboru, neboť i přesto, že si prošli výše zmíněným incidentem a paralýzou, stále se občas objevovaly problémy s financováním a s ochotou uvolnit prostředky na některá nutná opatření.

4.2.2 Soukromá organizace

Druhým subjektem, se kterým jsem se v rámci praxe setkal, byla menší soukromá organizace se zhruba 100 zaměstnanci, 35 uživatelskými stanicemi (počítači, notebooky) a třemi servery, z toho dva využívaly operační systém Windows Server 2016 a jeden Windows 10. Správu IT jsme převzali po odchodu interního zaměstnance ke konkurenční společnosti. Tento zaměstnanec nám přenechal manuál o obsahu cca pěti stránek A4, obsahující přístupové údaje, kontaktní osoby a popis sítě.

Po předchozích zkušenostech z příspěvkové organizace jsme na základě dohody s vedením firmy přistoupili k provedení analýzy situace a rizik, kterou jsem prováděl sám. Zde je nutno podotknout, že bez jakýchkoliv zkušeností se standardy řízení rizik. Na základě analýzy situace jsme pak s kolegy stanovili plán postupné transformace IT, který by vedl k lepšímu přehledu a minimalizaci rizik na přijatelnou úroveň. Tento plán byl poté předán vedení organizace k seznámení se a následnému zahájení jednání o rozsahu prováděných prací.

Než jsme však stihli přistoupit k provedení změn, došlo k bezpečnostnímu incidentu v podobě útoku ransomware na jeden ze server a zašifrování veškerých uložených dat. Vzhledem k tomu, že se na tomto serveru nacházel i software pro řízení výroby (od objednávky přes výrobu až po expedici, včetně účetnictví a správy majetku), došlo ke kompletní paralýze celého subjektu a zastavení výroby.

Okamžitě po tomto incidentu bylo souběžně spuštěno několik procesů. Prvním z nich byla analýza situace a sběr informací o způsobu, jakým útočník pronikl na server. Toto šetření jako nejpravděpodobnější příčinu určilo otevřený port RDP do sítě internet a neaktualizovaný operační systému, což v kombinaci vedlo ke zneužití zranitelnosti Remote Desktop protokolu.

Druhým procesem byla záchrana dat z napadeného serveru a jeho obnova do funkčního stavu. Jako nejsnažší cesta se jevila obnova ze zálohy, nicméně dokument, který vypracoval předchozí správce IT, neobsahoval žádné detaily o zálohách a v podstatě sděloval pouze to, že by měly existovat zálohy na NAS serveru. Jak se později ukázalo, zálohy skutečně existovaly, nicméně byly prováděny serverem na nepřetržitě připojený síťový disk, který byl připojen i v době incidentu, a tím pádem došlo i k zašifrování těchto záloh, což potvrdila analýza obsahu disku.

Nakonec se však povedlo na disku najít jednu zálohu, která byla ze dne před detekcí incidentu a která shodou okolností a díky příznivé shodě okolností unikla zašifrování. Došlo tedy k záchraně dat, čisté instalaci operačního systému a obnově ze zálohy. Tentokrát však byl na server instalován i antivir s pokročilými bezpečnostními prvky (mimo jiné například firewallem) a došlo k rekonfiguraci firewallu na výchozí bráně tak, aby přístup k určitým službám byl povolen pouze na dané IP adresy a postupnému přechodu na VPN.

Posledním procesem, který započal v době detekce incidentu, bylo odvirování klientských PC a jejich rekonfigurace. Vzhledem k tomu, že v době detekce nebyla známa příčina, jako jednou z možných příčin incidentu se jevila možnost napadení zevnitř infikovaným klientským PC. Při této činnosti byly detekovány soukromé aktivity na firemních počítačích, které mohly ohrozit bezpečnost firmy, například instalace programů nesouvisejících s výkonem práce nebo otevírání soukromé mailové korespondence. V rámci této činnosti bylo zjištěno, že na téměř všech klientských stanicích s Windows 7 byly zakázány automatické aktualizace.

Z rozhovorů s vedením později vyplynulo, že podobný incident se již pravděpodobnosti v minulosti stal, nicméně správce IT tuto skutečnost vedení částečně zamlčel a snažil se ji řešit ve svém volném čase. Taktéž jsme zjistili, že správa IT tvořila pouze 20 % úvazku správce IT, který se měl primárně věnovat jiné práci spadající pod obchodní oddělení.

Srovnáme-li situaci v tomto soukromém výrobním podniku s krajem zřizovanou příspěvkovou organizací, můžeme vidět několik podobných rysů. Prvním z nich je skutečnost, že obě organizace absentovaly řízení rizik. V obou případech taktéž docházelo k ignorování rizik správci IT. V případě soukromého subjektu sice vedení bralo IT jako důležitou součást firmy a dle vlastního tvrzení (podloženého jak rozhovory se zaměstnanci, tak fakturami o nákupu hardware a software) se snažilo o jeho rozvoj a o aktivní komunikaci se správcem IT, nicméně stejně jako u příspěvkové organizace docházelo k přehlížení některých rizik či dokonce k jejich bagatelizaci.

Myslím si, že v tomto případě je velká pravděpodobnost, že by k incidentu nedošlo, pokud by firma nasadila proces řízení rizik. Vedení firmy by v takovém případě za předpokladu dokumentace tohoto procesu mělo nejen přehled o aktuálním stavu, ale i výhled nutných investic, mezi které by se dalo zařadit i školení správce IT v oblasti bezpečnosti. Ačkoliv si firma nemohla finančně dovolit experta v této oblasti, s prostředky, kterými firma disponovala, by teoreticky bylo možné nasadit alespoň nějaký proces řízení rizik a postupně jej vylepšovat tak, aby byla zvýšena bezpečnost i s ohledem na to, že podstatná část chodu firmy je na IT oblasti závislá.

4.2.3 Malé podniky a živnostníci

Poslední typ organizací, se kterými jsem se setkal, byly malé podniky a živnostníci. Konkrétně jde o OSVČ s maximálně 10 zaměstnanci a pěti PC, jednu restauraci a jednu kavárnu. Ve všech třech případech organizace neměly stálého správce IT, pouze si najímaly firmy nebo jednotlivce na konkrétní úkony. Problémy většinou řešily až když nastaly. K IT

infrastruktuře navíc absentovala jakákoliv dokumentace a i kvůli tomu, že každou část dělal jiný člověk, chyběl celkový koncept a situace se stávala nepřehlednou.

Ke správě IT v těchto organizacích jsme byli s kolegy přizváni až ve chvíli, kdy došlo k několika vážný incidentům, které ohrozily chod podniků a které opět vedly k minimálně částečné paralýze. Největší problém, se kterým jsme se potýkali, byla absence konceptu a dokumentace spolu s nutností stlačit náklady na nejnižší možnou hranici.

Ve všech třech případech by se proces řízení rizik musel obejít bez vlastního správce IT a tedy i bez interního odborného pohledu. Jako cenově dostupné řešení se však nabízí nasazení řízení rizik s přizváním externího odborníka v oboru IT.

4.2.4 Shrnutí

Bezpečnostní situace ve všech výše uvedených organizacích byla ve velmi špatném stavu a dle mého názoru nebyla otázka zda, ale kdy dojde k bezpečnostnímu incidentu s maximálním dopadem, paralyzujícím chod organizace. Společným znakem je absence systematičnosti a taktéž neexistující nebo nedostatečná dokumentace situace, která by výrazně pomohla zotavení.

Myslím si, že nebýt těchto incidentů s maximálním dopadem, nebylo by si vedení firem vědomo toho, jakému riziku se vystavují a nemělo by motivaci investovat více prostředků, ať už časových nebo finančních, do zabezpečení firmy a do případného procesu řízení rizik. Jsem toho názoru, že je třeba organizacím nabídnout nejen jednoduchou možnost řízení rizik, ale taktéž je správně motivovat k nasazení tohoto procesu.

Kapitola 5

Návrh metodiky

5.1 První verze

Na začátku bylo třeba si ujasnit cílovou skupinu, pro kterou je metodika sestavována, a tomu přizpůsobit koncepci textu a volbu termínů. Vzhledem k tomu, že v tomto případě je cílovou skupinou management malého až středního podniku, rozhodl jsem se zvolit spíše méně odbornou formu.

Dokument jsem se rozhodl rozdělit na následující části:

- **Úvod**
- **Než začneme** - v této části jsou uvedeny důležité body, které je třeba mít na paměti, nejen předtím, než se podnik rozhodne začít s řízením rizik, ale i v průběhu procesu.
- **Postup** - hlavní část, ve které jsou popsány jednotlivé kroky.
- **Další kroky** - v této části informuji čtenáře o myšlence řízení rizik jako nikdy nekončícího procesu, který je třeba neustále zdokonalovat a v rámci kterého je nutné neustále získávat nové informace.
- **Závěr** - shrnuje důležité myšlenky pojící se s řízením rizik.

V rámci samotného postupu jsem se rozhodl vycházet především z myšlenky řízení rizik uvedené v příručce pro řízení rizik v IT Queenslandské vlády [5], která uvádí, že řízení rizik je strukturovaný proces zahrnující primárně aktivity k identifikaci rizika, vyhodnocení rizika, snížení rizika a vytvoření nouzového plánu, ale taktéž proces přezkoumávání postupů řízení rizik.

Prvním krokem je příprava. V této části je čtenář seznámen s nutností alokace dostatečných finančních, lidských a časových zdrojů, a taktéž s myšlenkou vedení dokumentace, která tvoří podstatnou část řízení rizik.

Druhým krokem je pak analýza aktuální situace. V této části jsem se rozhodl pro zjednodušení sloučit proces identifikace a vyhodnocení rizika. Samotnou analýzu jsem se rozhodl rozdělit na tématické okruhy s myšlenkou, že se jedná pouze o kostru a podnik si ji může upravit dle svých potřeb a rozšířit si ji o okruhy, které jsou pro konkrétní podnik specifické.

Volba okruhů a jejich řazení je následující:

- **Data a Zálohy** - dle zprávy NÚKIB[2] sice ransomware nepatří mezi nejčastější útoky, ale je kategorizován jako jeden ze dvou nejzávažnějších. Zpráva dále zmiňuje

zvyšující se trend těchto útoků. Není to však jediné ohrožení pro data. Vždy existuje možnost selhání hardware, lidská chyba a další faktory, které mohou vést k jejich ztrátě. Z těchto důvodů jsem se rozhodl tyto okruhy nejen zařadit, ale uvést jako první.

- **Antivirová ochrana** - v dnešní době některé antivirové programy umí chránit nejen proti malware, ale taktéž proti phishingu. S jedinou výjimkou všechny produkty testované nezávislou rakouskou antivirovou laboratoří AV-Comparatives v roce 2021 umí zabránit 90 % phishingových útoků, které NÚKIB ve své zprávě uvádí jako 2. nejčastější typ útoku[1].

- **Hesla** - tento okruh jsem vybral na základě standardu ISO 27001 [14], který pro certifikaci vyžaduje nastavenou politiku hesel.

- **Hardware a software** - používání zastaralého hardware a software bez podpory výrobce je dle zprávy NÚKIB[2] nejčastěji identifikován jako nedostatek při kontrolní a auditní činnosti, což mě vedlo k myšlence zařadit jej v seznamu okruhů na jedno z vyšších míst.

- **Omezení přístupů** - opět jeden z okruhů, který se dotýká standardu ISO 27001[14], konkrétně části řízení přístupů. Do této části jsem se rozhodl zařadit i okruh týkající se VPN připojení, neboť dle zprávy[2] NÚKIB sleduje narůstající trend útoků v podobě skenování vnější sítě.

- **Výměnná média** - dle standardu ISO 27001[14] představují výměnná média několik rizik a je třeba je řídit.

- **Uživatelé** - dle zprávy NÚKIB[2] se souhrnně phishing a spear-phishing řadí na 2. příčku nejčastějších útoků a zároveň na 1. příčku v otázce závažnosti útoku. Dále pak uvádí školení uživatelů jako jednu z vhodných možností snižování hrozby úspěšného útoku tohoto typu.

- **Plán a kontakty** - tento okruh vychází souhrnně ze standardu ISO 27001[14] a příručky Queenslandské vlády [5]. V obou případech je zahrnuto vytvoření krizového plánu, který neslouží k zabránění incidentu, ale k snížení jeho dopadů.

- **Další okruhy** - tento „okruh“ klade důraz na kreativitu procesu řízení rizik a na nutnost jeho uzpůsobení konkrétním potřebám podniku.

Třetím krokem je návrh a implementace konkrétních opatření. Opět zde vycházím z konceptu ISO 27001[14], konkrétně z myšlenky plánování postupů snížení rizik a současné tvorby dokumentace. V tomto případě je třeba určit prioritu, podle které by jednotlivé plány měly být v čase prováděny, osoby zodpovědné za implementaci a dohled, časovou a finanční náročnost, konkrétní ukotvení plánu v čase, přesný postup a taktéž očekávaný výsledek implementace, aby bylo možné po dokončení porovnat skutečný stav s požadovaným.

Posledním krokem v této části je pak iterace, neboť řízení rizik není pouze záležitostí jednorázové analýzy rizik, ale dlouhodobý proces, který přináší určité závazky, mezi které patří například právě pravidelné opakování analýzy rizik, porovnávání s předchozími výsledky a hledání postupu zlepšení celého procesu.

Kapitola 6

Nasazení metodiky v praxi

Nasazení metodiky probíhalo ve strojařské firmě s 80 zaměstnanci, 30 koncovými stanicemi, 1 serverem, 2 NAS, ročním obratem kolem půl miliardy korun, bez vlastního IT oddělení či zaměstnance. Po domluvě s vedením podniku jsem se rozhodl nezveřejňovat informace, které by mohly vést k identifikaci nebo kompromitaci podniku.

Jako první proběhla schůzka s majitelem firmy a jeho zástupcem, na které jsme se domluvili na podmínkách nasazení metodiky s ohledem na bezpečnost firmy a potřeby bakalářské práce. Poté jim byla metodika zaslána v digitální podobě na mail a domluvili jsme si dva dny času na prostudování. Po této lhůtě mě firma kontaktovala s tím, že by rádi metodiku nasadili, nicméně měli několik otázek, které metodika nepokrývala.

První otázka směřovala na časovou a finanční náročnost. Z dokumentu si sice byli vědomi potřeby alokovat potřebné zdroje, avšak nebyli si jisti, jak určit alespoň přibližná čísla. Nakonec se rozhodli pro počáteční investici ve výši zhruba 80 000 Kč a 3 týdnů času.

Další věc, která se ukázala jako nejasná, bylo rozdělení rolí a úkolů. Po vysvětlení nakonec došlo k ustanovení těchto rolí:

- Vedení firmy - rozděluje role, nařizuje součinnost ostatním zaměstnancům
- Řídící pracovník - zodpovědný za vedení a vytváření dokumentace a dodržování termínů
- Ostatní zaměstnanci - spolupracují s řídícím pracovníkem, poskytují mu potřebné informace
- IT expert - externí pracovník, poskytuje odborné znalosti

V rámci tohoto bodu byla zodpovězena i otázka, kdo vytváří dokumentaci, konkrétně tedy řídící pracovník ve spolupráci s IT expertem. Na základě těchto dodatečných informací vedení firmy přiřadila tyto role konkrétním pracovníkům. Jediný problém vyvstal u otázky IT experta, neboť firma neměla interního správce IT a při výběru externího dodavatele nevěděli, jaké by měli stanovit kritéria a požadavky na jeho odborné znalosti a kvalifikaci. Po konzultaci se vedení rozhodlo hledat člověka se zkušenosti v oblasti správy IT a se znalostí technologií, které používají, a jejichž seznam si vytvořili na základě dostupných informací.

Následně byli pracovníci vedením firmy seznámeni se svými rolemi a úkoly v rámci řízení bezpečnosti IT. V průběhu následujících dnů firma zkontaktovala několik kandidátů na pozici IT experta, se kterými měla v minulosti pozitivní zkušenost.

Ve chvíli, kdy firma přistoupila k přípravě okruhů pro analýzu situace, došlo na několik doplňujících otázek ke konkrétním bodům. Jako nejasně definovaná se ukázala otázka „S jakými daty pracujete?“ - bylo třeba specifikovat, že se jedná o seznam dat.

Posledním nejasným bodem byl bod „Co se stane v případě krádeže?“, u kterého bylo objasněno, že se jedná o otázku na postup v případě krádeže zařízení a rizika s ní spojená (například kompromitace dat).

Vzhledem k použití zabezpečovacího systému, který umožňuje přístup do areálu firmy a jednotlivých budov s pomocí čipové karty, rozhodl se řídící pracovník rozšířit analyzované okruhy o otázky týkající se ztráty či odcizení přístupové karty a zaznamenávání přístupů do objektu.

Ze začátku si řídící pracovník několikrát vyžádal konzultaci se mnou, neboť absence zkušeností vedla k obtížím s vytvořením prvních dokumentů. Zde by pravděpodobně pomohla nějaká forma vzorové dokumentace, která by sloužila jako inspirace, i za cenu rizika, že by mohlo dojít k přejmutí samotného vzoru jako finální podoby dokumentace bez dalšího rozšiřování.

Následující seznam obsahuje příklad rizik, která byla odhalena:

- Zaměstnanci měli přístup k datům, ke kterým nepotřebovali či dokonce nesměli mít přístup.
- Chybějící či neúplně zálohy klíčových dat.
- Soubory záloh viditelné a smazatelné ze serveru.
- Server důležitý pro řízení chodu firmy za hranicí životnosti.
- Neaktuální firmare, software, operační systém bez podpory (Windows 7)
- Absence oddělení veřejné WiFi sítě od vnitřní.
- Přístup na RDP serveru povolen z vnější sítě s výchozím portem.
- Uživatelé neproškoleni k využívání IT vybavení (při odchodu nechávají zařízení odemčená, chybí školení o rozpoznání phishingu, instalují software bez licence).

Řídící pracovník poté ve spolupráci s IT expertem vyhodnotili míru rizika a možné dopady u jednotlivých zjištěných nedostatků. Na základě diskuze s vedením poté vypracovali několik opatření, mezi které patří například:

- Rekonfigurace přístupových práv, změna hesel.
- Výměna hlavního serveru a několika koncových stanic.
- Aktualizace aplikací, systému a firmware, výměna nepodporovaného HW.
- Uzavření všech přístupů z vnější sítě a přechod na VPN.
- Vytvoření nové politiky záloh a jejich kompletní rekonfigurace.
- Přizvání externí firmy zabývající se poskytováním internetového připojení, budování a správou sítí s žádostí o hloubkovou analýzu sítě a její restrukturalizaci.
- Nalezení externí firmy, která by poskytla školení zaměstnanců v oblasti IT bezpečnosti.

Vzhledem k časovým možnostem jsem byl nucen požádat zúčastněné osoby o zpětnou vazbu již na začátku procesu implementace opatření. Zpětná vazba probíhala formou rozhovorů s vedením firmy, s řídícím pracovníkem a s IT expertem. Abych se jednotlivé osoby navzájem neovlivňovaly, rozhovory probíhaly odděleně.

Vedení firmy vyhodnotilo náklady na zavedení procesu řízení rizik bez implementace opatření na zhruba 85 000 Kč a 13 pracovních dnů. Dle jejich slov byli s výsledkem spokojeni, získali nástroje, které mohou dále vylepšovat. Nejlépe hodnotili analýzu rizik, konkrétně její členění a výběr otázek, který jim umožnil si uvědomit, že představa o stavu IT ve firmě neodpovídá realitě. Taktéž díky této zkušenosti pochopili důležitost a význam tvoření dokumentace a její údržby. Co však považovali za problém, byla absence lepšího popisu rozdělení rolí a úkolů v rámci procesu řízení rizik, které působilo zmatečně. V souvislosti s tímto zmínili i to, že postrádali informaci o vlastnostech a dovednostech osoby IT experta poskytujícího odborný názor. Taktéž by ocenili, kdyby měli k dispozici postup, jak odhadnout prvotní náklady na zavedení tohoto procesu.

Řídící pracovník hodnotil zavedení řízení rizik jako bolestivý proces, neboť s ním neměl žádné předchozí zkušenosti. Kritizoval převážně nedostatečný popis výstupních dokumentů a velice by ocenil, kdyby měl již od začátku k dispozici vzorové dokumenty. Přiznal však, že s vysokou pravděpodobností by dokumenty vytvářel přesně podle vzorového dokumentu. Po krátké době si však našel svůj způsob, jak tuto dokumentaci tvořit a udržovat ji přehlednou, přičemž předpokládá, že se získanými zkušenostmi se kvalita dokumentace zlepší.

Externí IT expert popsal svou zkušenost jako posun správným směrem. Z jeho vyprávění vyplynulo, že již několikrát předtím si jej firma najala na zásahy v rámci IT a tato práce se vždy prodražila převážně o čas, který strávil mapováním aktuální situace převážně kvůli absenci dokumentace, ale taktéž i z důvodu chaosu, který ve správě IT panoval. Ocenil také, že se v průběhu analýzy rizik naučil nové věci a zjistil, že je třeba si v rámci správy IT pokládat více otázek ohledně bezpečnosti a možných rizik. I přes dlouholeté zkušenosti byl opět zaskočen přístupem koncových uživatelů, konkrétně především laxním přístupem k otázce phishingu a bezpečnosti. Nejvíce jej překvapil jeden ze zaměstnanců, který firemní počítač využíval k soukromým účelům, odmítal spolupracovat, nechtěl vydat heslo k účtu administrátora, některé složky měl šifrované speciálním programem a snažil se zamlčet informace o způsobu použití zařízení.

Všechny zúčastněné strany se shodly na tom, že celý proces je teprve na začátku a firmu ještě čeká dlouhá cesta, která bude vyžadovat velké množství investic v čase, přičemž jejich výše byla na základě jednání vedení firmy a IT experta odhadnuta na zhruba 300 000 Kč. Vedení taktéž začalo uvažovat o zřízení stálé pozice správce IT nebo nalezení stálého dodavatele těchto služeb, neboť současný systém najímání různých externích subjektů pro každou práci působil chaos jak v samotném IT, tak i v dokumentaci. Výsledkem byla nutnost dohledávat informace z různých zdrojů, přičemž často byly nepřesné, nekompletní nebo zcela zapomenuty.

Vedení firmy se taktéž rozhodlo zajistit externí firmu, která by pravidelně školila zaměstnance v oblasti bezpečnosti, neboť byli zaskočeni nejen jejich neznalostí, ale především špatným přístupem, který celý proces řízení rizik komplikoval. Na otázku, zda by byli ochotni provést personální změny v případě, že by někteří zaměstnanci nadále nebyli ochotni spolupracovat, vedení firmy odpovědělo, že je to sice až poslední možnost, ale jsou ochotni po ní v krajním případě sáhnout.

Z osobního pohledu hodnotím změny, které firma provedla za kladné a posun k lepšímu, a to nejen v oblasti bezpečnosti samotné, ale i přístupu k ní. Přestali IT považovat za nutný

přívěšek, ale za klíčovou součást firmy a i díky této změně se rozhodli pravidelně a ve větším množství do této oblasti investovat.

Kapitola 7

Provedené změny

S ohledem na zjištěné nedostatky jsem navrhl a provedl tyto změny metodiky. Z časových důvodů však již nebylo možné její opětovné nasazení v praxi.

- **Nedostatečně vysvětlené rozdělení rolí** - na základě nutných činností v rámci řízení rizik jsem vytvořil 4 role a určil jejich úkoly s ohledem na kompetence. Rozhodl jsem se doporučit, aby role IT experta a správce IT byly oddělené, neboť by mohlo docházet k profesní slepotě a situaci, kdy správce IT nevidí nebo přehlíží chyby ve vlastní práci.
- **Specifikace parametrů pro výběr IT experta** - ačkoliv je těžké přesně určit kvalifikaci a odbornost osoby, vhodné pro tuto roli, je možné stanovit alespoň přibližné parametry, které by měla splňovat pro náplň práce.
- **Stanovení nákladů** - vzhledem k povaze práce není nikdy možné přesně stanovit počáteční náklady. Je třeba počítat s tím, že celé nasazení se může prodražit v závislosti na tom, jak velké zmatky má podnik v dokumentaci a znalosti aktuální situace. Po zkušenostech s nasazením však považuji klíčové tuto informaci sdělit vedení podniku, neboť při alokaci prostředků s ní musí počítat neboť hrozí riziko, že pokud by k této informaci došli sami v průběhu procesu, mohli by celé řízení rizik zastavit z důvodu obav o vysoké finanční náklady.
- **Nedostatečně vysvětlená podoba dokumentace** - tuto situaci jsem se rozhodl vyřešit přidáním sekce popisující možnou podobu dokumentů. Lepším řešením by bylo vytvoření vzorových dokumentů, což však s ohledem na časové možnosti nebylo možné.
- **Špatně formulované otázky** - některé otázky bylo třeba přeformulovat, neboť jejich současná podoba byla zmatečná.

Kapitola 8

Závěr

Cílem této bakalářské práce bylo vytvoření metodiky, která by umožnila malým a středním podnikům zavést proces řízení rizik v IT a dále jej rozvíjet. Vycházela především z již existujících standardů, jako například ISO 27 001 nebo standardu vytvořeného Mozilla Foundation, přičemž bere v potaz i zákonné povinnosti, které vyplývají například z autorského zákona nebo ze směrnice GDPR.

Důležitým zdrojem informací o naplnění těchto povinností a IT bezpečnosti byla především zpráva Národního ústavu pro kybernetickou bezpečnost, ale částečně také zkušenosti z praxe. Na základě těchto informací jsem navrhl dokument, který může sloužit malým a středním podnikům k zavedení procesu řízení rizik.

Tyto postupy jsem poté předal firmě podnikající v oblasti strojírenství, která mi umožnila sledovat celý proces nasazení a vyhodnotit kvalitu postupů. Výsledkem bylo úspěšné odhalení několika významných rizik pro fungování IT v této společnosti. Na základě zpětné vazby poté došlo k úpravě metodiky a dokumentu tak, aby lépe odpovídala na otázky spojené s nasazením řízení rizik.

Zjištěné nedostatky firmu velice znepokojily a ukázaly, že bez systematického přístupu k řízení rizik je vysoká pravděpodobnost přehlédnutí potencionálních zdrojů problémů.

Ačkoliv jsem již nějakou zkušenost s analýzou rizik v malých a středních podnicích měl z praxe, tato práce mi ukázala, že je třeba daleko více systematický přístup a nelze na řízení rizik nahlížet jako na úkon, který vykonává správce IT, ale jako na proces, na kterém se podílí celý podnik a při kterém je nutná spolupráce všech zaměstnanců.

Do budoucna by bylo dobré otestovat tuto metodiku v praxi ve více druzích podniků a výslednou zpětnou vazbu opět zapracovat v podobě změn. Taktéž by bylo vhodné na základě dokumentů, které při těchto nasazeních vzniknou vytvořit vzorovou dokumentaci, která by byla dostatečně obecná, ale zároveň návodná a inspirativní.

Literatura

[1] AV Comparatives. *Anti-Phishing Tests*. AV-Comparatives [cit. 2022-04-08]. Dostupné z: https://www.av-comparatives.org/testmethod/anti-phishing-tests/.

[2] bezpečnost, N. úřad pro kybernetickou a informační. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2020*. NÚKIB, 2021. Dostupné z: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/.

[3] Evropský parlament a Rada EU. *Nařízení Evropského parlamentu a Rady (EU) 2016/679*. Úřední věstník Evropské unie, 2016. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016R0679.

[4] Government, Q. Business Queensland. *Information technology (IT) risk management* [online]. 2020 [cit. 2021-10-26]. Dostupné z: https://www.business.qld.gov.au/running-business/protecting-business/risk-management/it-risk-management.

[5] Government, Q. Business Queensland. *Managing information technology risks* [online]. 2020 [cit. 2021-10-26]. Dostupné z: https://www.business.qld.gov.au/running-business/protecting-business/risk-management/it-risk-management/managing.

[6] Lupa.cz. Tisková zpráva. *Softwarové pirátství bude stále častěji postihováno jako daňový únik* [online]. 2010 [cit. 2021-10-23]. Dostupné z: https://www.lupa.cz/tiskove-zpravy/piratstvi-bude-postihovano-jako-danovy-unik/.

[7] Mozilla Foundation. *Assessing Security Risk* [online]. Mozilla Foundation [cit. 2021-11-23]. Dostupné z: https://infosec.mozilla.org/guidelines/assessing_security_risk.html.

[8] Mozilla Foundation. *Likehood Indicators* [online]. Mozilla Foundation [cit. 2021-11-23]. Dostupné z: https://infosec.mozilla.org/guidelines/risk/likelihood_indicators.

[9] Mozilla Foundation. *Phishing* [online]. Mozilla Foundation [cit. 2022-01-12]. Dostupné z: https://infosec.mozilla.org/guidelines/phishing.html.

[10] Mozilla Foundation. *Rapid Risk Assessment* [online]. Mozilla Foundation [cit. 2021-11-23]. Dostupné z: https://infosec.mozilla.org/guidelines/risk/rapid_risk_assessment.html.

[11] Mozilla Foundation. *Scoring and other levels* [online]. Mozilla Foundation [cit. 2021-12-15]. Dostupné z: https://infosec.mozilla.org/guidelines/risk/scoring_and_other_levels.

[12] Mozilla Foundation. *Standard Levels* [online]. Mozilla Foundation [cit. 2021-11-23]. Dostupné z: https://infosec.mozilla.org/guidelines/risk/standard_levels.

[13] Národní úřad pro kybernetickou a informační bezpečnost. *FAQ* [online]. Národní úřad pro kybernetickou a informační bezpečnost [cit. 2021-10-06]. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/faq/.

[14] Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. *ČSN EN ISO/IEC 27001: Systémy řízení bezpečnosti informací – Požadavky.* 2014.

[15] Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. *ČSN EN ISO/IEC 27000: Systémy řízení bezpečnosti informací – Přehled a slovník.* 2020.

[16] ČESKO. *Zákon č. 121 ze dne 7. dubna 2000 o právu autorském.* Sbírka zákonů České republiky, 2000. částka 36. Dostupné z: https://aplikace.mvcr.cz/sbirka-zakonu/.

[17] ČESKO. *Zákon č. 181 ze dne 23. července 2014 o kybernetické bezpečnosti.* Sbírka zákonů České republiky, 2014. částka 75. Dostupné z: https://aplikace.mvcr.cz/sbirka-zakonu/.

Příloha A

Upravená verze metodiky

Fakulta informačních technologií
Vysoké učení technické v Brně

Metodika řízení rizik IT pro malé a střední podniky

2022 Vojtěch Olej (xolejv00)

Úvod

Cílem tohoto dokumentu je poskytnout jednoduchý, ale přitom účinný postup, jak provést analýzu rizik v IT, navrhnout opatření a zvýšit IT bezpečnost podniku. Výstupem by poté měly být dokumenty mapující postup analýzy, její výsledky a navrhovaná opatření, aby bylo možné celý postup pravidelně opakovat bez nutnosti začínat od nuly a taktéž aby všechny klíčové zjištěné informace byly uchovány pro další použití.

1 Než začneme

Než přistoupíme k samotnému řízení rizik, je třeba mít na paměti tyto důležité body:

- **Alokace prostředků** - vedení podniku musí zajistit, aby byly alokovány dostatečné prostředky na řízení rizik, a to jak finanční, tak časové. Bez těchto prostředků není možné řízení rizik zavést. Tyto prostředky se však podniku vrátí ve formě zvýšené bezpečnosti a komfortu. Je těžké stanovit počáteční vstupní náklady, neboť ty se odvíjí od spousty faktorů a je třeba počítat s tím, že konečné náklady mohou být klidně i řádově vyšší, především v případě, že dokumentace stavu IT neexistuje nebo je zmatečná a zavádějící.
- **Odborné znalosti** - je nutné mít k dispozici osobu, která je schopna erudovaně odpovědět na odborné otázky týkající se IT infrastruktury. Bez této osoby nelze zaručit, že získané informace budou správné a budou odpovídat realitě. V případě, že podnik nemá takovou osobu k dispozici interně, je nutné najmout externistu.
- **Zapojení celého podniku** - účast všech zaměstnanců je klíčová. Každý zaměstnanec pracuje s IT prostředky podniku jinak. Jejich spolupráce s osobou vykonávající analýzu je však klíčová, neboť jen oni mohou poskytnout přesné a úplně informace o tom, jakým způsobem pracují s IT ve firmě nebo například jaká data a kde ukládají a zpracovávají. Je úkolem managementu podniku, aby zajistilo splnění tohoto bodu.
- **Vedení dokumentace** - pro řízení rizik a zvýšení bezpečnosti IT je dokumentace klíčová. Umožňuje nám sumarizovat informace, předávat je a uchovávat pro budoucí použití. Dále nám umožňují sledovat stanovené cíle nebo postupy a jejich naplnění. Pro začátek stačí obyčejné textové dokumenty a tabulky, důležité je, aby dokumentace byla jasná, čitelná, srozumitelná a aktuální.

2 Postup

Analýza rizik slouží k tomu, abychom s pomocí správně kladených otázek hledali, co všechno se může pokazit, jaké jsou důsledky a zjistili, zda tomu lze předejít, nebo alespoň zmírnit následky.

V následujících krocích si představíme jednoduchý postup, jak provést analýzu rizik, vyhodnotit je a navrhnout postupy a opatření s cílem zvýšit bezpečnost IT.

2.1 Krok 1 - Příprava

Je třeba určit odpovědnou osobu, která bude vykonávat analýzu rizik. Tato osoba se musí seznámit s postupy řízení rizik v tomto dokumentu a musí být schopna se jimi řídit a případně je dále rozšiřovat.

Správná dokumentace je klíčová, a proto si na začátku zvolíme, jakým způsobem ji chceme vést. Doporučeným postupem je využití sdíleného disku nebo cloudových služeb, neboť s jejich pomocí může vícero lidí spolupracovat na tvorbě jednoho dokumentu, a jejich vytisknutí a archivování ve chvíli, kdy jsou dokončeny.

Dále je třeba si stanovit plán a postup v souladu s informacemi uvedenými v tomto dokumentu. Plánování je klíčovou součástí, neboť pokud je provedeno správně, snižuje chaos v procesu a tím i časové a finanční náklady.

Následující rozdělení rolí je pouze orientační. Je možné, aby jedna osoba vykonávala více rolí, nicméně je doporučené rozdělit roli řídícího pracovníka a IT experta v případě, že IT expert je zároveň správcem IT z důvodu, aby nedocházelo ke zkreslení při analýze a hodnocení vlastní práce a postupů.

- **Vedení podniku** - rozděluje role, vyčleňuje finanční a časové zdroje, zajišťuje spolupráci všech zaměstnanců a delegaci rolí.
- **Řídící pracovník** - má na starosti vedení a tvorbu dokumentace, deleguje jednotlivé úkoly, hlídá termíny, pokládá otázky a vykonává analýzu rizik.
- **IT expert** - poskytuje odborné rady a názory, pomáhá s analýzou situace a návrhem řešení.
- **Ostatní zaměstnanci** - poskytují součinnost řídícímu pracovníkovi a IT expertovi.

Pro roli IT experta je vhodné vybrat osobu, která má co největší obecný přehled v oblasti IT. V ideálním případě by měla znát minimálně technologie využívané v podniku, nebo být schopna se v krátkém čase s těmito technologiemi seznámit. Jakékoliv zkušenosti z oblasti bezpečnosti IT či řízení rizik jsou výhodou.

Dokumentaci je vhodné vést ve dvou formách (případně v jejich kombinaci). V případě textového dokumentu je vhodné jednotlivé otázky členit na odrážky a informace mapující situaci pak jako podřazené odrážky. Doporučené je použití jednoduššího textového editoru (např. Word, WordPad, Writer). Pro tabulky je pak vhodné zvolit vhodný tabulkový editor (např. Excel, Tabulky Google). Informace by měly být jasné, výstižné, věcné a měly by přesně popisovat aktuální situaci do detailu. Nejtěžší v této oblasti je udělat první krok a získat první zkušenosti, poté je možno dokumentaci dále rozvíjet a vylepšovat.

2.2 Krok 2 - Analýza situace

Analýza situace je systematický sběr informací o aktuálním stavu. V případě řízení rizik v IT se jedná o zmapování aktuálního hardware, software a dat, včetně nastavení a využití. Při mapování zároveň provádíme i další krok, a to hledání slabin a rizik. Ty se jednodušeji hledají ve chvíli, kdy máme aktuální část IT vybavení v živé paměti, přičemž vždy je možné se k nim časem vrátit a rozšířit je.

Součástí této části metodiky je i níže uvedené rozdělení s příklady otázek a doprovodným textem k vysvětlení významu. Vzhledem k tomu, že každý podnik je jiný, je třeba okruhy upravit dle konkrétní situace.

2.2.1 Data

Představují uložené informace. Ochrana dat by se měla zaměřovat především na dva prvky. První z nich je ztráta nebo poškození. V některých případech je možné data obnovit nebo znovu vytvořit, jindy však může jít o natolik unikátní informace, že bez existující zálohy není možné je nahradit.

Druhým prvkem je pak zcizení dat, které představuje riziko především u důvěrných informací a může způsobit škody na financích či reputaci. Ke zcizení nebo úniku dat může dojít ať už vlivem útoku, lidskou chybou nebo v důsledku nevhodně nastavených přístupových práv.

- S jakými daty pracujeme?
- Kam je ukládáme?
- O jaký typ dat se jedná z hlediska nahraditelnosti a důvěrnosti?
- Kdo k nim má přístup?
- Je nutné, aby tyto osoby měly přístup?
- Máme data zálohovaná? (více níže)
- Máme citlivá data šifrovaná?

Doporučený výstup: tabulka obsahující výše uvedené otázky jako sloupce

2.2.2 Zálohy

Zálohy představují záchrannou brzdu v případě, že dojde k poškození nebo ztrátě dat z hlavního zdroje. Mezi data, která lze zálohovat, patří například i nastavení serverů a zařízení - v takovém případě lze při výměně zařízení použít zálohu dat k jeho rychlé konfiguraci a zkrátit tím dobu výpadku.

V případě záloh je důrazně doporučeno mít i offline zálohy, tedy takové, které nelze smazat ze zálohovaného zařízení, například na externí disk, který je po vytvoření zálohy odpojen a uložen na bezpečném místě.

Ideálním postupem automatického zálohování je zálohování metodou „pull“, kdy si zálohovací zařízení (např. NAS server) stahuje zálohovaná data z koncových zařízení, které nemají přístup na zálohovací zařízení a tedy nemohou zálohovaná data smazat, upravit nebo přepsat.

- Kde máme zálohy?
- Jak často se vytváří?
- Používáme verzování (ukládání historie změn)?
- Jakou nejstarší zálohu máme?
- Kdo k nim má přístup? Může je smazat / přepsat?

- Co se stane, když záloha selže? Máme systém varování?
- Je nastaven proces kontroly záloh (jejich celistvosti a správnosti)?

Doporučený výstup: tabulka rozšiřující informace z okruhu 2.2.1.

2.2.3 Antivirová ochrana

Ideální volbou je komplexní balíček, který v sobě skloubí antivirovou ochranu, firewall a ochranu proti podvodným webům.

Pro vyšší počet stanic je pro jednoduchost a přehlednost lepší využít centrálně spravované antivirové ochrany (například ESET Protect), která obsahuje pokročilejší funkce jako upozornění v případě napadení firemní sítě, izolaci jednotlivých stanic aj.

- Máme dostatečnou antivirovou ochranu?
- Máme ji na všech zařízeních, kde je třeba?
- Je unifikovaná a nastavená podle zvoleného konceptu?
- Máme přehled aktuálnosti a funkčnosti?
- Dozvíme se o případném útoku?

Doporučený výstup: textový dokument obsahující výše uvedené otázky jako body.

2.2.4 Hesla

Politika hesel je jedním z klíčových prvků bezpečnosti IT, neboť zabraňuje neoprávněnému přístupu.

- Používají se bezpečná hesla?
- Jak často se hesla mění?
- Nepíší si je uživatelé „na papírek“?
- Nevyplatilo by se nám používat správce hesel?
- Co se stane, když uživatel heslo zapomene? Nedojde ke kompletní ztrátě přístupu?
- Je možné využít MFA (víceprvkové ověření, jako otisk, jednorázové heslo, SMS kód aj.)?

Doporučený výstup: textový dokument obsahující výše uvedené otázky jako body.

2.2.5 Hardware

Mít přehled o využívaném fyzickém HW vybavení je důležité především z hlediska plánování výměn, sledování životnosti a předcházením výpadků. Dále nám tento přehled umožňuje se strukturovaně zamyslet nad riziky, které se s jednotlivým vybavením pojí.

- Jaký HW v podniku využíváme?
- Kdy byl HW zakoupen? Jaká je jeho životnost? Je ještě v záruce?
- Jak kritický je pro chod podniku?
- Co se stane, když vypadne? Můžeme ho opravit nebo nahradit? Jak rychle?
- Co se stane v případě krádeže?
- Postačuje tento HW současným požadavkům? Dá se do budoucna rozšiřovat a škálovat?
- Je chráněný před přepětím nebo výpadkem proudu?
- Mohou si zaměstnanci brát HW domů (např. pro účely Home Office)?
- Mohou jej zaměstnanci používat pro soukromé účely?

Doporučený výstup: kombinace tabulky s informacemi o jednotlivém HW a textového dokumentu odpovídajícího na obecné otázky.

2.2.6 Software

I zde je opět důležité mít přehled, tvořit si seznamy. S používáním software se pojí spousta rizik nelegálního užití, od úplně absence licence (nelegální software), přes používání v nesouladu s licencí (software s licencí pouze pro osobní použití) až po porušení licenčních podmínek (licence pro jednu stanici využívána na více stanicích). Dále je vhodné software udržovat aktuální, neboť aktualizace mohou sloužit i k opravě chyb v zabezpečení.

Některá zařízení, jako například kamerové systémy, zabezpečovací zařízení aj., používají ke svému chodu firmware. I ten je třeba udržovat aktuální, protože opět může jít o potenciální bezpečnostní riziko.

- Máme seznam používaného software?
- Máme přehled o použitých licencích?
- Máme přehled o licenčních podmínkách? Dodržujeme je?
- Používáme aktuální verzi?
- Je naše verze SW stále podporovaná výrobcem? Vychází na ni aktualizace?
- Využíváme automatických aktualizací? Pokud ano, kontrolujeme jejich funkčnost?
- Používáme aktuální verzi firmware v zařízeních?

Doporučený výstup: kombinace tabulky používaného software a textového dokumentu odpovídající na obecné otázky.

2.2.7 Omezení přístupů

Základní myšlenkou izolace je, že každý člověk a zařízení by měl vidět pouze nezbytně nutné prvky a vše ostatní by měl mít skryté nebo nepřístupné bez přihlášení, protože nemohu napadnout, poškodit či ukrást něco, k čemu nemám přístup nebo co nevidím. Jakýkoliv útok na jeden PC či zařízení nesmí vést k ohrožení okolních či vyšších prvků sítě (např. napadený uživatelský počítač nesmí ohrozit server se zálohami).

Základním nástrojem je využití firewallu pro filtrování vyžádané a nevyžádané komunikace. Cílem by mělo být omezení přístupu k vnitřním službám z internetu na nezbytné minimum, v ideálním případě všechny neveřejné služby skrýt za VPN.

VPN je nástroj, který nám při správném nastavení umožňuje bezpečné spojení s firemní sítí, například v případě práce z domova. Při připojení dochází k ověření identity, čímž se snižuje riziko neautorizovaného přístupu, a taktéž k šifrovanému přenosu dat, čímž dochází k efektivnímu zabránění odposlechnutí komunikace a zachycení přenášených dat.

- Jsou přístupy k HW / SW (WiFi, IoT, kamery, server, NAS, maily) omezeny na přihlášení (pokud to umožňují)?
- V případě používání veřejné WiFi, je omezen přístup uživatelů do vnitřní sítě?
- Je nastaven Firewall a omezen přístup z internetu?
- Pokud potřebujeme přístup k službám ve vnitřní síti, můžeme k tomu využít VPN?
- Využíváme-li VPN, využíváme nejnovější standardy a šifrování?
- Fyzický přístup - jsou klíčové prvky IT infrastruktury (server, NVR, NAS, …) zamknuty?

Doporučený výstup: textový dokument obsahující jednotlivé otázky jako body.

2.2.8 Výměnná média

Výměnná média představují hlavní riziko ve třech ohledech. Prvním je, že se s jejich pomocí může šířit škodlivý kód. Druhým rizikem je jejich ztráta či odcizení a tím i únik dat. Poslední riziko pak přináší tzv. „USB killery“, což jsou zařízení, která vypadají jako obyčejný USB flash disk, ale ve skutečnosti po připojení dojde k vytvoření přepětí a zničení zařízení.

- Kdo používá výměnná média?
- K jakému účelu je využívá?

- Můžeme nastavit lepší politiku pro práci s nimi (zákaz vynášení mimo prostory podniku, omezení používání, šifrování obsahu)?
- Nelze je nahradit lepším řešením (cloud, sdílená složka, …)?

Doporučený výstup: kombinace tabulky obsahující informace o způsobu používání výměnných médií a dokumentu odpovídajícím na obecné otázky.

2.2.9 Uživatelé

Samotní uživatelé, resp. nedostatečná znalost a ostražitost mohou představovat riziko pro IT infrastrukturu. Útoky typu „phishing“, při kterých se snaží útočník donutit s pomocí triků a lží („sociální inženýrství“) uživatele k vykonání určité akce, jsou časté a mohou vyústit v bezpečnostní incident.

- Mají všichni pracovníci stanovená jasná pravidla používání IT vybavení?
- Existuje systematická kontrola dodržování těchto pravidel?
- Probíhají školení uživatelů v oblasti IT bezpečnosti?
- Ověřujeme náchylnost uživatelů k phishingovým útokům (např. pomocí testů, testovacích phishingových zpráv aj.)?
- Máme přesně stanovený proces příchodu nového pracovníka nebo odchodu starého (blokace přístupů, změna hesel, …)?

Doporučený výstup: textový dokument obsahující výše uvedené otázky jako body.

2.2.10 Plán a kontakty

Rizika nelze nikdy plně eliminovat, vždy zůstává nějaké zbytkové riziko, které je přijatelné. Důležitým prvkem, jak se s těmito riziky vypořádat, je mít připraveny nouzové plány a kontakty, a zpřístupnit tyto informace zaměstnancům, aby v případě incidentu dotčené osoby věděly, jak postupovat.

Mezi nouzové kontakty patří jak lidé v rámci podniku, kteří situaci mohou řešit, tak i externí dodavatelé, servisní firmy aj.

Nouzové plány pro případ incidentu by měly sloužit nejen k nápravě stavu, ale taktéž k analýze incidentu, vyhodnocení a případně k přepracování plánu a systému řízení rizik. Cílem by mělo být nejen incident odstranit a uvést podnik zpět do normálního stavu, ale taktéž se z incidentu poučit a pokud možno snížit riziko jeho opětovného výskytu.

- Máme aktuální seznam nouzových kontaktů?
- Má každý kontakt uvedenou i předpokládanou dobu odezvy / nápravy?
- Je tento seznam aktuální?
- Máme připraveny nouzové plány a postupy pro případ výskytu incidentu?

Doporučený výstup: textový dokument obsahující výše uvedené otázky jako body.

2.2.11 Další okruhy

Existuje množství dalších okruhů, na které se lze zaměřit. Vždy je však třeba brát v potaz potřeby daného podniku. Pokud například víme, že výroba vyžaduje stálé internetové připojení a v případě výpadku internetu, byť na krátkou dobu, dochází k pozastavení výroby v řádu hodin, je třeba toto riziko brát při analýze v potaz a zaměřit se na něj.

Důležité je mít na paměti, že řízení rizik je z velké míry kreativní proces, při kterém je třeba uvažovat s širokým rozhledem, zvažovat všechny scénáře a pokládat spoustu otázek.

2.3 Krok 3 - Návrh a implementace opatření

Ve chvíli, kdy máme zpracovanou analýzu současného stavu, můžeme přistoupit k vytvoření výběru opatření ke snížení rizika či dopadů, na jehož základě stavíme konkrétní plán implementace.

Při výběru konkrétního opatření je třeba brát v potaz více faktorů, jako například finanční a časovou náročnost, účinnost a kvalitu, udržitelnost, negativní dopady na jiné aspekty chodu podniku aj.

Vždy je třeba mít na paměti, že cílem je snížení rizika výskytu incidentu nebo jeho případných dopadů na přijatelnou úroveň. Dále je třeba sestavit plán implementace, který je třeba mít zdokumentovaný a je doporučené v něm uvést následující body:

- Jak vysoké je riziko a dopady?
- Jaká je pravděpodobnost výskytu?
- Kdo opatření implementuje?
- Kdo dohlíží na implementaci?
- Jaká je odhadovaná časová a finanční náročnost implementace?
- Jaký je časový rámec (začátek, konec) implementace?
- Jaký by měl být postup implementace?
- Jaký by měl být výsledek implementace?

Pokud by při implementaci nastala situace, kdy nelze dva a více plánů provádět současně, je třeba stanovit, který z nich bude mít vyšší prioritu. V rámci tohoto rozhodování by měla být brána v potaz nejen pravděpodobnost výskytu, velikost rizika a dopady, ale taktéž časová náročnost implementace. Prvotně by měly být provedeny plány, které ošetřují více pravděpodobné riziko s vyšším dopadem a s kratší časovou náročností.

2.4 Krok 4 - Iterace

Analýzu rizik a implementaci opatření je třeba provádět pravidelně, alespoň 1x ročně, neboť s časem se rizika mohou měnit, stejně tak jako se mění zkušenosti a znalosti osob, které řízení bezpečnosti provádí. Taktéž dochází k zastarávání dokumentace, která nepopisuje aktuální situace, což v případě bezpečnostního incidentu může vyústit v problémy s přehledností a prodloužit čas nápravy do normálního stavu.

Dále je doporučeno provádět analýzu rizik ve chvíli, kdy dochází k plánování změn v podniku. V takovém případě lze případná rizika odhalit ještě před implementací změn a díky tomu ušetřit časové i finanční prostředky. V tomto případě nemusí být nutné provádět plnou analýzu rizik, nicméně je třeba si vždy stanovit, které části IT infrastruktury se změna dotýká, a dle toho uzpůsobit pokládané otázky.

3 Další kroky

Důležitým faktorem procesu řízení rizik je jeho neustálé zlepšování. Je třeba hledat další informace, vzdělávat se, zlepšovat se a tím posouvat proces řízení rizik na další úroveň. Existuje několik cest, kterými je možné se vydat, od školení přes samostudium.

- Čtení aktuálních informací a doporučení Národního úřadu pro kybernetickou bezpečnost (NÚKIB)
- Čtení výročních zpráv o kybernetické bezpečnosti na stránkách NÚKIB
- Samovzdělávání pomocí kurzů, např. ve Vzdělávacím portálu NÚKIB
- Norma ISO/IEC 27001 - standard řízení bezpečnosti rizik

4 Závěr

Tento dokument nemůže zajistit stoprocentní bezpečnost a nastavení procesů řízení rizik IT srovnatelný s mezinárodními standardy. Je však možné se s jeho pomocí naučit alespoň základním principům a ty pak dále rozvíjet. Je třeba mít neustále na paměti, že řízení rizik není jednorázová akce, ale proces, který vyžaduje čas a úsilí, ale na oplátku poskytuje vyšší úroveň bezpečnosti. Důležité je neusnout na vavřínech a dále se vzdělávat, neboť prostředí IT je extrémně dynamické a co platilo před pěti lety, nemusí platit dnes.

Příloha B

Původní verze metodiky

Fakulta informačních technologií
Vysoké učení technické v Brně

Metodika řízení rizik IT pro malé a střední podniky

2022 Vojtěch Olej (xolejv00)

Úvod

Cílem tohoto dokumentu je poskytnout jednoduchý, ale přitom účinný postup, jak provést analýzu rizik v IT, navrhnout opatření a zvýšit IT bezpečnost podniku. Výstupem by poté měly být dokumenty mapující postup analýzy, její výsledky a navrhovaná opatření, aby bylo možné celý postup pravidelně opakovat bez nutnosti začínat od nuly a taktéž aby všechny klíčové zjištěné informace byly uchovány pro další použití.

1 Než začneme

Než přistoupíme k samotnému řízení rizik, je třeba mít na paměti tyto důležité body:

- **Alokace prostředků** - vedení podniku musí zajistit, aby byly alokovány dostatečné prostředky na řízení rizik, a to jak finanční, tak časové. Bez těchto prostředků není možné řízení rizik zavést. Tyto prostředky se však podniku vrátí ve formě zvýšené bezpečnosti a komfortu. Je jednodušší problémům předcházet, než je napravovat.
- **Odborné znalosti** - je nutné mít k dispozici osobu, která je schopna erudovaně odpovědět na odborné otázky týkající se IT infrastruktury. Bez této osoby nelze zaručit, že získané informace budou správné a budou odpovídat realitě. V případě, že podnik nemá takovou osobu k dispozici interně, je nutné najmout externistu.
- **Zapojení celého podniku** - účast všech zaměstnanců je klíčová. Každý zaměstnanec pracuje s IT prostředky podniku jinak. Jejich spolupráce s osobou vykonávající analýzu je však klíčová, neboť jen oni mohou poskytnout přesné a úplně informace o tom, jakým způsobem pracují s IT ve firmě nebo například jaká data a kde ukládají a zpracovávají. Je úkolem managementu podniku, aby zajistilo splnění tohoto bodu.
- **Vedení dokumentace** - pro řízení rizik a zvýšení bezpečnosti IT je dokumentace klíčová. Umožňuje nám sumarizovat informace, předávat je a uchovávat pro budoucí použití. Dále nám umožňují sledovat stanovené cíle nebo postupy a jejich naplnění. Pro začátek stačí obyčejné textové dokumenty a tabulky, důležité je, aby dokumentace byla jasná, čitelná, srozumitelná a aktuální.

2 Postup

Analýza rizik slouží k tomu, abychom s pomocí správně kladených otázek hledali, co všechno se může pokazit, jaké jsou důsledky a zjistili, zda tomu lze předejít, nebo alespoň zmírnit následky.

V následujících krocích si představíme jednoduchý postup, jak provést analýzu rizik, vyhodnotit je a navrhnout postupy a opatření s cílem zvýšit bezpečnost IT.

2.1 Krok 1 - Příprava

Je třeba určit odpovědnou osobu, která bude vykonávat analýzu rizik. Tato osoba se musí seznámit s postupy řízení rizik v tomto dokumentu a musí být schopna se jimi řídit a případně je dále rozšiřovat.

Správná dokumentace je klíčová, a proto si na začátku zvolíme, jakým způsobem ji chceme vést. Doporučeným postupem je využití sdíleného disku nebo cloudových služeb, neboť s jejich pomocí může vícero lidí spolupracovat na tvorbě jednoho dokumentu, a jejich vytisknutí a archivování ve chvíli, kdy jsou dokončeny.

Dále je třeba si stanovit plán a postup v souladu s informacemi uvedenými v tomto dokumentu. Plánování je klíčovou součástí, neboť pokud je provedeno správně, snižuje chaos v procesu a tím i časové a finanční náklady.

2.2 Krok 2 - Analýza situace

Analýza situace je systematický sběr informací o aktuálním stavu. V případě řízení rizik v IT se jedná o zmapování aktuálního hardware, software a dat, včetně nastavení a využití. Při mapování zároveň provádíme i další krok, a to hledání slabin a rizik. Ty se jednodušeji hledají ve chvíli, kdy máme aktuální část IT vybavení v živé paměti, přičemž vždy je možné se k nim časem vrátit a rozšířit je.

Součástí této části metodiky je i níže uvedené rozdělení s příklady otázek a doprovodným textem k vysvětlení významu. Vzhledem k tomu, že každý podnik je jiný, je třeba okruhy upravit dle konkrétní situace.

2.2.1 Data

Představují uložené informace. Ochrana dat by se měla zaměřovat především na dva prvky. První z nich je ztráta nebo poškození. V některých případech je možné data obnovit nebo znovu vytvořit, jindy však může jít o natolik unikátní informace, že bez existující zálohy není možné je nahradit.

Druhým prvkem je pak zcizení dat, které představuje riziko především u důvěrných informací a může způsobit škody na financích či reputaci. Ke zcizení nebo úniku dat může dojít ať už vlivem útoku, lidskou chybou nebo v důsledku nevhodně nastavených přístupových práv.

- S jakými daty pracujeme?
- Kam je ukládáme?
- O jaký typ dat se jedná z hlediska nahraditelnosti a důvěrnosti?
- Kdo k nim má přístup?
- Je nutné, aby tyto osoby měly přístup?
- Máme data zálohovaná? (více níže)
- Máme citlivá data šifrovaná?

Doporučený výstup: tabulka obsahující výše uvedené otázky jako sloupce

2.2.2 Zálohy

Zálohy představují záchrannou brzdu v případě, že dojde k poškození nebo ztrátě dat z hlavního zdroje. Mezi data, která lze zálohovat, patří například i nastavení serverů a zařízení - v takovém případě lze při výměně zařízení použít zálohu dat k jeho rychlé konfiguraci a zkrátit tím dobu výpadku.

V případě záloh je důrazně doporučeno mít i offline zálohy, tedy takové, které nelze smazat ze zálohovaného zařízení, například na externí disk, který je po vytvoření zálohy odpojen a uložen na bezpečném místě.

Ideálním postupem automatického zálohování je zálohování metodou „pull“, kdy si zálohovací zařízení (např. NAS server) stahuje zálohovaná data z koncových zařízení, které nemají přístup na zálohovací zařízení a tedy nemohou zálohovaná data smazat, upravit nebo přepsat.

- Kde máme zálohy?
- Jak často se vytváří?
- Používáme verzování (ukládání historie změn)?
- Jakou nejstarší zálohu máme?
- Kdo k nim má přístup? Může je smazat / přepsat?
- Co se stane, když záloha selže? Máme systém varování?
- Je nastaven proces kontroly záloh (jejich celistvosti a správnosti)?

Doporučený výstup: tabulka rozšiřující informace z okruhu 2.2.1.

2.2.3 Antivirová ochrana

Ideální volbou je komplexní balíček, který v sobě skloubí antivirovou ochranu, firewall a ochranu proti podvodným webům.

Pro vyšší počet stanic je pro jednoduchost a přehlednost lepší využít centrálně spravované antivirové ochrany (například ESET Protect), která obsahuje pokročilejší funkce jako upozornění v případě napadení firemní sítě, izolaci jednotlivých stanic aj.

- Máme dostatečnou antivirovou ochranu?
- Máme ji na všech zařízeních, kde je třeba?
- Je unifikovaná a nastavená podle zvoleného konceptu?
- Máme přehled aktuálnosti a funkčnosti?
- Dozvíme se o případném útoku?

Doporučený výstup: textový dokument obsahující výše uvedené otázky jako body.

2.2.4 Hesla

Politika hesel je jedním z klíčových prvků bezpečnosti IT, neboť zabraňuje neoprávněnému přístupu.

- Používají se bezpečná hesla?
- Jak často se hesla mění?
- Nepíší si je uživatelé „na papírek“?
- Nevyplatilo by se nám používat správce hesel?
- Co se stane, když uživatel heslo zapomene? Nedojde ke kompletní ztrátě přístupu?
- Je možné využít MFA (víceprvkové ověření, jako otisk, jednorázové heslo, SMS kód aj.)?

Doporučený výstup: textový dokument obsahující výše uvedené otázky jako body.

2.2.5 Hardware

Mít přehled o využívaném fyzickém HW vybavení je důležité především z hlediska plánování výměn, sledování životnosti a předcházením výpadků. Dále nám tento přehled umožňuje se strukturovaně zamyslet nad riziky, které se s jednotlivým vybavením pojí.

- Jaký HW v podniku využíváme?
- Kdy byl HW zakoupen? Jaká je jeho životnost? Je ještě v záruce?
- Jak kritický je pro chod podniku?
- Co se stane, když vypadne? Můžeme ho opravit nebo nahradit? Jak rychle?
- Co se stane v případě krádeže?
- Postačuje tento HW současným požadavkům? Dá se do budoucna rozšiřovat a škálovat?
- Je chráněný před přepětím nebo výpadkem proudu?
- Mohou si zaměstnanci brát HW domů (např. pro účely Home Office)?
- Mohou jej zaměstnanci používat pro soukromé účely?

Doporučený výstup: kombinace tabulky s informacemi o jednotlivém HW a textového dokumentu odpovídajícího na obecné otázky.

2.2.6 Software

I zde je opět důležité mít přehled, tvořit si seznamy. S používáním software se pojí spousta rizik nelegálního užití, od úplně absence licence (nelegální software), přes používání v nesouladu s licencí (software s licencí pouze pro osobní použití) až po porušení licenčních podmínek (licence pro jednu stanici využívána na více stanicích). Dále je vhodné software udržovat aktuální, neboť aktualizace mohou sloužit i k opravě chyb v zabezpečení.

Některá zařízení, jako například kamerové systémy, zabezpečovací zařízení aj., používají ke svému chodu firmware. I ten je třeba udržovat aktuální, protože opět může jít o potenciální bezpečnostní riziko.

- Máme seznam používaného software?
- Máme přehled o použitých licencích?
- Máme přehled o licenčních podmínkách? Dodržujeme je?
- Používáme aktuální verzi?
- Je naše verze SW stále podporovaná výrobcem? Vychází na ni aktualizace?
- Využíváme automatických aktualizací? Pokud ano, kontrolujeme jejich funkčnost?
- Používáme aktuální verzi firmware v zařízeních?

Doporučený výstup: kombinace tabulky používaného software a textového dokumentu odpovídající na obecné otázky.

2.2.7 Omezení přístupů

Základní myšlenkou izolace je, že každý člověk a zařízení by měl vidět pouze nezbytně nutné prvky a vše ostatní by měl mít skryté nebo nepřístupné bez přihlášení, protože nemohu napadnout, poškodit či ukrást něco, k čemu nemám přístup nebo co nevidím. Jakýkoliv útok na jeden PC či zařízení nesmí vést k ohrožení okolních či vyšších prvků sítě (např. napadený uživatelský počítač nesmí ohrozit server se zálohami).

Základním nástrojem je využití firewallu pro filtrování vyžádané a nevyžádané komunikace. Cílem by mělo být omezení přístupu k vnitřním službám z internetu na nezbytné minimum, v ideálním případě všechny neveřejné služby skrýt za VPN.

VPN je nástroj, který nám při správném nastavení umožňuje bezpečné spojení s firemní sítí, například v případě práce z domova. Při připojení dochází k ověření identity, čímž se snižuje riziko neautorizovaného přístupu, a taktéž k šifrovanému přenosu dat, čímž dochází k efektivnímu zabránění odposlechnutí komunikace a zachycení přenášených dat.

- Jsou přístupy k HW / SW (WiFi, IoT, kamery, server, NAS, maily) omezeny na přihlášení (pokud to umožňují)?
- V případě používání veřejné WiFi, je omezen přístup uživatelů do vnitřní sítě?
- Je nastaven Firewall a omezen přístup z internetu?
- Pokud potřebujeme přístup k službám ve vnitřní síti, můžeme k tomu využít VPN?
- Využíváme-li VPN, využíváme nejnovější standardy a šifrování?
- Fyzický přístup - jsou klíčové prvky IT infrastruktury (server, NVR, NAS, …) zamknuty?

Doporučený výstup: textový dokument obsahující jednotlivé otázky jako body.

2.2.8 Výměnná média

Výměnná média představují hlavní riziko ve třech ohledech. Prvním je, že se s jejich pomocí může šířit škodlivý kód. Druhým rizikem je jejich ztráta či odcizení a tím i únik dat. Poslední riziko pak přináší tzv. „USB killery“, což jsou zařízení, která vypadají jako obyčejný USB flash disk, ale ve skutečnosti po připojení dojde k vytvoření přepětí a zničení zařízení.

- Kdo používá výměnná média?
- K jakému účelu je využívá?
- Můžeme nastavit lepší politiku pro práci s nimi (zákaz vynášení mimo prostory podniku, omezení používání, šifrování obsahu)?
- Nelze je nahradit lepším řešením (cloud, sdílená složka, …)?

Doporučený výstup: kombinace tabulky obsahující informace o způsobu používání výměnných médií a dokumentu odpovídajícím na obecné otázky.

2.2.9 Uživatelé

Samotní uživatelé, resp. nedostatečná znalost a ostražitost mohou představovat riziko pro IT infrastrukturu. Útoky typu „phishing“, při kterých se snaží útočník donutit s pomocí triků a lží („sociální inženýrství“) uživatele k vykonání určité akce, jsou časté a mohou vyústit v bezpečnostní incident.

- Mají všichni pracovníci stanovená jasná pravidla používání IT vybavení?
- Existuje systematická kontrola dodržování těchto pravidel?
- Probíhají školení uživatelů v oblasti IT bezpečnosti?
- Ověřujeme náchylnost uživatelů k phishingovým útokům (např. pomocí testů, testovacích phishingových zpráv aj.)?
- Máme přesně stanovený proces příchodu nového pracovníka nebo odchodu starého (blokace přístupů, změna hesel, …)?

Doporučený výstup: textový dokument obsahující výše uvedené otázky jako body.

2.2.10 Plán a kontakty

Rizika nelze nikdy plně eliminovat, vždy zůstává nějaké zbytkové riziko, které je přijatelné. Důležitým prvkem, jak se s těmito riziky vypořádat, je mít připraveny nouzové plány a kontakty, a zpřístupnit tyto informace zaměstnancům, aby v případě incidentu dotčené osoby věděly, jak postupovat.

Mezi nouzové kontakty patří jak lidé v rámci podniku, kteří situaci mohou řešit, tak i externí dodavatelé, servisní firmy aj.

Nouzové plány pro případ incidentu by měly sloužit nejen k nápravě stavu, ale taktéž k analýze incidentu, vyhodnocení a případně k přepracování plánu a systému řízení rizik. Cílem by mělo být nejen incident odstranit a uvést podnik zpět do normálního stavu, ale taktéž se z incidentu poučit a pokud možno snížit riziko jeho opětovného výskytu.

- Máme aktuální seznam nouzových kontaktů?
- Má každý kontakt uvedenou i předpokládanou dobu odezvy / nápravy?
- Je tento seznam aktuální?
- Máme připraveny nouzové plány a postupy pro případ výskytu incidentu?

Doporučený výstup: textový dokument obsahující výše uvedené otázky jako body.

2.2.11 Další okruhy

Existuje množství dalších okruhů, na které se lze zaměřit. Vždy je však třeba brát v potaz potřeby daného podniku. Pokud například víme, že výroba vyžaduje stálé internetové připojení a v případě výpadku internetu, byť na krátkou dobu, dochází k pozastavení výroby v řádu hodin, je třeba toto riziko brát při analýze v potaz a zaměřit se na něj.

Důležité je mít na paměti, že řízení rizik je z velké míry kreativní proces, při kterém je třeba uvažovat s širokým rozhledem, zvažovat všechny scénáře a pokládat spoustu otázek.

2.3 Krok 3 - Návrh a implementace opatření

Ve chvíli, kdy máme zpracovanou analýzu současného stavu, můžeme přistoupit k vytvoření výběru opatření ke snížení rizika či dopadů, na jehož základě stavíme konkrétní plán implementace.

Při výběru konkrétního opatření je třeba brát v potaz více faktorů, jako například finanční a časovou náročnost, účinnost a kvalitu, udržitelnost, negativní dopady na jiné aspekty chodu podniku aj.

Vždy je třeba mít na paměti, že cílem je snížení rizika výskytu incidentu nebo jeho případných dopadů na přijatelnou úroveň. Dále je třeba sestavit plán implementace, který je třeba mít zdokumentovaný a je doporučené v něm uvést následující body:

- Jak vysoké je riziko a dopady?
- Jaká je pravděpodobnost výskytu?
- Kdo opatření implementuje?
- Kdo dohlíží na implementaci?
- Jaká je odhadovaná časová a finanční náročnost implementace?
- Jaký je časový rámec (začátek, konec) implementace?
- Jaký by měl být postup implementace?
- Jaký by měl být výsledek implementace?

Pokud by při implementaci nastala situace, kdy nelze dva a více plánů provádět současně, je třeba stanovit, který z nich bude mít vyšší prioritu. V rámci tohoto rozhodování by měla být brána v potaz nejen pravděpodobnost výskytu, velikost rizika a dopady, ale taktéž časová náročnost implementace. Prvotně by měly být provedeny plány, které ošetřují více pravděpodobné riziko s vyšším dopadem a s kratší časovou náročností.

2.4 Krok 4 - Iterace

Analýzu rizik a implementaci opatření je třeba provádět pravidelně, alespoň 1x ročně, neboť s časem se rizika mohou měnit, stejně tak jako se mění zkušenosti a znalosti osob, které řízení bezpečnosti provádí. Taktéž dochází k zastarávání dokumentace, která nepopisuje aktuální situace, což v případě bezpečnostního incidentu může vyústit v problémy s přehledností a prodloužit čas nápravy do normálního stavu.

Dále je doporučeno provádět analýzu rizik ve chvíli, kdy dochází k plánování změn v podniku. V takovém případě lze případná rizika odhalit ještě před implementací změn a díky tomu ušetřit časové i finanční prostředky. V tomto případě nemusí být nutné provádět plnou analýzu rizik, nicméně je třeba si vždy stanovit, které části IT infrastruktury se změna dotýká, a dle toho uzpůsobit pokládané otázky.

3 Další kroky

Důležitým faktorem procesu řízení rizik je jeho neustálé zlepšování. Je třeba hledat další informace, vzdělávat se, zlepšovat se a tím posouvat proces řízení rizik na další úroveň. Existuje několik cest, kterými je možné se vydat, od školení přes samostudium.

- Čtení aktuálních informací a doporučení Národního úřadu pro kybernetickou bezpečnost (NÚKIB)
- Čtení výročních zpráv o kybernetické bezpečnosti na stránkách NÚKIB
- Samovzdělávání pomocí kurzů, např. ve Vzdělávacím portálu NÚKIB
- Norma ISO/IEC 27001 - standard řízení bezpečnosti rizik

4 Závěr

Tento dokument nemůže zajistit stoprocentní bezpečnost a nastavení procesů řízení rizik IT srovnatelný s mezinárodními standardy. Je však možné se s jeho pomocí naučit alespoň základním principům a ty pak dále rozvíjet. Je třeba mít neustále na paměti, že řízení rizik není jednorázová akce, ale proces, který vyžaduje čas a úsilí, ale na oplátku poskytuje vyšší úroveň bezpečnosti. Důležité je neusnout na vavřínech a dále se vzdělávat, neboť prostředí IT je extrémně dynamické a co platilo před pěti lety, nemusí platit dnes.