Univerzita Hradec Králové

Fakulta informatiky a managementu

Katedra informačních technologií

Bezpečnost podnikové IT infrastruktury a implementace ISO 27000

Diplomová práce

Autor: Tomáš Stránský

Studijní obor: Aplikovaná informatika

Vedoucí práce: Mgr. Josef Horálek, Ph.D.

Česká Třebová duben 2015

Prohlášení

Prohlašuji, že jsem diplomovou práci zpracoval samostatně a s použitím uvedené literatury.

V České Třebové dne 26.4.2015 Tomáš Stránský

Poděkování

Rád bych poděkoval vedoucímu diplomové práce Mgr. Josefu Horálkovi, Ph.D. za jeho čas, ochotu a odbornou pomoc, kterou mi věnoval při tvorbě této práce. Také chci poděkovat Mgr. Martinu Blohoňovi za poskytnutí rad ohledně právního systému ČR, Šárce Stránské a Mgr. Katce Balcarové za finální kontrolu textu a gramatiky.

Anotace

Cílem práce je navrhnout komplexní zabezpečení podnikové infrastruktury s využitím doporučení a požadavků ISO 27000.

Teoretická část práce obsahuje popis zmíněných norem, představení zákona o kybernetické bezpečnosti a jeho dopadů na podniky podléhající i nepodléhající tomuto zákonu. Dále obsahuje teorii penetračního testování a jejich využití pro detekci zranitelností podniku.

Hlavním tématem praktické části je analýza rizik informační bezpečnosti provedená v prostředí reálného podniku. K tomu jsou využity metody SWOT analýza a penetrační testování. Na základě výsledků obou metod jsou vybrána významná rizika a zpracováno jejich hodnocení. Závěrem je provedena případová studie, která má za cíl doporučit vhodná opatření vedoucí ke zmírnění těchto rizik.

Annotation

Title: Security of enterprise IT infrastructure and implementation of ISO 27000.

The aim of this diploma thesis is to propose a comprehensive data security system within an IT infrastructure for a company which seeks to comply with the recommendations and requirements of ISO 27 000.

The theoretical part consists of a description of CSN ISO/IEC 27 000, an introduction of the law relating to cyber security and the impact this has on business subjects. It also includes penetration testing theory and the application of this theory in order to detect vulnerabilities within a company.

The main theme of the practical section is information security risk analysis. This is undertaken within a real company environment and uses SWOT analysis and penetration testing. Based upon the results achieved from both methods, significant risks are identified and evaluated. The aim of the study is to provide recommendations and remedies that help mitigate risks, which are achieved by generating data from a real-life case study.

Obsah

1. Úvod

Význam informací obecně lze jistě pokládat za jeden z nejdůležitějších aspektů dnešního světa. Nejvýznamnější vliv na jejich hodnotu má jejich přesnost a srozumitelnost, ale také přítomnost ve správný čas a na správném místě. K tomu všemu, s neustále vzrůstající tendencí, přispívají především moderní informační a komunikační technologie. Z globálního pohledu mají informační technologie často velmi významný vliv na fungování téměř všech lidských činností a dnešní svět je tedy na nich už značně závislý. Důsledkem toho je, že množství, kvalita, úplnost a další vlastnosti informací jsou neustále negativně ovlivňovány. Snadný přístup k informačním technologiím navíc přináší mnoho příležitostí pro nekalé zacházení s informacemi.

Disciplína, která si klade za úkol chránit informace, s ohledem na jejich důležitost, se nazývá informační bezpečnost. V moderních organizacích a podnicích již je nedílnou součástí řízení a snaží se o podporu klíčových strategií k dosažení a zabezpečení plánovaných cílů.

Důležitým faktorem je úroveň či stupeň informační bezpečnosti. Ten bývá závislý jak na prostředí, ve kterém se organizace nachází, tak na vyspělosti informační bezpečnosti organizace. Dobré úrovně může organizace dosáhnout zavedením systémů řízení bezpečnosti informací, který dokládá certifikát ISO/IEC 27001:2014.

První část této práce se bude zabývat popisem norem řady ISO/IEC 27000. Zde bude představen ucelený pohled na řadu norem včetně popisného seznamu. Jednotlivé podkapitoly se budou zabývat podrobněji důležitými body všech souvisejících podnorem, které je vhodné představit s ohledem na relevantnost poskytnutých informací a potřeby této práce.

Následující teoretická část bude věnována dalšímu určujícímu stupni informační bezpečnosti. Ten je dán legislativou České republiky, kterou představuje Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Jelikož cílem práce bude prověření stavu

informační bezpečnosti v podniku nepodléhajícímu tomuto zákonu, budou popsány i dopady zákona na tyto typy organizací.

Pro poskytnutí poněkud odlišného pohledu na problematiku informační bezpečnosti se bude další část práce zabývat penetračním testováním a jeho využitím pro detekci zranitelností organizace. Kapitola popíše základní pojmy, metody testování a především poskytne důležité informace o přípravě a průběhu testování, tím pomůže organizaci s prevencí proti případným potížím.

Hlavním cílem praktické části bude metodicky vytvořit a zpracovat analýzu rizik v prostředí reálného podniku. Na začátku bude společnost představena a popsány její strategické cíle. Dále bude v rámci analýzy rizik provedena SWOT analýza, jejímž cílem bude najít rizika, která souvisejí se vztahem bezpečnosti informací a informačních technologií společnosti. Druhou metodou pro detekci rizik bude penetrační testování. Tato podkapitola bude obsahovat konkrétní zadání a přípravu na provedení testů, manažerské shrnutí výsledků a podrobný popis vyplývajících rizik. Závěrem analýzy rizik bude seznam významných rizik nalezených ve SWOT analýze i penetračním testování a jejich hodnocení dle důležitosti.

V návaznosti na analýzu rizik bude provedena případová studie, jejímž cílem bude navrhnout vhodná opatření pro zlepšení informační bezpečnosti ve zkoumaném podniku.

Pro motivaci se hodí citát:

„Nic není pro mír lepší než důkladná příprava na setkání s nepřítelem.“

George Washington

2. Literární rešerše

Jedním z hlavních významů práce, stejně jako cílem implementace ISO 27000, je možnost reagovat na rychlý vývoj podnikatelského prostředí. Na tento dynamicky rozvíjející se vývoj musí organizace přijmout relevantní systémy řízení, aby i nadále posilovala mechanismy správy a managementu informací. Všechna přijatá opatření však musí být v souladu s řadou zákonů a norem. Aby bylo možné provozovat a udržovat více systémů řízení v efektivní podobě, je nezbytné jejich společné řízení, které by mělo být integrované do stávajících modulárních systémů. Jednou ze zkoumaných vazeb je integrace a analýza chování normy ISO 9001 (Systém řízení kvality) a ISO 27001 v oblasti řízení bezpečnosti informací, jak uvádí Wang a Tsai (2009), kde autoři kladly důraz na správu dokumentů a záznamů, jejich kontrolu, opravu a prevenci, systémy interního auditování s vazbou na plan-do-check-act (PDCA).

Komplexnější pohled lze nalézt v článku *Pattern-Based Support for Context Establishment and Asset Identification of the ISO 27000 in the Field of Cloud Computing* (BECKERS et al., 2011), který se zabývá stanovením ontologického rámce pro zlepšení přípravy bezpečnostních auditů, založených na normě ISO/IEC 27001 a tím posílit bezpečnostní stav společností. Cílem článku bylo vysvětlit, jak je možné bezpečnostní ontologie použít jako nástroj na podporu certifikace ISO/IEC 27001, které poskytují stěžejní informace pro přípravu auditů, vytváření a udržování bezpečnostní politiky podniku. Podobným tématem se pak zabývají autoři Neubauer a kol. (2008), jež podrobně řeší problematiku optimalizace nasazení norem ISO 27000 s přihlédnutím k bezpečnostním auditům a přípravám podnikové IT infrastruktury a firemních procesů na ně.

Významným vědeckým článkem zabývajícím se problematikou auditování dle ISO 27000 a ISO 9001 předkládá Hoy a kol. (2014). Poukazuje na vysokou potřebu plné integrace požadavků ISO 27000 do firemních procesů, jelikož jinak je získání odpovídajících bezpečnostních certifikací udělovaných na základě auditů velice obtížné a nepravděpodobné.

Přestože informační technologie hrají významnou roli v podpoře a inovacích jednotlivých podniků, jejich efektivita je úzce spojena s úspěšností řízení organizace a IT služeb. V posledních letech se význam celosvětově používaných standardů a osvědčených postupů v oblasti řízení IT procesů, jako je COBIT a ITIL, doplňuje o požadavky na bezpečnost. O tomto tématu pak pojednává Fenz (2007), který představuje případovou studii správy služeb v oblasti finančního sektoru IT realizací návrhů, které vychází z metodiky ITIL, rozšířené o bezpečnostní standardy ISO 27000. Obdobný pohled představuje Neubauer (2008), s důrazem na zvyšující se bezpečnostní hrozby a jejich vztah k best practices řízení firmy a firemních procesů.

Informační bezpečnost se dnes zaměřuje jak na veřejný tak i soukromý sektor ve snaze chránit data a informace. Článek *General Comparison of FISMA, HIPAA, ISO 27000 and PCI-DSS Standards* (GIKAS et al., 2010) představuje dvě legislativní normy z USA HIPAA a FISMA a diskutuje je se sadou norem ISO 27000. Obdobně zpracovává problematiku i Fal' (2010), který se zaměřuje na implementaci výše zmíněných norem formou případové studie. Případovou studií zabývající se implementací do norem ISO 27000 ve veřejné správě Turecka se pak zabývá Ozkan a kol. (2010). Problematikou bezpečnosti dat z pohledu zachování jejich důvěrnosti se podrobně zabývá i Gutiérrez-Martínez (2010), jenž představuje efektivní využití norem ISO 27000 ve zdravotnických organizacích.

Implementací ISO 27001 se dále podrobně zabývá Shojaie (2014), který popisuje možnosti implementace ISO norem s využitím metodiky ISMS – Coras, zaměřené a řízení firemních rizik.

Jelikož řada norem ISO 27000 se vyvíjí společně s aktuálními hrozbami a novými pohledy na ochranu IT infrastruktury a firemních procesů, je pozornost vědeckých prací orientována i na postihnutí změn mezi ISO 27000:2005 a ISO 27000:2013, jak uvádí Alebrahim (2014). S tímto je spojena i problematika zajištění bezpečnosti v moderních IT platformách jako je cloud, což je diskutováno v So a kol. (2014). Využívání těchto platforem v komerční sféře a návrhy jejich zabezpečení se zabývá Beckers (2014), jenž ISO 27000 konkrétně vztahuje na bankovní systém a splnění bezpečnostních standardů jejich cloud aplikací.

Z uvedeného je tedy zřejmé, že problematika informační bezpečnosti a implementace ISO 27000 má velký vliv nejen na samotnou IT infrastrukturu, ale i na firemní procesy, např. z důvodů úspěšného bezpečnostního auditu, což je aktuální a dynamicky se rozvíjející téma. Proto bude i v předložené práci představena řada norem ISO 27000 a její základní požadavky. Tematicky s touto normou souvisí i nový zákon o kybernetické bezpečnosti, který bude uveden včetně jeho specifik a vztahu k této práci. Metodika implementace ISO 27000 do řízení informačních technologií se bude, s ohledem na rozsah práce a praktickou využitelnost, zaměřovat na témata týkající se bezpečnostních rizik, jejich zpracování a využití s cílem zvýšit informační bezpečnost konkrétní firmy.

3. Představení normy ISO / IEC 27000

Tato kapitola představuje normu ISO/IEC 27000, řady jejích podnorem a vysvětluje důležité pojmy v obecné rovině s odkazem na využití v této práci. Znalost norem ISO/IEC 27000 je základním předpokladem pro zabývání se systémem pro řízení bezpečnosti informací.

3.1. Stručná historie

Původ řady norem ISO/IEC 27000 sahá do roku 1987, kdy bylo ve Velké Británii založeno konsorcium CCSC (Consortium for Computing Sciences in Colleges) britského Ministerstva obchodu a průmyslu. To bylo pověřeno stanovením kritérií pro hodnocení bezpečnosti IT produktů včetně vytvoření zkušebního a certifikačního schématu. V pozdější době vše vedlo ke vzniku souboru ITSEC (The Information Technology Security Evaluation Criteria) a zřízení ITSEC systému ve Velké Británii. (*The history*, 2013)

Pro pomoc uživatelům CCSC sepsala kodex osvědčených postupů v oblasti informační bezpečnosti „Users Code of Practice“, který byl publikován v roce 1989. Ten byl dále rozvíjen výzkumným ústavem NCC (National Computing Centre) a konsorciem uživatelů, tvořeným především uživateli britského průmyslu, to mělo zajistit, aby kodex byl smysluplný a praktický z hlediska uživatele. Konečný výsledek byl vydán jako britský standard dokumentem PD003 pod názvem “A code of practice for information security management” a po dalších úpravách jako britská norma BS7799:1995. Druhá část BS7799-2:1998 byla přidána v únoru 1998. Po rozsáhlé revizi a veřejné konzultaci byla zveřejněna v dubnu 1999 první revize standardu BS7799:1999. První část této normy byla navržena jako standard ISO pomocí „Fast Track“ mechanismu v roce 1999 a s drobnými změnami byla publikována o několik měsíců později jako ISO/IEC 17799:2000. Evolucí prošla také druhá část britské normy, až v roce 2005 došlo k vydání ISO/IEC 27001:2005 a ISO/IEC 17799:2005. V červenci 2007 pak byla vydána technická oprava a došlo k přečíslování „17799“ na „27002“, čímž vzniklo ISO/IEC 27002:2005. (*The history*, 2013)

3.2. ISO / IEC 27000

Řada norem ISO 27000 byla speciálně vyhrazena pro záležitost zabezpečení informací. Tyto normy však samozřejmě vycházejí také z dalších témat. Mezi nejzásadnější patří normy řady ISO 9000 (řízení jakosti) a ISO 14000 (řízení ochrany životního prostředí). (*An Introduction*, 2013)

ISO (Mezinárodní organizace pro normalizaci) a IEC (Mezinárodní elektrotechnická komise) tvoří specializovaný systém celosvětové normalizace. Národní orgány, které jsou členy ISO nebo IEC, se podílejí na vypracování mezinárodních norem prostřednictvím technických komisí ustavených příslušnými organizacemi pro jednotlivé obory technické činnosti. Technické komise ISO a IEC spolupracují v oborech společného zájmu. Práce se zúčastňují také další vládní a nevládní mezinárodní organizace, s nimiž ISO a IEC navázaly pracovní styk. V oblasti informační technologie zřídily ISO a IEC společnou technickou komisi ISO/IEC JTC 1. (ÚNMZ, 2014, s. 5)

„Hlavním úkolem společné technické komise je příprava mezinárodních norem. Návrhy mezinárodních norem přijaté technickými komisemi se rozesílají národním orgánům k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75% hlasujících národních orgánů. ISO/IEC 27000 vypracovala společná technická komise ISO/IEC JTC1 Informační technologie, subkomise SC 27 IT Bezpečnostní techniky. V současnosti je k dispozici třetí vydání.“ (ÚNMZ, 2014, s. 5)

Mezinárodní normy pro systémy řízení poskytují model určený k využití při vytváření a provozování systému řízení. Tento model obsahuje rysy, u kterých experti v daném oboru dosáhli shody, pokud jde o poslední stav mezinárodního vývoje. ISO/IEC JTC 1/SC 27 udržuje komisi expertů, která se věnuje vývoji mezinárodních norem systému řízení bezpečnosti informací – Information Security Management System (ISMS).

Organizace mohou použitím řady norem ISMS vyvinout a implementovat rámec pro řízení bezpečnosti svých informačních aktivit zahrnujících finanční informace, duševní vlastnictví a podrobnosti o zaměstnancích nebo informace, které

jim byly svěřeny zákazníky nebo třetími stranami. Tyto normy mohou být také použity pro přípravu na nezávislé posouzení jejich systému řízení bezpečnosti informací (ISMS). (ÚNMZ, 2014, s. 6)

Řada norem ISO/IEC 27000 má pomoci organizacím všech typů a velikosti zavést a provozovat ISMS. Sestává se z následujících mezinárodních norem se společným názvem Informační technologie – Bezpečnostní techniky:

- ISO/IEC 27000 Systém řízení bezpečnosti informací – Přehled a slovník
- ISO/IEC 27001 Systém řízení bezpečnosti informací – Požadavky
- ISO/IEC 27002 Soubor postupů pro opatření bezpečnosti informací
- ISO/IEC 27003 Směrnice pro implementaci systému řízení bezpečnosti informací
- ISO/IEC 27004 Řízení bezpečnosti informací – Měření
- ISO/IEC 27005 Řízení rizik bezpečnosti informací
- ISO/IEC 27006 Požadavky na orgány poskytující audit a certifikaci systémů řízení bezpečnosti informací
- ISO/IEC 27007 Směrnice pro audit systémů řízení bezpečnosti informací
- ISO/IEC TR 27008 Směrnice pro audit opatření ISMS
- ISO/IEC 27010 Směrnice pro řízení bezpečnosti informací pro meziodvětvové komunikace a komunikace mezi organizacemi
- ISO/IEC 27011 Směrnice pro řízení bezpečnosti informací pro telekomunikační organizace na základě ISO/IEC 27002
- ISO/IEC 27013 Návod pro integrovanou implementaci ISO/IEC 27001 a ISO/IEC 20000-1
- ISO/IEC 27014 Správa bezpečnosti informací
- ISO/IEC TR 27015 Směrnice pro řízení bezpečnosti informací pro finanční služby
    - ISO/IEC TR 27016 Řízení bezpečnosti informací – Organizační ekonomika . (ÚNMZ, 2014, s. 6)

3.2.1. Předmět normy ISO / IEC 27000

Účelem ISO/IEC 27000 je poskytovat přehled systémů řízení bezpečnosti informací a definovat související termíny. Použitelná je pro všechny typy i velikosti organizací, např. vládní úřady, neziskové organizace nebo obecně všechny společnosti uchovávající citlivá osobní či firemní data. (ÚNMZ, 2014, s. 8)

3.2.2. Vybrané termíny a definice

- Audit (audit) je systematický, nezávislý a dokumentovaný proces k získání důkazů z auditu a jejich objektivní ohodnocení, aby se určil rozsah, v jakém jsou auditní kritéria splněna.
- Autenticita (authenticity) je vlastnost vyjadřující, že entita je tím, za co se vydává.
- Autentizace (authentication) je poskytnutí záruky, že prohlašovaná charakteristika entity je správná.
- Dostupnost (availability) je přístupnost a použitelnost na žádost oprávněné entity.
- Důvěrnost (confidentiality) je splnění požadavku.
- Cíl (objective) je výsledek, kterého má být dosaženo.
- Hrozba (threat) je potencionální příčina nechtěného incidentu, jehož výsledkem může být poškození systému nebo organizace.
- Informační systém (information system) jsou aplikace, služby, aktiva, informační technologie nebo další komponenty zacházející s informacemi.
- Integrita (integrity) je vlastnost přesnosti a úplnosti.
- Kompetence (competence) je schopnost použít znalosti a dovednosti k dosažení zamýšlených výsledků.
- Opatření (control), řízení a kontrola jsou prostředky modifikující riziko.
- Organizace (organization) je osoba nebo skupina osob, které mají své vlastní funkce s odpovědnostmi, pravomocemi a vztahy, pomocí nichž mohou dosáhnout svých cílů.

- Politika (policy) je celkový záměr a směřování organizace, formálně vyjádřené jejím vrcholovým managementem.
- Požadavek (requirement) je potřeba nebo očekávání, které je stanovené, obecně předpokládané nebo závazné.
- Proces (process) je soubor aktivit majících vzájemný vztah nebo vzájemně na sebe působících a přeměňujících vstupy na výstupy.
- Riziko (risk) je účinek nejistoty na dosažení cílů. Riziko bezpečnosti informací je spojeno s možností, že hrozby využijí zranitelností informačního aktiva nebo skupiny informačních aktiv a tak způsobí organizaci škodu.
- Řízení přístupu (access control) jsou prostředky zajišťující, aby přístup k aktivům byl autorizován a omezen na základě obchodních a bezpečnostních požadavků.
- Událost (event) je výskyt nebo změna určité množiny okolností.
- Útok (attack) je pokus o zničení, vystavení hrozbě, změnu, vyřazení z činnosti, zcizení aktiva nebo získání neoprávněného přístupu k aktivu či uskutečnění neoprávněného použití aktiva.
- Vrcholový management (top management) je osoba nebo skupina lidí, kteří řídí a kontrolují organizaci na nejvyšší úrovni.
- Zbytkové riziko (residual risk) je riziko zbývající po ošetření rizika.
- Zranitelnost (vulnerability) je slabé místo aktiva nebo opatření, které může být využito jednou nebo více hrozbami. (ÚNMZ, 2014, s. 8-18)

3.2.3. Systémy řízení bezpečnosti informací

Organizace všech typů a velikostí uchovávají a zpracovávají informace. Všechny tyto informace jsou ohroženy mnoha škodlivými vlivy jako třeba útokem, chybou nebo přírodními účinky. Obecně se informace považují za druh aktiv, které mají určitou různou hodnotu a tudíž vyžadují příslušnou ochranu. Ochrana informačních aktiv je nezbytná proto, aby organizace mohla dosáhnout svých cílů, udržovala soulad s právními normami a udržovala a zlepšovala svoji image. Činnosti,

jako jsou zavedení vhodných opatření nebo ošetření neakceptovatelných rizik bezpečnosti informací, se nazývají prvky řízení bezpečnosti informací. Každá organizace by tedy měla stanovit svoji politiku a cíle bezpečnosti informací a dosáhnout těchto cílů efektivně pomocí systému řízení. (ÚNMZ, 2014, s. 18)

Přehled a principy

ISMS (Systém řízení bezpečnosti informací) je složen z politik, postupů, směrnic, příslušných zdrojů a činností, které organizace řídí, aby zajistila ochranu informačních aktiv. ISMS představuje systematický přístup k ustanovení, implementování, provozování, monitorování, přezkoumávání, udržování a zlepšování bezpečnosti informací organizace, aby byly dosaženy její cíle. Je také založen na posuzování a ošetření rizik. Pro úspěšnou implementaci ISMS přispívá analýza požadavků na ochranu informačních aktiv a aplikace opatření s cílem zajistit ochranu těchto informačních aktiv v souladu s požadavky. (ÚNMZ, 2014, s. 18)

Informace

Informace představují aktivum, které vyžadují odpovídající ochranu. Mohou být uchovávány v mnoha formách, a to v digitální (datové soubory), v materiální (např. na papíře) nebo jako nevyjádřené informace ve formě znalostí zaměstnanců. Přenášeny mohou být fyzicky, elektronicky nebo verbální komunikací. (ÚNMZ, 2014, s. 19)

Bezpečnost informací

Bezpečnost informací zahrnuje důvěrnost, dostupnost a integritu. Aby mohla zajistit úspěch v činnosti organizace a kontinuitu této činnosti a minimalizovat dopady incidentů na bezpečnost informací, je třeba použít a řídit vhodná opatření bezpečnosti informací, včetně zohlednění širokého rozsahu hrozeb. (ÚNMZ, 2014, s. 19)

Řízení

Řízení zahrnuje dohled a přijímání rozhodnutí nezbytných k dosažení podnikatelských cílů organizace ochranou informačních aktiv organizace. Řízení bezpečnosti informací je realizováno pomocí formulací a používáním politik, postupů

a směrnic bezpečnosti informací, které pak v celé organizaci používá každý, kdo je nějakým způsobem s organizací spojen. (ÚNMZ, 2014, s. 19)

Systém řízení

Systém řízení používá k dosažení cílů organizace rámec zdrojů. Systém řízení zahrnuje organizační strukturu, politiky, plánování činností, odpovědnosti, praktiky, postupy, procesy a zdroje. (ÚNMZ, 2014, s. 19)

Procesní přístup

Procesní přístup pomáhá organizaci fungovat efektivně a účinně. Jakákoliv činnost využívající zdroje vyžaduje řízení, aby umožnila přeměnu vstupů na výstupy pomocí souboru činností, které mají vzájemný vztah nebo interakci (což nazýváme proces). Výstup z procesu může být vstupem pro další proces a obvykle je tato transformace prováděna v plánovaném a řízeném prostředí. (ÚNMZ, 2014, s. 19)

Ustavení, monitorování, udržování a zlepšování

Je třeba, aby organizace provedla při ustavení, monitorování, udržování a zlepšování ISMS následující kroky:

a) identifikace informačního aktiva a s nimi spojené bezpečnostní požadavky;
b) posoudila rizika bezpečnosti informací a ošetřila rizika bezpečnosti informací;
c) vybrala a implementovala příslušná opatření k zvládnutí neakceptovatelných rizik;
d) monitorovala, udržovala a zvyšovala efektivnost opatření spojených s informačními aktivy organizace.

Aby bylo zajištěno, že ISMS efektivně a trvale chrání informační aktiva organizace, je nezbytné, aby tyto kroky byly neustále opakovány a tak mohly být zjišťovány změny týkající se rizik nebo strategií a cílů činnosti organizace. (ÚNMZ, 2014, s. 20)

Identifikace požadavků na bezpečnost informací

Požadavky na bezpečnost informací vycházejí v rámci celkové strategie a podnikatelských cílů organizace, při její velikosti a geografickém rozložení, ze znalosti:

a) zjištěných informačních aktiv a jejich hodnoty;
b) potřeb vyplývajících z činnosti organizace týkajících se zpracování, uchovávání a komunikace informací;
c) právních, předpisových a smluvních požadavků.

Provádění metodického posuzování rizik hrozících informačním aktivům organizace vyžaduje analýzu hrozeb ve vztahu k informačním aktivům, zranitelnostem a pravděpodobnosti hrozby k informačním aktivům a analýzu potencionálního dopadu jakéhokoliv incidentu bezpečnosti informací na informační aktiva. Výdaje na příslušná opatření by měly být úměrné předpokládanému dopadu realizovaného rizika na činnost organizace. (ÚNMZ, 2014, s. 20-21)

Posuzování rizik bezpečnosti informací

Řízení rizik bezpečnosti informací vyžaduje vhodnou metodu na posuzování rizik a na ošetření rizik, která může zahrnovat odhad nákladů a výnosů, právní požadavky, zájmy zúčastněných stran a další vhodné vstupní informace a proměnlivé faktory.

Posuzování rizik by mělo identifikovat, kvantifikovat a stanovit prioritu rizika v porovnání s kritérii pro přijetí rizika a cílů závazných pro organizaci. Výsledky by měly nasměrovat a určit příslušnou činnost managementu a systém preferencí pro řízení rizik bezpečnosti informací a pro implementaci opatření vybraných k ochraně před těmito riziky.

Posuzování rizik by mělo zahrnovat systematický přístup k předběžnému odhadu velikosti rizik (analýza rizik) a porovnání odhadnutých rizik s kritérii rizik, aby se stanovila závažnost rizik (hodnocení rizik). (ÚNMZ, 2014, s. 21)

Ošetřování rizik bezpečnosti informací

Organizace by měla před zvážením, jak ošetřit určité riziko, stanovit kritéria pro určení, zda rizika mohou nebo nemohou být akceptována. Rizika mohou být akceptována, jestliže je například odhadnuto, že riziko je nízké nebo že náklady na ošetření rizika nejsou pro organizaci rentabilní. Akceptovaná rozhodnutí by měla být zaznamenána.

Pro každé identifikované riziko je po posuzování rizika nutné rozhodnout o ošetření rizika. Možná ošetření rizika zahrnují:

a) použití vhodných opatření vedoucích ke snížení rizik;
b) vědomé a objektivní přijetí rizika, za předpokladu, že srozumitelným způsobem naplňují politiku a kritéria organizace pro přijetí rizika;
c) vyhnutí se rizikům tím, že nebudou přípustné činnosti, které by mohly vyvolat výskyt rizik;
d) sdílení rizik s jinými stranami, například s pojišťovnami nebo dodavateli.

Pro ta rizika, kde rozhodnutí o ošetření rizika znamená aplikaci vhodných opatření, by měla být tato opatření vybrána a implementována. (ÚNMZ, 2014, s. 21)

Výběr a implementace opatření

Po identifikaci požadavků na bezpečnost informací, po určení a posouzení rizik bezpečnosti informací vůči identifikovaným informačním aktivům a po přijetí rozhodnutí o ošetření rizik bezpečnosti informací je třeba vybrat a implementovat příslušná opatření vedoucí ke snížení rizik.

Opatření by měla zajistit snížení rizik na přijatelnou úroveň se zohledněním:

a) požadavků a omezení daných národní a mezinárodní legislativou a předpisy;
b) cílů organizace;
c) provozních požadavků a omezení;

d) nákladů na zavedení a provoz související se snížením rizik, při současném zachování proporcionality k požadavkům a omezením organizace;
e) jejich implementování, aby byla monitorována, vyhodnocována a zlepšována účinnost a efektivnost opatření bezpečnosti informací a byla tak zajištěna podpora cílů organizace. Výběr a implementace opatření by měly být dokumentovány v prohlášení o aplikovatelnosti a měly by tak pomoci zajistit shodu s požadavky;
f) potřeby uvést do rovnováhy investice spojené se zavedením a provozem opatření a ztrátu, která by pravděpodobně vznikla jako důsledek incidentů v oblasti bezpečnosti informací. (ÚNMZ, 2014, s. 21)

3.2.4. Řada norem ISMS

„Řada norem systému řízení bezpečnosti informací (ISMS) je složena ze vzájemně souvisejících norem, ať již zveřejněných nebo připravovaných, a obsahuje celou řadu významných strukturálních komponent. Tyto komponenty jsou zaměřeny na normativní technické normy popisující požadavky ISMS (ISO/IEC 270001) a požadavky certifikačního orgánu (ISO/IEC 27006) na organizace certifikující shodu s ISO/IEC 27001. Ostatní technické normy poskytují návod pro různé stránky implementace ISMS a zabývají se generickým procesem, směrnicemi ve vztahu k opatřením, stejně jako návody specifickými podle odvětví.“ (ÚNMZ, 2014, s. 23)

Tab. 1: Řady norem ISMS. Zdroj: upraveno autorem dle (ÚNMZ, 2014, s. 24).

Norma obsahující terminologii	27000 Přehled a slovník	
Normy specifikující požadavky	27001 Systémy řízení bezpečnosti informací - Požadavky	27006 Požadavky na orgány poskytující audit a certifikaci systémů řízení bezpečnosti informací
Normy popisující obecně směrnice	27002 Soubor postupů pro opatření bezpečnosti informací	TR 27008 Směrnice pro audit opatření ISMS
	27003 Směrnice pro implementaci systému řízení bezpečnosti informací	27013 Návod pro integrovanou implementaci ISO/IEC 27001 a ISO/IEC 20000-1
	27004 Řízení bezpečnosti informací - Měření	27014 Správa bezpečnosti informací
	27005 Řízení rizik bezpečnosti informací	TR 27016 Řízení bezpečnosti informací - Organizační ekonomika
	27007 Směrnice pro audit systémů řízení bezpečnosti informací	
Normy popisující směrnice specifické pro odvětví	27010 Směrnice pro řízení bezpečnosti informací pro meziodvětvové komunikace a komunikace mezi organizacemi	TR 27015 Směrnice pro řízení bezpečnosti informací pro finanční služby
	27011 Směrnice pro řízení bezpečnosti informací pro telekomunikační organizace na základě ISO/IEC 27002	TS 27017 Směrnice pro opatření bezpečnosti informací při použití služeb cloud computingu na základě ISO/IEC 27002
Normy popisující směrnice specifické pro opatření	2703x	2704x

Řada norem ISMS

3.2.5. Využití ISO / IEC 27000

Tato norma je úvodem do řady norem ISO/IEC 27000. Slouží jako obecný přehled o problematice systémů pro řízení bezpečnosti informací (ISMS), vymezuje důležité termíny pro jednotnou komunikaci a definuje základní pojmy potřebné pro porozumění ISMS. Morálně navazuje na řadu norem ISO 9000, jehož úspěšným splněním (certifikací ISO 9001) podniky velmi často prokazují svoji vysokou úroveň kvality (jakosti). Certifikací ISO/IEC 27001 tedy podniky prokazují vysokou úroveň bezpečnosti vzhledem k informacím.

3.3. ISO / IEC 27001

Základem řady norem, které se danou problematikou zabývají už detailněji je norma ISO/IEC 27001, je také předmětem a kritériem pro udělení certifikátu o řízení bezpečnosti informací. Tato kapitola popisuje uvedenou normu a vysvětluje vztah k ostatním normám řady ISO/IEC 27000.

3.3.1. Předmět normy ISO / IEC 27001

ISO/IEC 27001 specifikuje požadavky na ustanovení, implementování, udržování a neustálé zlepšování systému řízení bezpečnosti informací v kontextu organizace. Tato mezinárodní norma také zahrnuje požadavky na posuzování a ošetření rizik bezpečnosti informací přizpůsobené potřebám organizace. Požadavky této normy jsou obecně použitelné a jsou aplikovatelné ve všech organizacích bez ohledu na jejich typ, velikost a povahu činností. Vyloučení jakýchkoli požadavků obsažených v kapitolách 3.3.2. až 3.3.8. je nepřijatelné, pokud chce organizace dosáhnout shody s normou ISO/IEC 27001. Tato norma používá termíny a definice obsažené v ISO/IEC 27000 (podkapitola 3.2.2.). (ÚNMZ, 2014, s. 7)

3.3.2. Kontext organizace

Porozumění organizaci

„Organizace musí určit externí a interní aspekt, který je významný pro její záměry a který ovlivňuje její schopnost dosáhnout zamýšlených výstupů systému řízení bezpečnosti informací organizace.“ (ÚNMZ, 2014, s. 7)

Porozumění potřebám a očekáváním

Organizace musí dále určit:

a) zainteresované strany, které mají vztah k systému řízení bezpečnosti informací;
b) požadavky těchto zainteresovaných stran, které jsou relevantní k bezpečnosti informací. (ÚNMZ, 2014, s. 7)

Stanovení rozsahu ISMS

Pro stanovení rozsahu musí organizace určit hranice a aplikovatelnost systému řízení bezpečnosti informací. Při určování tohoto rozsahu musí organizace zvážit:

a) externí a interní aspekt (uvedený výše);
b) požadavky zainteresovaných stran (výše);
c) propojení a závislosti mezi činnostmi prováděnými organizací a těmi činnostmi, které jsou prováděné jinými organizacemi.

Rozsah ISMS musí být dostupný jako dokumentovaná informace. (ÚNMZ, 2014, s. 7)

ISMS

Organizace musí ustavit, implementovat, udržovat a neustále zlepšovat systém řízení bezpečnosti informací v souladu s požadavky ISO/IEC 27001. (ÚNMZ, 2014, s. 7)

3.3.3. Vůdčí role

Vůdčí role a závazek

Vrcholový management organizace musí s ohledem na ISMS demonstrovat vůdčí roli a závazek tím, že:

a) zajistí stanovení politiky bezpečnosti informací a cílů bezpečnosti informací slučitelných se strategickým směrováním organizace;
b) zajistí integraci požadavků systému řízení bezpečnosti informací do procesů organizace;
c) zajistí dostupnost zdrojů potřebných pro systém řízení bezpečnosti informací;
d) komunikuje význam efektivního řízení bezpečnosti informací a význam dosažení shody s požadavky systému řízení bezpečnosti informací;
e) zajistí dosažení zamýšlených výstupů systému řízení bezpečnosti informací organizace;
f) směřuje a podporuje osoby k přispívání efektivnosti systému řízení bezpečnosti informací;
g) prosazuje neustálé zlepšování;
h) podporuje ostatní relevantní řídící role k prokázání jejich vůdčí role v oblastech jejich odpovědnosti. (ÚNMZ, 2014, s. 8)

Politika

Vrcholový management musí stanovit politiku bezpečnosti informací, která:

a) je přiměřená záměrům organizace;
b) zahrnuje cíle bezpečnosti informací nebo poskytuje rámec pro nastavení cílů bezpečnosti informací;
c) zahrnuje závazek ke splnění aplikovatelných požadavků týkajících se bezpečnosti informací.

Politika bezpečnosti informací musí:

a) být dostupná jako dokument;
b) být komunikována v rámci organizace;

c) být přiměřeně dostupná zainteresovaným stranám. (ÚNMZ, 2014, s. 8)

Role, odpovědnosti a pravomoci

Vrcholový management organizace musí zajistit, že odpovědnosti a pravomoci pro role relevantní bezpečnosti informací jsou přiřazeny a komunikovány. Odpovědnosti a pravomoci musí přiřadit pro:

a) zajištění, že systém řízení bezpečnosti informací je ve shodě s požadavky ISO/IEC 27001;
b) podávání zpráv o výkonnosti systému řízení bezpečnosti informací vrcholovému managementu organizace. (ÚNMZ, 2014, s. 8)

3.3.4. Plánování

Opatření zaměřená na rizika

Při plánování systému řízení bezpečnosti informací musí organizace zvážit externí a interní aspekt, požadavky zainteresovaných stran (podkapitola 3.3.2.) a určit rizika, na která se potřebuje zaměřit pro:

a) zajištění, že systém řízení bezpečnosti informací organizace může dosáhnout zamýšlených výstupů;
b) předcházení nebo snížení nežádoucích následků;
c) dosažení neustálého zlepšování.

Organizace musí plánovat:

a) opatření zaměřená na tato rizika a příležitosti;
b) jak
    1) integrovat a implementovat tato opatření do procesů ISMS;
    2) vyhodnocovat efektivnost těchto opatření. (ÚNMZ, 2014, s. 8-9)

Posuzování rizik

Organizace musí definovat a aplikovat proces posuzování rizik bezpečnosti informací, který:

a) stanoví a udržuje kritéria rizik bezpečnosti informací, která zahrnují:
    1) kritéria akceptace rizik;
    2) kritéria pro provádění posouzení rizik bezpečnosti informací;
b) zajistí, že opakovaná posouzení rizik bezpečnosti informací produkují konzistentní, opodstatněné a porovnatelné výsledky;
c) identifikuje rizika bezpečnosti informací:
    1) používá proces posuzování rizik bezpečnosti informací k identifikaci rizik spojených se ztrátou důvěrnosti, integrity a dostupnosti informací v rozsahu systému řízení bezpečnosti informací;
    2) identifikuje vlastníky rizik;
d) analyzuje rizika bezpečnosti informací:
    1) posuzuje potencionální následky, které by nastaly, pokud by se realizovala rizika identifikovaná v bodě c) 1);
    2) posuzuje reálnou pravděpodobnost výskytu rizik identifikovaných v bodě c) 1);
    3) určuje úroveň rizik;
e) hodnotí rizika bezpečnosti informací:
    1) porovnává výsledky analýzy rizik s kritérii rizik stanovených v bodě a);
    2) stanovuje priority analyzovaných rizik pro ošetření rizika.

Organizace musí uchovávat dokumentované informace o procesu posuzování rizik bezpečnosti informací. (ÚNMZ, 2014, s. 9)

Ošetření rizik

Organizace musí definovat a používat proces ošetření rizik bezpečnosti informací pro:

a) výběr vhodných variant pro ošetření rizika bezpečnosti informací s ohledem na výsledky posuzování rizik;
b) určení všech opatření nezbytných k implementaci vybrané varianty pro ošetření rizika bezpečnosti informací;

c) porovnání opatření určených v bodě b) s opatřeními pro verifikaci, že žádné nezbytné opatření nebylo vynecháno;
d) vytvoření „Prohlášení o aplikovatelnosti“, které obsahuje nezbytná opatření z bodu b) a c) a zdůvodnění pro jejich zahrnutí, ať už jsou nebo nejsou implementována, zdůvodnění pro vyloučení opatření pro verifikaci.
e) Formulaci plánu ošetření rizik bezpečnosti informací;
f) získání souhlasu vlastníků rizik ohledně plánu ošetření rizik bezpečnosti informací a přijetí zbytkových rizik bezpečnosti informací.

Organizace musí uchovávat dokumenty o procesu ošetření rizik bezpečnosti informací. (ÚNMZ, 2014, s. 9)

Cíle

Organizace musí stanovit cíle bezpečnosti informací relevantní jednotlivým funkcím a úrovním řízení. Cíle bezpečnosti informací musí:

a) být konzistentní s politikou bezpečnosti informací;
b) být měřitelné, pokud je to proveditelné;
c) vzít v úvahu aplikovatelné požadavky bezpečnosti informací a výsledky z posuzování rizik a ošetření rizik;
d) být komunikovány;
e) být dle potřeby aktualizovány.

Organizace musí uchovávat dokumentované informace o cílech bezpečnosti informací. Při plánování jak dosáhnout cílů bezpečnosti informací musí organizace určit:

f) co bude vykonáno;
g) jaké zdroje budou vyžadovány;
h) kdo bude odpovědný;
i) kdy to bude dokončeno;
j) jak budou výsledky vyhodnoceny. (ÚNMZ, 2014, s. 10)

3.3.5. Podpora

Zdroje

„Organizace musí určit a zajistit zdroje potřebné pro ustavení, implementování, udržování a neustálé zlepšování systému řízení bezpečnosti informací.“ (ÚNMZ, 2014, s. 10)

Kompetence

Organizace musí:

a) určit nezbytné kompetence osob vykonávajících pro organizaci práci, která má vliv na výkonnost bezpečnosti informací;
b) zajistit, že tyto osoby jsou kompetentní na základě odpovídajícího vzdělání, školení nebo zkušeností;
c) tam, kde je to aplikovatelné, přijmout opatření k získání nezbytné kompetence a vyhodnocovat efektivnost těchto přijatých opatření;
d) uchovávat odpovídající dokumentované informace jako důkazy o kompetenci. (ÚNMZ, 2014, s. 10)

Povědomí

Osoby pracující pro organizaci si musí být vědomy:

a) politik bezpečnosti informací;
b) svého přínosu k efektivnosti systému řízení bezpečnosti informací, včetně výhod zlepšené výkonnosti bezpečnosti informací;
c) důsledků nepřizpůsobení se požadavkům systému řízení bezpečnosti informací. (ÚNMZ, 2014, s. 10)

Komunikace

Organizace musí ve vztahu k systému řízení bezpečnosti informací určit potřebu pro interní a externí komunikaci, která zahrnuje:

a) o čem komunikovat;
b) kdy komunikovat;
c) s kým komunikovat;

d) kdo musí komunikovat;
e) procesy, kterými musí být komunikace realizována. (ÚNMZ, 2014, s. 10)

Dokumentované informace

Systém řízení bezpečnosti informací musí zahrnovat:

a) dokumentované informace požadované ISO/IEC 27001
b) dokumentované informace určené organizací za nezbytné pro efektivnost systému řízení bezpečnosti informací. (ÚNMZ, 2014, s. 11)

Vytváření a aktualizace

Při vytváření a aktualizaci dokumentovaných informací musí organizace zajistit odpovídající:

a) identifikaci a popis (např. název, datum, autor);
b) formát (např. jazyk, verze softwaru, grafika) a média (např. papírové, elektronické);
c) přezkoumání a schválení vhodnosti a přiměřenosti. (ÚNMZ, 2014, s. 11)

Řízení dokumentovaných informací

Dokumentované informace vyžadované systémem řízení bezpečnosti informací a ISO/IEC 27001 musí být řízeny, aby bylo zajištěno následující:

a) dokumentované informace jsou dostupné a vhodné pro použití, a to kdekoliv a kdykoliv je to potřebné;
b) dokumentované informace jsou odpovídajícím způsobem chráněny (např. před prozrazením, nevhodným použitím nebo ztrátou integrity).

Pro řízení dokumentovaných informací musí organizace věnovat pozornost následujícím činnostem, pokud jsou aplikovatelné:

c) distribuci, přístupu, vyhledání a použití;
d) ukládání a zachování, včetně zachování čitelnosti;
e) řízení změn (např. verzí);
f) uchování a likvidace. (ÚNMZ, 2014, s. 11)

3.3.6. Provozování

Plánování a řízení

„Organizace musí plánovat, implementovat a řídit procesy potřebné ke splnění požadavků bezpečnosti informací a implementovat opatření z podkapitoly 3.3.4. Organizace musí také implementovat plány k dosažení cílů bezpečnosti informací určených v 2.3.4. Organizace musí udržovat dokumentované informace v nezbytném rozsahu, aby měla jistotu, že procesy byly prováděny, jak bylo plánováno. Organizace musí řídit plánované změny a přezkoumávat následky neúmyslných změn přijímáním opatření ke snížení jakýchkoliv nepříznivých dopadů, pokud je to nezbytné. Organizace musí zajistit, že jsou outsourcované procesy určeny a řízeny.“ (ÚNMZ, 2014, s. 11)

Posuzování rizik

Organizace musí posuzovat rizika bezpečnosti informací v pravidelných intervalech nebo pokud jsou plánovány nebo nastanou významné změny, a to s ohledem na kritéria stanovená v podkapitole 3.3.4. Organizace musí uchovávat dokumentované informace o výsledcích posuzování rizik bezpečnosti informací. (ÚNMZ, 2014, s. 12)

Ošetření rizik

Organizace musí implementovat plán ošetření rizik bezpečnosti informací. Organizace musí uchovávat dokumentované informace o výsledcích ošetření rizik bezpečnosti informací. (ÚNMZ, 2014, s. 12)

3.3.7. Hodnocení výkonnosti

Monitorování, měření, analýza a hodnocení

Organizace musí vyhodnocovat výkonnost bezpečnosti informací a efektivnost systému řízení bezpečnosti informací. Organizace musí také uchovávat odpovídající dokumentované informace jako důkazy o výsledcích monitorování a měření. (ÚNMZ, 2014, s. 12)

Interní audit

Organizace musí v plánovaných intervalech provádět interní audity k získání informací o tom, zda systém řízení bezpečnosti informací vyhovuje vlastním požadavkům organizace na systém řízení bezpečnosti informací a požadavkům ISO/IEC 27001. Dále také je-li efektivně implementován a udržován. (ÚNMZ, 2014, s. 12)

Přezkoumání vedením

Vrcholový management organizace musí v plánovaných intervalech přezkoumávat systém řízení bezpečnosti informací organizace pro zajištění jeho neustálé vhodnosti, přiměřenosti a efektivnosti. (ÚNMZ, 2014, s. 12-13)

3.3.8. Zlepšování

Neshody a nápravná opatření

Při výskytu neshody musí organizace:

a) reagovat na neshodu pokud je to aplikovatelné, přijmout opatření k řízení a nápravě neshody, zabývat se následky;
b) vyhodnotit potřebu pro opatření k odstranění příčin neshody, aby se neshoda znovu nevyskytla, prostřednictvím přezkoumání neshody, určení příčin neshody a určit, zda existují podobné neshody nebo by se mohly potencionálně vyskytnout;
c) implementovat jakákoliv potřebná opatření;
d) přezkoumat efektivnost každého přijatého nápravného opatření;
e) provést změny v systému řízení bezpečnosti informací, pokud je to nezbytné.

Nápravná opatření musí být přiměřená dopadům neshod, kterým čelí. (ÚNMZ, 2014, s. 13)

Neustálé zlepšování

„Organizace musí neustále zlepšovat vhodnost, přiměřenost a efektivnost systému řízení bezpečnosti informací.“ (ÚNMZ, 2014, s. 13)

3.3.9. Využití ISO / IEC 27001

Norma dále rozvádí ISO/IEC 27000. Specifikuje požadavky na ustanovení, implementování, udržování a neustálé zlepšování systému řízení bezpečnosti informací (ISMS). Říká jak porozumět cílům a potřebám organizace, jak vytvořit politiku bezpečnosti informací, jak nakládat s riziky a zdroji organizace. Definuje také pojmy jako interní audit a neustálé zlepšování. Obecně je předpisem pro další normy z řady ISO/IEC 27000, které většinou podrobněji popisují jednotlivé aspekty této normy.

3.4. ISO / IEC 27002

ISO/IEC 27002 logicky navazuje a dále rozvádí ISO/IEC 27001, tato podkapitola uvádí vztah ISO/IEC 27002 k této práci.

3.4.1. Předmět normy ISO / IEC 27002

ISO/IEC 27002 poskytuje seznam obecně akceptovaných cílů opatření a opatření pro doporučené postupy, které mají být použity jako návod k implementaci při výběru a provádění opatření, jejichž cílem je dosáhnout bezpečnosti informací. (ÚNMZ, 2014, s. 9)

3.4.2. Využití ISO / IEC 27002

Tato norma obsahuje už konkrétní typy opatření. Vzhledem ke relevantnosti a využitelnosti je možné provést výběr některých opatření (případně všech) v rámci

procesu zavádění ISMS, které popisuje norma ISO/IEC 27001. Tato opatření bezpečnosti informací je možné popsat v rámci doporučených metodik.

Jako dvě z vhodných metodik pro odhalování zranitelností systému i opakovatelnou kontrolu správnosti nasazení opatření, je v normách zmíněna SWOT analýzu a penetrační testování. Obecné využití penetračního testování popisuje kapitola 5., zpracování konkrétní SWOT analýzy a penetračních testů jsou představeny v kapitole 6.

3.5. ISO / IEC 27003

Obsahem této podkapitoly je základní informace o normě ISO/IEC 27003 a jejím využití.

3.5.1. Předmět normy ISO / IEC 27003

ISO/IEC 27003 poskytuje praktický návod pro implementaci a informace pro ustavení, implementování, provozování, monitorování, přezkoumávání, udržování a zlepšování ISMS dle ISO/IEC 27001. (ÚNMZ, 2011, s. 8)

3.5.2. Využití ISO / IEC 27003

Pomocí praktického návodu je možné vytvořit plán implementace ISMS, který se obvykle provádí jako projekt s cílem zavedení ISO/IEC 27001. Tento projekt má definovány konkrétní činnosti a jejich cíle včetně doporučených postupů, jak cílů dosáhnout. V rámci některých činností je vhodné vytvořit i podnikové směrnice.

V kapitole 7. je vytvořen popis vybraných činností a provedena případová studie sloužící k zabezpečení podnikové infrastruktury vzhledem ke konkrétní organizaci.

3.6. ISO / IEC 27004

ISO/IEC 27004 poskytuje návod a doporučení pro vývoj a měření tak, aby se dala posoudit efektivnost ISMS, cílů opatření a opatření použitých k implementaci a řízení bezpečnosti informací podle specifikace ISO/IEC 27001. (ÚNMZ, 2011, s. 9)

3.7. ISO / IEC 27005

ISO/IEC 27005 poskytuje směrnice pro řízení rizik bezpečnosti informací. Přístup popsaný v této mezinárodní normě podporuje obecná pojetí specifikovaná v ISO/IEC 27001. (ÚNMZ, 2013, s. 8)

4. Dopady zákona o kybernetické bezpečnosti na podnikovou politiku

Tato část popisuje Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Stručně představuje co je jeho obsahem, definuje, kdo zákonu podléhá a popisuje dopady na organizace podléhající i nepodléhající zákonu. Jedná se o velmi aktuální téma v oblasti informační bezpečnosti a je proto velmi vhodné se mu věnovat.

4.1. Důvody vzniku

Obecně kyberprostor označuje globalizovaný svět dnes již velmi silně propojený s fyzickým světem. Představuje souhrn technologií, systémů, procesů, autorů nejrůznějších aplikací, síťových prostředí nebo sociálních sítí. Do tohoto světa je již přesunuta veliká část našich činností. Ostatní činnosti, které přesunuty do tohoto světa nejsou, mohou být na kyberprostoru buď závislé, nebo je alespoň nějakým způsobem ovlivňují. Zákon o kybernetické bezpečnosti by měl pomoci dodržování určitých bezpečnostních pravidel, které povedou ke správnému fungování kyberprostoru.

Dnešní vyspělé státy jsou na kyberprostoru čím dál tím více ekonomicky závislé a jejich významné procento HDP je realizováno přímo přes informační a komunikační technologie, například pomocí e-shopů nebo třeba už nákupem technologií potřebných k fungování vlastního kyberprostoru. Další část HDP se realizuje pomoví e-business, elektronického účtování, elektronické fakturace, atd. Konkurenceschopnost státu pak vyplývá z jeho důvěryhodnosti pro investory, kteří vyhodnocují bezpečnost fyzického prostředí, ale i bezpečnost kyberprostoru, tak aby jejich know-how bylo dobře chráněno.

Výše uvedené závěry jsou ve shodě s viceprezidentem Českého Institutu Manažerů Informační Bezpečnosti (ČIMIB), Ing. Alešem Špidlou (2014).

4.2. Stručný přehled

Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) nabyl účinnosti 1.1.2015, skládá se ze šesti hlav.

Hlava I - Základní ustanovení

Hlava I vymezuje předmět úpravy, práva a povinnosti fyzických i právnických osob, působnost a pravomoci orgánů. Vylučuje systémy, které nakládají s utajovanými informacemi. Vymezuje několik pojmů (níže) a definuje povinné osoby v oblasti kybernetické bezpečnosti.

- Kybernetický prostor je digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, službami a sítěmi elektronických komunikací.
- Kritická informační infrastruktura je prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti.
- Bezpečnost informací je zajištění důvěrnosti, integrity a dostupnosti informací.
- Významný informační systém je informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci.
- Správce informačního systému je orgán nebo osoba, které určují účel zpracování informací a podmínky provozování informačního systému.
- Správcem komunikačního systému je orgán nebo osoba, které určují účel komunikačního systému a podmínky jeho provozování.
- Významná síť je síť elektronických komunikací zajišťující přímé zahraniční propojení do veřejných komunikačních sítí nebo zajišťující přímé připojení ke kritické informační infrastruktuře. (Česko, 2014)

Hlava II – Systém k zajištění kybernetické bezpečnosti

Obecně popisuje bezpečnostní opatření, kybernetickou bezpečnostní událost (událost, která může způsobit narušení bezpečnosti informací) a incident (konkrétní narušení bezpečnosti informací), včetně jejich evidence a způsobu hlášení úřadům.

Pojem opatření se rozděluje do kategorií na varování (zveřejněná informace o známé hrozbě), reaktivní opatření (řešení incidentu) a ochranné opatření (obecné zvýšení ochrany).

Důležitou částí je také popis kontaktních údajů a účel, povinnosti a rozdíly mezi národním a vládním CERTem. (Česko, 2014)

Hlava III – Stav kybernetického nebezpečí

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

O vyhlášení stavu kybernetického nebezpečí rozhoduje ředitel Národního bezpečnostního úřadu (NBÚ), provádí se na úřední desce NBÚ a pomocí rozhlasového a televizního vysílání. Tento stav se vyhlašuje na dobu nezbytně nutnou, nejdéle však na 7 dní (ta lze prodloužit až na 30 dní). (Česko, 2014)

Hlava IV – Výkon státní správy

Definuje povinnosti a funkce Národního bezpečnostnímu úřadu vzhledem ke státní správě. (Česko, 2014)

Hlava V – Kontrola, nápravná opatření a správní delikty

NBÚ kontroluje, jestli orgány a osoby, které podléhají zákonu o kybernetické bezpečnosti, plní povinnosti vyplývající ze zákona. Pokud zjistí nedostatky, ukládá nápravná opatření včetně časové lhůty pro odstranění. Je-li v bezprostředním ohrožení kritická informační infrastruktura, komunikační systém kritické informační

infrastruktury nebo významný informační systém, může NBÚ zakázat používání tohoto systému do doby, než bude zavedeno vhodné bezpečnostní opatření.

Zákon definuje i jak může dojít ke správnímu deliktu a ukládá maximální výše pokut. (Česko, 2014)

Hlava VI – Závěrečná ustanovení

NBÚ a Ministerstvo vnitra stanoví vyhláškou významné informační systémy a jejich určující kritéria. NBÚ pak podrobněji stanoví, jak tvořit dokumentaci, rozsah bezpečnostních opatření, kategorie a způsob hlášení bezpečnostních incidentů, jak oznámí reaktivní opatření a náležitosti oznámení kontaktních údajů. (Česko, 2014)

Pro snadnější orientaci a práci se zákonem o kybernetické bezpečnosti byla vydána Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti).

4.3. Uplatnění zákona

Kritéria pro výběr významných informačních systémů určuje Vyhláška o významných informačních systémech a jejich určujících kritériích. V příloze č. 1 této vyhlášky je konkrétní jmenný seznam významných informačních systémů a jejich správců. Mezi jmenované správce patří dle Česka (2014) například Česká inspekce životního prostředí, Český statistický úřad, Český telekomunikační úřad, Generální finanční ředitelství, všechna ministerstva, Správa státních hmotných rezerv, Úřad vlády ČR a další.

Kritickou infrastrukturu definuje Nařízení vlády č. 432/2010 Sb. o kritériích pro určení prvku kritické infrastruktury. Odvětví spadající do určujících kritérií jsou:

- Elektřina - výroba elektřiny, přenosová soustava, distribuční soustava.
- Zemní plyn - přepravní a distribuční soustava, skladování plynu.
- Ropa a ropné produkty - přepravní soustava, distribuční soustava, skladování ropy a pohonných hmot, výroba pohonných hmot.

- Centrální zásobování teplem - výroba tepla, distribuce tepla.
- Vodní hospodářství.
- Potravinářství a zemědělství - rostlinná výroba, živočišná výroba, potravinářská výroba.
- Zdravotnictví.
- Doprava - silniční, železniční, letecká a vnitrozemská vodní doprava.
- Komunikační a informační systémy - technologické prvky pevné a mobilní sítě elektronických komunikací, technologické prvky sítí pro rozhlasové a televizní vysílání, satelitní komunikace, poštovní služby.
- Finanční trh a měna.
- Nouzové služby - integrovaný záchranný systém, radiační monitorování, předpovědní, varovné a hlásné služby.
- Veřejná správa - veřejné finance, sociální ochrana a zaměstnanost, zpravodajské služby (Česko, 2014)

Významné informační systémy i kritická infrastruktura se ještě dále kategorizují. Jejich práva a povinnosti jsou uvedené v Tab. 2. Výjimkou je stav kybernetického nebezpečí, během něho tyto povinnosti neplatí.

Tab. 2: Práva a povinnosti osob a orgánů veřejné moci. Zdroj: upraveno autorem dle (Česko, 2014)

Subjekty spravující/zajišťující povinnosti	elektronické komunikace[1]	významné sítě[2]	informační systémy KII[3]	komunikační systémy KII[4]	významné IS[5]
Hlásit kontaktní údaje	ano	ano	ano	ano	ano
Detekovat kybernetické bezpečnostní události		ano	ano	ano	ano
Hlásit kybernetické bezpečnostní incidenty		ano	ano	ano	ano
Zpracovávat bezpečnostní dokumentaci a zavádět bezpečnostní opatření			ano	ano	ano
Provádět opatření vydaná NBÚ			ano	ano	ano

[1] Poskytovatelé služeb elektronických komunikací a subjekty zajišťující sítě elektronických komunikací.

[2] Subjekty zajišťující významné sítě.

[3] Správci informačních systémů zařazených do kritické informační infrastruktury.

[4] Správci komunikačních systémů zařazených do kritické informační infrastruktury.

[5] Správci významných IS.

4.4. Dopady na podniky nepodléhající zákonu

Tvůrci vyhlášky o kybernetické bezpečnosti se inspirovali některými částmi norem řady ISO/IEC 27000, v kybernetickém zákonu lze najít dokonce i souhlasné body. Pokud tedy některá organizace má již platný certifikát ISO/IEC 27001, měla by již splňovat zásadní požadavky zákona o kybernetické bezpečnosti. Organizace podléhající zákonu o kybernetické bezpečnosti musí dále řešit např. komunikaci s národním CERTem ohledně kontaktních údajů a hlášení kybernetických incidentů.

„Kybernetická bezpečnost není záležitostí zákona o kybernetické bezpečnosti, ale spíše pudu sebezáchovy té konkrétní instituce. Informační systémy obsahují spoustu informací, které jsou velmi důležité pro chod fungování instituce, firmy, státu. Kdo si myslí, že v okamžiku, kdy nespadá pod působnost zákona o kybernetické bezpečnosti, že tyto věci nemusí řešit, tak tomu přeju hodně štěstí.“ (Špidla, 2014) Bylo by tedy vhodné, aby podniky nepodléhající zákonu o kybernetické bezpečnosti, měly alespoň povědomí o tomto zákonu a nějakým způsobem se z něho inspirovali.

Dalším faktorem je to, že organizace podléhající zákonu o kybernetické bezpečnosti řeší v rámci tohoto zákona i své dodavatele. Pokud je některá organizace nebo podnik dodavatelem nebo provozovatelem systému, který podporuje například prvek kritické infrastruktury (a nepodléhá zákonu o kybernetické bezpečnosti), budou na něj kladeny požadavky na udržení určité úrovně bezpečnosti.

Podniky a organizace nejspíše budou také využívat služeb významných informačních systémů, případně kritické infrastruktury, což může vést k dalším bezpečnostním opatřením využívajícím například šifrování, digitální certifikáty a podobně.

V neposlední řadě také organizace nepodléhající zákonu může bezpečnostní incident sama způsobit, bude tedy kontaktována národním CERTem za účelem odstranění chyb.

4.5. Hlášení kybernetického bezpečnostního incidentu

V rámci zákona o kybernetické bezpečnosti byla definována dvě pracoviště pro nahlašování kybernetických bezpečnostních incidentů.

Vládní CERT České republiky (GovCERT.CZ). Jeho provozovatelem je Národní centrum kybernetické bezpečnosti (NCKB), které je součástí Národního bezpečnostního úřadu (NBÚ). Úlohou centra je koordinace spolupráce na národní i mezinárodní úrovni při předcházení kybernetickým útokům i při návrhu a přijímání opatření při řešení incidentů i proti probíhajícím útokům. (NCKB, 2011)

Dalším je národní CERT. Tuto roli v současné době plní tým CSIRT.CZ. Ten přijímá kontaktní údaje od orgánů a osob uvedených v § 3 písm. a) a b) a hlášení kybernetických bezpečnostních incidentů od orgánů a osob uvedených v § 3 písm. b) zákona o kybernetické bezpečnosti.

Obě pracoviště jsou povinna přijímat od povinných orgánů a osob definovaných v § 3 zákona o kybernetické bezpečnosti informace o kybernetických bezpečnostních incidentech a také kontaktní informace daných subjektů. (CSIRT, 2015)

5. Využití penetračních testů pro detekci zranitelností

Dle normy ISO/IEC 27002 (ÚNMZ, 2014, s. 72) je třeba informační systémy pravidelně přezkoumávat z hlediska souladu s politikami a normami bezpečnosti informací organizace. Toto přezkoumávání lze provádět bezpečnostními testy, které by se měly opakovat v nějakých periodách. To jaké testy a jak často budou opakovány, nám může stanovit například politika bezpečnosti organizace (dokument vypracovaný v souladu s bezpečnostními požadavky organizace a normou ISO/IEC 27001). Dále je vhodné výsledky testů zpracovat tak, aby byly mezi sebou (jednotlivými periodami) porovnatelné, či ještě lépe měřitelné dle stanovených metrik. Jak již bylo zmíněno v kapitole 3.4.2., penetrační testování je jednou z vhodných metodik pro opakovanou detekci slabých míst bezpečnosti informací.

5.1. Vybrané pojmy

Etický hacker (white hat)

Úkolem etického hackera je najít slabá místa informačního systému a posoudit, jak by je případný útočník dokázal zneužít. Této práci se říká penetrační testování. (Harris et al., 2008, s. 30)

Cracker (black hat)

Opakem etického hackera je cracker, který se snaží narušit bezpečnost, zneužít informace nebo poškodit informační systém organizace.

Šedý hacker (gray hat)

Cílem šedého hackera je, podobně jako u crackera, určitým způsobem narušit bezpečnost informačního systému, ale bez úmyslu škodit. Šedý hacker většinou oznámí nález bezpečnostního problému administrátorovi nebo výrobci software a nabídne (třeba za poplatek) podrobné informace či odstranění chyby. (Harris et al., 2008, s. 30)

Script kiddie

Script kiddie je nekvalifikovaný a technicky méně zdatný než opravdový hacker. Vyznačuje se používáním skriptů nebo programů, které vyvinuli opravdoví odborníci k útokům na počítačové systémy a sítě.

Exploit

Exploity jsou speciální programy nebo skripty, umožňující neoprávněným způsobem získat přístup do systému nebo počítače, či nežádoucí instalaci škodlivého software. Souvisejícím pojmem je Zero day attack, což je pokus o zneužití chyby, která ještě není obecně známá.

Černá skříňka (black box)

Při použití testů černé skříňky není k dispozici přístup k programovému kódu. Software si pak lze představit jako černou skříňku, jejíž obsah není zvenčí viditelný. Neznáme tedy, jak přesně systém pracuje s daty, můžeme pouze sledovat, jaký výsledek získáme na výstupu. (Hlava, 2011)

Bílá skříňka (white box)

Opakem je použití testů bílé skříňky, kde je k dispozici zdrojový kód a vnitřní struktura software. Můžeme otestovat všechny průchody zdrojovým kódem nebo testovat zadávání neočekávaných vstupních hodnot, případně provádět jiné testy přímo na zdrojovém kódu. (Hlava, 2011)

5.2. Metody testování

Cílem níže uvedených metod je etickým způsobem odhalit možné narušení bezpečnosti síťové infrastruktury. Metody by měly simulovat skutečné postupy a způsoby, které by mohl použít opravdový útočník s cílem poškodit organizaci (či zneužít její informace). Proto by se při výběru některé z metod neměla klást zbytečná omezení, ale naopak snažit se využít i postupy a způsoby metody jiné.

V rámci testování je zmiňován takzvaný holistický přístup, což znamená, že se testování dynamicky přizpůsobuje zjištěným informacím a nalezeným zranitelnostem. Díky tomu získává organizace širší pohled na zabezpečení své infrastruktury.

5.2.1. Hledání slabých míst (vulnerability assessment)

Jde o metodu obvykle prováděnou pomocí různých nástrojů pro automatické skenování (Nessus, Retina, Internet Security Scanner, adt.), které otestují porty a služby na stanoveném bloku IP adres. Výsledky mohou odhalit typ a verzi operačního systému a aplikací, nainstalované bezpečnostní záplaty, data SNMP (protokol určený ke sběru dat pro potřeby správy sítě) nebo dokonce seznam uživatelských účtů. Tyto získané informace se porovnají s databází příslušného softwaru nebo jinou databází obecně známých slabých míst. Tam lze nalézt podrobnější popis bezpečnostních potíží dané verze a odpovídající obranu, která by měla vést k jejich odstranění. Hledání slabých míst je tedy ideální pro odhalení základních bezpečnostních problémů informačního systému. (Harris et al., 2008, s. 30)

5.2.2. Penetrační testování (pen testing)

Penetrační testování je příležitostí pro kouzla etického hackera. Nalezené chyby, pomocí hledání slabých míst, je možné přezkoušet a odhalit tak skutečná rizika. Etický hacker může využít všechny možné prostředky k tomu, aby proniknul do informačního systému organizace. Během penetračního testování se etický hacker snaží získat přístup do libovolného informačního systému, a pak dál do celé organizace. Jeho cílem je získat přístup do co nejvíce systémů, přístup s nejvyšším oprávněním nebo přístup k co nejcitlivějším informacím.

Hledání slabých míst má za úkol najít seznam všech zneužitelných chyb. Penetrační test by měl organizaci ukázat, jak by tyto chyby dokázal zneužít skutečný útočník. Výsledky penetračních testů by také měly obsahovat rady, jak riziko spojené

s jednotlivými chybami snížit a zvýšit bezpečnost celého informačního systému. (Harris et al., 2008, s. 31)

Penetrační testy se dají rozdělit na dvě kategorie. První jsou externí penetrační testy. Ty si kladou za cíl prověřit bezpečnost internetového připojení a všech služeb dostupných z internetu. Mezi ně patří webové stránky včetně jejich služeb (registrace, e-shop, atd.), poštovní server, FTP server a další. Snaha je o průnik z vnějšku do vnitřní síťové infrastruktury.

Druhou kategorií jsou interní penetrační testy, ty prověřují bezpečnostní politiky a mechanizmy organizace, které mají za úkol zamezit zaměstnancům (hostům, útočníkům) v neoprávněném přístupu a zneužití dat. Prověřují se zde nejen úmyslné pokusy jak získat důležitá data, ale i možnosti zcela náhodného přístupu k citlivým datům.

Vypracované metodiky, které se zabývají penetračním testováním, jsou dostupné například v rámci The Open Source Security Testing Methodology Manual (OSSTMM), metodik National Institute of Standards and Technology (NIST) nebo metodik Německé národní autority (BSI).

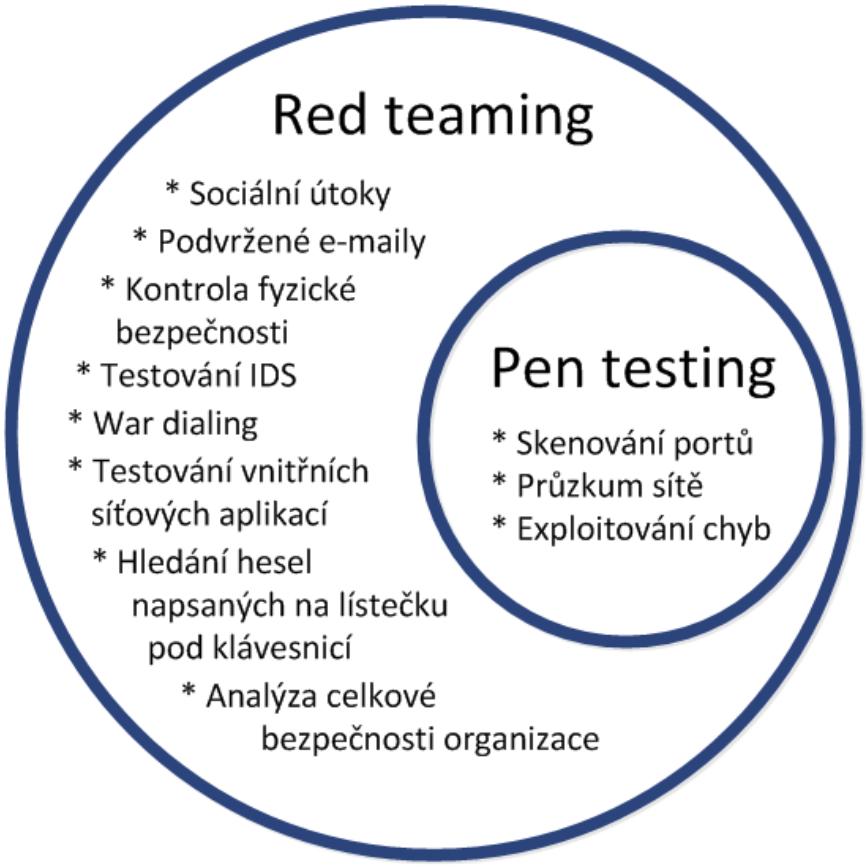
5.2.3. Red Teaming

Penetrační testování ukazuje, jak hluboko je schopen se útočník do síťové infrastruktury dostat. Red teaming je v podstatě širší pohled na hledání cest dovnitř organizace. Název „red teaming“ nemá český ekvivalent, je ale možné ho vysvětlit takto: červený tým (red team) je odvozený od armády, v žargonu se dobrá strana nazývá modrý tým a nepřítel červený tým, red teaming je tedy jinými slovy simulace nepřítele. Aby taková simulace byla věrohodná, neměl by červený tým dostat od zadavatele testů žádné výhody (informace, přístup k počítačové zásuvce, atd.).

Způsoby, jak červený tým získá přístup do sítě, nejsou nijak omezeny. Může mezi ně patřit podvodný e-mail obsahující formulář, který žádá o prověření síly vašeho hesla nebo jeho změnu hesla z důvodu expirace (podvržené e-maily). Nebo

telefonát do firmy na ekonomické oddělení, kde útočník vystupuje v pověření majitele a žádá o finanční přehledy (war dialing). Nebo se člen týmu může vydávat za technika povolaného k servisnímu zásahu v serverovně (kontrola fyzické bezpečnosti). Těmto typům útoků se říká sociální útoky. (Harris et al., 2008, s. 90)

Dalším způsobem, jak prověřit bezpečnost, je testování IDS (systém pro monitorování síťového provozu za účelem odhalení podezřelých aktivit), kde nápadným chováním jako je skenování sítě, kopírování většího množství dat do internetu nebo jinými aktivitami se bude útočník snažit o své odhalení. (Harris et al., 2008, s. 90)



Obr. 1: Red teaming a pen testing. Zdroj: upraveno autorem dle (Harris et al., 2008, s. 84).

5.2.4. Systémové testy

Tyto testy se od penetračních testů a red teamingu liší především tím, že se často soustředí jen na jeden systém nebo aplikaci. Navíc nesledují předem daný proces testování a vyžadují více nápadů daného etického hackera či testera. Systémové testy mají dvě části, ohledání povrchu (surface enumeration) a cílené zneužití nalezených slabých míst.

Při ohledání povrchu se nejdříve označí všechna místa, kde se systém dostává do styku s vnějšími daty. To je třeba provést velmi pečlivě, protože se od toho odvíjí celý zbytek testu. Součástí ohledání je instalace a běžný provoz systému (či aplikace). Při instalaci se sledují akce prováděné během instalačního procesu a stav systému bezprostředně po instalaci v porovnání se stavem v průběhu provozu. Dále se sleduje vlastní chování systému a nakonec (podobně jako u instalace) se sleduje proces odinstalace.

V druhé fázi je potřeba nalezená slabá místa zneužít. Zde přijdou vhod zkušenosti a schopnosti etického hackera (chceme-li systémového testera). Mezi způsoby může patřit útok přes soubory či databázi, útok přes registry, útok přes pojmenované roury (komunikační prostředek mezi jednotlivými procesy operačního systému), útoky přes slabá ACL (access control list, česky „seznam pro řízení přístupu“) a síťové útoky. (Harris et al., 2008, s. 93)

Tyto testy lze provádět z pohledu černé a bílé skříňky (pojmy z kapitoly 5.1). Aby byl správně daný systém otestován, měly by být testy velmi precizně provedené. Navíc zpracování výsledků může být poměrně zdlouhavé. Nevýhodou systémových testů je tedy časová náročnost, vysoké nároky na odbornost a u rychle se vyvíjejících systémů potřeba častého testování nových verzí.

Pro podporu vývoje a nasazování aplikací byla založena v roce 2001 komunita bezpečnostních odborníků Open Web Application Security Project (OWASP), jejímž cílem je napomáhat tvorbě programového vybavení, které je funkční a zároveň splňuje bezpečnostní standardy zajišťující poskytování aplikace a bezpečnost dat.

5.3. Příprava a průběh penetračního testování

Vzhledem k tomu, že penetrační testování je specializovaná činnost vyžadující hlubší znalosti a schopnosti v oblasti prověřování bezpečnosti IT infrastruktury a úzce souvisí s hackingem, je často vhodné pro tyto testy najmout specializovanou firmu. Při provádění testů se zaměstnanci této firmy mohou dostat k citlivým datům prověřované organizace nebo při špatném jednání dokonce ohrozit správné fungování některého systému. Je tedy třeba správně stanovit hranice a podmínky průběhu testování, stejně tak mít povědomí o možných rizicích vyplývající se zákona.

5.3.1. Právní rámec penetračního testování

Zákon č. 40/2009 sb.

1.1.2010 nabyl účinnosti trestní zákon č. 40/2009 Sb. Hlava V. tohoto zákona se týká trestných činů proti majetku, napadení sítě, což je bráno jako majetková trestná činnost. Ačkoli data nepředstavují hmotný majetek, poškození dat může vést ke ztrátě hmotného majetku.

§230 se zabývá neoprávněným přístupem k počítačovému systému a nosiči informací a řeší trestnou činnost v průběhu napadení. Jeho úkolem je řešit situace, kdy útočník napadne síť a způsobí škodu, informace dále nezneužije.

§231 pojednává o opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat. Jde o doplněk k předchozímu §230, který ošetřuje případy, kdy útočník zneužije neoprávněně získané informace nebo je poskytne třetí osobě. Řeší také poškození záznamu v počítačovém systému a na nosiči informací i zásah do vybavení počítače z nedbalosti, způsobené zanedbáním pravidel. (*Legislativní pohled*, 2010)

Zákon č. 101/2000 Sb.

1.1.2015 vyšlo v platnost nové znění zákona o ochraně osobních údajů. Jedná se o základní právní předpis upravující ochranu osobních údajů a činnost Úřadu pro ochranu osobních údajů. Zákon reflektuje Listinu základních práv a svobod, pro ochranu občana před neoprávněným zásahem do jeho soukromého a osobního života neoprávněným shromažďováním, zveřejňováním nebo zneužitím osobních údajů. S rostoucím vlivem informačních technologií je toto právo stále více narušováno. (Česko, 2000)

Další zákony

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti (podrobněji v kapitole 4.).

Zákon č. 127/2005 Sb., o elektronických komunikacích.

Zákon č. 89/2012 Sb., občanský zákoník, §504 Obchodní tajemství a §2985 Porušení obchodního tajemství

Zákon č. 121/2000 Sb., autorský zákon, §58 Zaměstnanecké dílo

5.3.2. Postup tvorby

V rámci příprav je vybrána vhodná firma pro provedení penetračních testů, třeba dle stanovených kritérií výběrového řízení (odbornost, cena, reference, osobní jednání, atd.). S touto firmou se podepíše smlouva a dohoda o mlčenlivosti. Následuje plánování a upřesnění rozsahu, způsobu a hloubky testování.

Vlastní testování by mělo probíhat, pokud možno, mimo běžnou pracovní dobu organizace a dle konkrétního časového plánu. Pracovník provádějící penetrační testy (v roli etického hackera) by měl úzce komunikovat s pověřeným zaměstnancem organizace a předem ho informovat jaké systémy a kdy hodlá testovat. Po otestování si oba musí odsouhlasit, že nedošlo k nežádoucím chybám nebo poruchám na testovaném systému.

Po dokončení testů se provádí vyhodnocení, jehož výsledkem je technická zpráva. Ta se spolu s doporučením bezpečnostních opatření předá organizaci (zadavateli).

Pro bezpečnostního pracovníka stanoveného organizací je řádné provedení všech výše uvedených fází nezbytné. Po nasazení bezpečnostních oprav a opatření v organizaci je také vhodné penetrační testy zopakovat a porovnat s předchozími výsledky nebo ještě lépe penetrační testy provádět ve stanovených periodách (dle potřeb organizace, např. jednou ročně).

Na druhé straně, etický hacker nesmí zákazníka kvůli bezpečnostním nedostatkům žádným způsobem ztrapňovat nebo zesměšňovat. Právě kvůli těmto nedostatkům byl do organizace pozván, je v ní hostem a jeho úkolem je vyřešit problém. Penetrační tým by navíc neměl získaná citlivá data číst, aby se předešlo případným právním žalobám ohledně vynášení důvěrných informací. (Harris et al., 2008, s. 31)

5.3.3. Způsoby a nástroje

Skenování

V podstatě jde o proces odeslání dotazů (sondy) – poznačení co a kam jsme poslali – čekání na to, jestli přijdou nějaké návratové informace a co budou obsahovat. Na vstupu se definuje rozsah sítě pro skenování, případně rozsah portů nebo další kritéria (UDP nebo TCP, ping scan nebo no ping scan, atd). Výstupem je seznam IP adres, které odpověděly včetně portů a dalších informací dle použitého skenu.

Nejznámějším nástrojem je nmap (Windows) nebo zenmap (Linux). Velmi používaným nástrojem je balík Paketto Keiretsum, který obsahuje scanrad pro rychlé skenování TCP portů (náhrada za traceroute), minewt pro směrování a překlad adres, linkcat pro svoje široké použití (skener portů, telnet, a další), paratrace jako schopná náhrada za traceroute (umí obejít stavové filtry) a phentropy na grafické zpracování dat. (Harris et al., 2008, s. 104)

Identifikace OS a síťových služeb

Pro identifikaci operačního systému se obecně používají dva přístupy, pasivní a aktivní. Pasivní přístup sleduje pakety, které běhají po síti a snaží se z nich zjistit, jaký operační systém by je mohl posílat. Jedná se o nejméně nápadnou metodu, na druhé straně je potřeba se nabourat do nějakého počítače, přes který tento odposlech bude možné provádět. Používaným nástrojem je například p0f.

Aktivní přístup spočívá v tom, že se odesílají data cílovému počítači a analyzují se jeho odpovědi. V síti je však toto chování odhalitelné pomocí IDS (Intrusion Detection System) nebo IPS (Intrusion Prevention System), proto je třeba opatrnosti a dotazy takovéhoto charakteru nezahltit celou síť. Informace o operačním systému lze odhalit podle standardně otevřených portů (výchozí instalace OS), nebo lépe dle spuštěných síťových služeb programem amap. Také to lze pomocí dotazu, který vrátí zpět obvyklou reakci či hlášku typickou pro některý operační systém, případně podle parametrů TCP spojení nebo pomocí protokolu ICMP (Internet Control Message Protocol) programem xprobe2. (Harris et al., 2008, s. 116)

Odposlech sítě

Odposlech sítě je vlastně snaha o zachycení síťových rámců z nějakého síťového média. Anglicky se používá název packet capturing (zachytávání paketů), což je v podstatě nepřesné, protože jde o zachytávání rámců (druhá vrstva ISO/OSI modelu).

Stejně jako na identifikaci OS se dá na odposlech sítě pohlížet jako na pasivní a aktivní. Při pasivním odposlechu se síťový adaptér přepne do promiskuitního režimu, kdy zachytává vše, co může. To funguje dobře v sítích s rozbočovači (hub) a sběrnicovou topologií. Používají se pro to knihovny WinPcap (Windows) a libpcap (Unix).

V současné době jsou však již standardem sítě s přepínači (switch), kde se využívá takzvaný aktivní odposlech. Zde je k zachycení rámců potřeba odklonit síťový provoz, například pomocí falšování APR (Address Resolution Protocol) požadavků a odpovědí. To lze zajistit podvržením dvojicí IP adresa / MAC adresa do APR tabulky

cíle. Ten sice posílá data na správnou IP adresu, té ale odpovídá naše podvržená fyzická MAC adresa. Tento postup se nazývá APR cache poisoning (otrávení APR cache) a umožňují ho programy WinARP-sk, arpspoof a další. Odklonění síťového provozu jde také za pomoci DNS poisoningu (otrava DNS), což funguje nejen na sítích s přepínači, ale i na virtuálních sítích (VLAN) se směrovači (router). Zde je nejlepším řešením otrávit překlad mezi kvalifikovanými doménovými jmény (FQDN) a IP adresami v DNS cache počítače. K tomu se využívají třeba programy WinDNSSpoof (Windows) a dnsspoof (Unix). (Harris et al., 2008, s. 131)

Autentizace systému

Velmi výhodné je zneužít odposlechu sítě k získání autentizačních informací. Protokoly zajišťující autentizaci Windowsových a Unixových systémů jsou NTLMv2 (NT LAN manager, verze 2), určený primárně pro Windows NT a SMB (Server Message Block) a protokol kerberos (Windows 2000 a novější). U všech autentizačních mechanizmů je velmi důležitá (mimo jiné) délka hesla a abeceda, ze které je heslo sestaveno. Například prolomení hesla o délce čtyř znaků a využívající pouze malá písmena, může trvat několik sekund, zatímco prolomení hesla o osmi znacích, využívající všechny běžné znaky klávesnice (malá, velká písmena, číslice a další znaky jako je tečka, zavináč, a tak dále) může trvat několik měsíců.

Novější autentizeční protokol kerberos lze prolomit třeba programy kerbsniff a kerbcrack. Kerbsniff sleduje síťový provoz a zachytává hesla, ty pak ukládá do souboru. Program kerbcrack je z tohoto souboru čte a pomocí slovníkového útoku (uhodnutí hesla pomocí seznamu slov) nebo hrubou silou (testování kombinací znaků) se snaží hesla zlomit.

Hesla také bývají často uložena v takzvané hešované (hash) podobě. Heš je v podstatě "zašifrovaný" otisk hesla. Použitím útoku brutální silou lze i z této heše získat původní heslo. Tento útok spočívá v tom, že se postupně zkouší generovat slova, ty se hešují a porovnávají se zachycenou heší, to je ale velmi zdlouhavé. Jednodušší je využít duhové tabulky (rainbow tables), které jsou dostupné na internetu a na zaslanou heš vrátí (pokud jí znají) už odpovídající heslo. (Harris et al., 2008, s. 142)

Automatické penetrační testování

Pro snadnější a rychlejší přípravu penetračních testů se dnes často využívají specializované programy. Nejpoužívanější jsou Nessus (open software od Tenable Network Security), Retina (výrobce eEye Digital Security), ISS Security Scanner (výrobce Internet Security System) a OpenVAS. Výsledky testů provedené programem Nessus jsou součástí kapitoly 6.

Sofistikovanějším a opravdu komplexním nástrojem pro penetrační testování, je program Core Impact Pro (výrobce Core Security Technologies). Pomocí výše zmíněných programů lze nalézt chyby v síťové infrastruktuře, informace o tom jak je zneužít a doporučení, jak chyby odstranit nebo jinak zabezpečit. Core Impact jde ještě o něco dále, pomocí něho se dají provádět pokusy o reálné zneužití. To je nejlepší způsob, jak prověřit, že díky nalezené chybě je systém opravdu napadnutelný. Pro práci s Core Impact je zapotřebí znát alespoň základy skriptovacího jazyka Python, který je zapotřebí především ke tvorbě a úpravám exploitů. (Harris et al., 2008, s. 155)

5.4. Využití penetračního testování

Obecný pohled na informační bezpečnost zahrnuje vznik informace, zpracování, ukládání, přenos a její likvidaci, přičemž informace může být uložena v informačním systému nebo třeba vytištěna na papíře. V této rovině se nabízejí řešení, jako jsou implementace ISO/IEC 27001 nebo plnění požadavků zákona o kybernetické bezpečnosti.

Během řešení informační bezpečnosti je třeba informační systém nějakým metodickým postupem ohodnotit a otestovat. Tady přichází na řadu bezpečnostní audit, jehož součástí by měly být právě penetrační testy. „Žádná jiná metoda nedodá takové množství informací o možnosti průniku jako metoda: uvažujte a konejte jako útočník.“ (Přibyl, 2010). Díky těmto testům by tedy organizace měla zjistit, jak předejít nebo se ubránit případným útokům. To jsou nesporné výhody této metody.

Příklady rizik, které lze odhalit penetračními testy:

- Nedodržování platných standardů (RFC, W3C, ISO)
- Nedůsledná konfigurace zařízení (povoleny zbytečné/nevyužité síťové služby, slabé šifrování)
- Nevyhovující topologie systému
- Neznalost managementu
- Nepořádek

Příklad dopadů:

- Ztráta dobré pověsti organizace
- Porušení důvěrnosti informací
- Právní postih v případě zneužití/znehodnocení informací
- Ztráta zakázky
- Ušlý zisk během odstávky systému (Vymazal a Richter, 2012)

Přestože provedením penetračních testů získáme mnoho užitečných informací, nezahrnují všechny aspekty informační bezpečnosti. Oproti red teamingu třeba neřeší fyzickou bezpečnost, nejsou dostatečně universální pro vývoj aplikací a mohou být až příliš sofistikované pro prověřování méně potřebných síťových služeb. Pohled na organizaci očima hackera je tedy jistě velmi účinný, ale ne všeobsahující.

6. Analýza bezpečnostních rizik ve firemním prostředí

Žádná firma není izolována od zbytku světa. Naopak existuje v dynamickém prostředí trhu, kde na ní neustále působí mnoho pozitivních i negativních vlivů. Tyto vlivy potom určují směr vývoje a úspěšnost firmy. Důležité je, aby firma o těchto vlivech věděla a dokázala se s nimi vypořádat. Za tímto účelem se používá analýza rizik. Analýza v této kapitole byla vypracována na základě informací získaných od Čermáka (2013), Šutáka a Macka (2008).

Obr. 2: Risk analýza. Zdroj: upraveno autorem dle (Čermák, 2013).

Pro odhalení rizik jsou vybrány dvě metody. Pomocí definice hrozeb a zranitelností a jejich následné syntézy je sestavena SWOT analýza, která odhalí rizika z pohledu IT. Druhou metodou je penetrační testování, které je provedeno z pohledu hackera. To odhalí zranitelnosti a následně i rizika vyplývající z případného útoku. Na závěr dojde k hodnocení rizik (kapitola 6.4) a doporučení pro zavedení některých opatření (kapitola 7).

6.1. Představení společnosti a strategické cíle

Analýza bezpečnostních rizik je provedena v prostředí reálné společnosti. Protože jsou v této práci zveřejněny citlivé informace společnosti a aby byla zaručena prevence proti případnému zneužití, bylo vedením společnosti rozhodnuto nezveřejňovat v této práci název a vodítka vedoucí k podniku. Dále bude tedy společnost nazývána jako „podnik XY".

Podnik XY je významnou českou výrobní společností, která spadá do kategorie středně velkých firem do 1000 zaměstnanců. Podnik má ve svém oboru velmi dobré postavení na českém a slovenském trhu (2. nejvyšší produkce výrobků) a poměrně dobré postavení na evropském trhu. Produkce výrobků je cílena na zákazníka, podnik je tedy schopen poměrně pružně reagovat na zákazníkova přání.

Podnik XY je umístěn do jedné lokality, ta není významně ohrožena riziky spojenými se špatnou infrastrukturou a živelnými katastrofami. Má také dobré zázemí v holdingu, což představuje silný potenciál pro finanční i obchodní strategie.

Strategické cíle

Jedním z hlavních strategických cílů vedení společnosti je vybudovat z podniku XY předního výrobce na evropském trhu a být perspektivním zaměstnavatelem opravdových profesionálů. Chce produkovat kvalitní výrobky a poskytovat kvalitní služby zákazníkům, proto management společnosti vydává politiku jakosti, cíle jakosti a vytváří potřebné zdroje, které jsou orientovány na výcvik a vzdělávání pracovníků, rozvoj infrastruktury, management pracovního prostředí a rozvoj systémů měření. Účinnost systému je vedením pravidelně přezkoumávána.

Podnik XY je od roku 2001 držitelem certifikátu kvality ISO 9001. Výrobky jsou funkčně i designově průběžně modernizovány s ohledem na požadavky zákazníků a neustále se zvyšujícího standardu bezpečnosti a kvality.

6.2. SWOT analýza podnikové IT bezpečnosti

SWOT analýza je nástroj strategického plánování. Vytváří přehled o strategické situaci podniku dle interních a externích schopností firmy. Kategorizuje vnitřní silné a slabé stránky, vnější příležitosti a hrozby podniku a řadí je dle důležitosti. Na základě takového hodnocení je možné určit, co by mělo být učiněno pro to, aby firma dosáhla svých cílů. SWOT je zkratka Strenght (síla), Weakness (slabosti), Opportunity (příležitost), Threat (hrozba). Kapitola využívá postupů dle metodiky Sakála (2010, s. 5-14) a Businessballs (2012).

6.2.1. Rozsah a cíle analýzy

Rozsah analýzy

SWOT analýza je zaměřena na firemní prostředí podniku XY. Jejím předmětem výzkumu je vztah informačních technologií a bezpečnosti informací. Rozsah analýzy je tedy dán firemním prostředím (kapitola 6.1) a předmětem analýzy. Z důvodu komplexnosti není dále limitován.

Cíle analýzy

- Poskytnout manažerský logický rámec pro hodnocení současné situace,
- definovat slabé stránky podnikové bezpečnosti (kapitola 6.2.2.),
- odhalit možná rizika a kategorizovat je (kapitoly 6.2.4. a 6.4.),
- získat konkrétní cíle vedoucí ke zlepšení bezpečnosti informací (kapitola 7).

6.2.2. Podmínky SWOT analýzy

Definici podmínek SWOT analýzy je potřeba věnovat zvláštní pozornost a snažit se odhalit všechny aspekty, které mohou předmět SWOT analýzy nějakým způsobem ovlivňovat, na tomto závisí výsledná kvalita analýzy.

Silné stránky (strenght)

Jedná se o vnitřní pozitivní podmínky, které umožňují podniku získat převahu nad konkurencí. Předností podniku je kompetence a zdroje, které umožňují podniku získat konkurenční výhodu. Do této kategorie spadají kvalitnější používané metody, dobré finanční postavení a vztahy s dodavateli či odběrateli, vyspělé technologie, funkční individuální řešení, distribuční kanály, nebo vysoká odbornost pracovníků či vyspělý tým manažerů.

Slabé stránky (weakness)

Slabosti nebo také nedostatky jsou vnitřní podmínky, které mohou vést k nižší výkonnosti podniku. Slabostí je třeba nedostatek či absence určitých zdrojů a schopností, neznalost nebo nezpůsobilost zaměstnanců, špatná komunikace uvnitř podniku nebo chyba v rozvoji důležitých zdrojů.

Příležitosti (opportunity)

Příležitosti jsou vnější současné nebo budoucí podmínky v prostředí, které jsou příznivé současným nebo potencionálním výstupům podniku. Tyto příznivé podmínky mohou být jakékoliv příležitosti ke zvýhodnění, změny v zákonech, zvyšující se počet potencionálních zákazníků nebo potřebných odborníků, uvedení nových technologií. Posuzování důležitosti příležitostí je třeba provádět z pohledu dlouhodobého vývoje prostředí a jeho vlivu na podnik.

Hrozby (threat)

Externí současné nebo budoucí podmínky v prostředí, které jsou nepříznivé současným nebo budoucím výstupům podniku. Mohou obsahovat vstup nebo rozvoj silného konkurenta na trhu, odchod odborníků z řad zaměstnanců, nepříznivé změny v legislativě, ohrožení dodávek, zvýšení kybernetického nebezpečí a podobně.

Tab. 3: Podmínky pro bezpečnost IT v podniku XY. Zdroj: autor.

	Pozitivní	Negativní
Vnitřní	**Silné stránky (S)**	**Slabé stránky (W)**
	+ silné finanční zázemí holdingu + roční investiční plánování + možnost operativního schválení investice v případě nouze + funkční informační systém ERP + flexibilní prostředí pro servery a zálohy + propojení výrobních strojů na podnikové IT + systém počítačových kiosků na výrobě + webový přístup servisů do ERP + e-shop pro prodej náhradních dílů + elektronický webový katalog + know-how IT pracovníků + kompetence IT k řízení menších projektů + schopnost tvořit programové úpravy v ERP + funkční řízení přístupů k datům v ERP (CRM, SCM, Výroba, Ekonomika, Mzdy, E-moduly) + specializovaná školení konstruktérů	- nepoužívaný SW pro správu dat konstrukční dokumentace - nedostatečné řízení přístupu ke konstrukční dokumentaci - absence záložní serverovny - absence politiky IT bezpečnosti - chybějící popis firemních procesů - zastaralé řízení podnikové domény - absence IDS - outsoursing pro doménu, mailserver, podnikový firewall a VPN - závěsná páteřní optika směr nákup, sklady a výroba - nedostatečná fyzická bezpečnost - vytížení IT oddělení - absence pravidelných školení zaměstnanců - neúplná dokumentace strukturované kabeláže
Vnější	**Příležitosti (O)**	**Hrozby (T)**
	+ zákon o kybernetické bezpečnosti + implementace ISO/IEC 27001 + zvyšující se IT gramotnost absolventů škol + technologie podnikové sociální sítě + dostupná tablet PC jako náhrada statických počítačových kiosků + podpora QR kódů v ERP + nový mobilní klient v ERP + sofistikovaná technologie Safetica + zrychlení a zjednodušení přechodu na Active Directory + projektové nebo procesní řízení + systém pro plánování výrobních kapacit + implementace DMS a worflow v ERP + zlevňování a zkvalitňování cloudových služeb	- ohrožení dodávek nebo výrazné zdražení IT zdrojů - nepřipravenost na rychlý růst podniku - únik nebo ztráta citlivých dat podniku - únik osobních informací zaměstnanců - odchod odborníků z řad zaměstnanců - útok pomocí virů a malwarů - sociální útoky (phishing, war dialing, atd.) - záměrné i nevědomé útoky na síťovou infrastrukturu (kolize IP s routerem, nepovolené DHCP, chybné DNS nebo WINS, přehlcení sítě pakety, atd.) - časté nebo dlouhodobé výpadky elektřiny - přepětí v el. síti způsobené bleskem - přerušení dodávky nebo výpadek WiFi spoje do internetu - živelná katastrofa

Jednotlivým podmínkám je možné přiřadit i ocenění důležitosti a porovnáním celkového počtu „bodů“ podtabulek získat vektor současné strategie. To je ale vhodné jen tehdy, pokud lze podmínky měřit nebo jinak objektivně ohodnotit (např. cena, důležitost, analýza dopadů, výpadek cost, a podobně).

Tématem SWOT analýzy je vztah informačních technologií k bezpečnosti informací, což nabízí široké možnosti definovat pozitivní i negativní podmínky. Některé body je vhodné popsat podrobněji:

- Roční investiční plánování podléhá pravidlům podnikové politiky, umožňuje oddělením jednat bez potřeby dalšího schvalování.
- Flexibilní prostředí pro servery a zálohy představuje VMware a Veeam. To přináší výhody technologie virtualizace, jako je přidělování HW prostředků více virtuálním strojům, přesuny serverů mezi HW, repliky, testovací prostředí, sofistikované zálohování, atd.
- Nepoužívaný SW pro správu dat konstrukční dokumentace je implementovaný databázový systém, který z důvodů časové vytíženosti nebylo možné uvést do ostrého provozu. Prozatím konstrukční data zůstávají v adresářové struktuře, která má nedostatečné řízení přístupů a další nedostatky.
- Absence politiky IT bezpečnosti představuje neexistence IT směrnic, postupů a pravidel. Vše je v současné době řešeno příkazem ředitele, s nímž se zaměstnanci seznámí pouze při nástupu do zaměstnání. Na ten navazuje jedna stručná směrnice pro definici nejzákladnějších potřeb, jako je síla hesel a rozdělení základních odpovědností mezi uživateli a pracovníky IT.
- Chybějící popis firemních procesů vyvolává nejasné dělení pracovních odpovědností, neefektivitu práce i plánování změn v procesech a špatné povědomí zaměstnanců o dění v podniku (pravá ruka neví, co dělá levá).
- Zastaralé řízení podnikové domény představuje starý systém, který slouží k základnímu ovládání linuxové podnikové „domény“. Tento

systém je již několik let neaktualizovaný a oproti moderním systémům morálně zastaralý.

- Nedostatečná fyzická bezpečnost umožňuje zaměstnancům vynášet data na přenosných médiích, přístup k nezamčeným počítačům a podobně.
- Absence pravidelných školení zaměstnanců má za následek horší povědomí zaměstnanců o efektivní práci s informačními technologiemi. Zaměstnanci dostávají pouze vstupní školení a školení na nové technologie.
- Zákon o kybernetické bezpečnosti a ISO/IEC 27001 je velkým zdrojem ponaučení, které se přímo zabývá IT bezpečností.
- Technologie podnikové sociální sítě je velmi moderní nástroj, který pomáhá překlenout informační bariéry mezi odděleními a zaměstnanci.
- Zrychlení a zjednodušení přechodu na AD (ActiveDirectory) představuje funkční interface mezi linuxovou doménou a AD pro migraci účtů a profilových dat.
- Projektové nebo procesní řízení podniku, stejně jako systém pro plánování výrobních kapacit a DMS (Document Management System), přispívají k vyšší efektivitě řízení a toku informací.
- Ohrožení dodávek IT zdrojů (HW, SW opravy, spotřební materiál, atd.) má přímý vliv na zabezpečení kontinuálnosti firemních procesů, proto se jedná o problém informační bezpečnosti.
- Přerušení dodávky internetu zapříčiní nedostupnost webových služeb, jako je přístup zaměstnanců a servisních středisek do ERP, e-shop pro prodej náhradních dílů, VPN. Na druhé straně znemožní funkci mailového serveru a obecně internetu.

6.2.3. Syntéza podmínek SWOT analýzy

Syntéza SWOT analýzy propojí vnější příležitosti a hrozby na vnitřní silné a slabé stránky podniku. Touto kombinací a napojením vzniká strategie, která pomáhá uvést podnik do souladu s okolními vlivy. Takto formulovaná strategie umožňuje podniku orientovat se jen na příležitosti, které odpovídají schopnostem podniku. Také pomáhá definovat, zmírnit dopady nebo se úplně vyhnout hrozbám, proti kterým se podnik v současné době nedokáže bránit. Podobným způsobem je syntéza využita i u dalších podmínek.

- Strategie SO (Strenght - Opportunity): využití příležitostí, technologií či metod pro rozvoj silných stránek. Tuto variantu volí podniky, které mají dostatek příležití a zdrojů. Označuje se jako ofenzivní strategie.
- Strategie ST (Strenght - Threat): použití silných stránek na obranu proti hrozbám. Pokud se jedná o silný podnik, který se nachází v prostředí s mnoha hrozbami, zvažují se možnosti eliminace hrozeb nebo přesun podniku do jiného prostředí. Této strategii se říká defenzivní strategie.
- Strategie WO (Weakness - Opportunity): překonání slabin využitím příležitostí, nebo odstranění slabin, pro vznik nových příležitostí. Strategii je vhodná, pokud chce podnik posílit a odstranit své slabiny.
- Strategie WT (Weakness - Threat): vývoj strategií pomáhající omezit hrozby, ohrožující slabé stránky. Ve vztahu k analýze rizik lze chápat slabé stránky jako zranitelnosti a strategii WT jako definici ohrožení.

Obr. 3: Definice ohrožení. Zdroj: upraveno autorem dle (Čermák, 2013).

Tab. 4: Syntéza SWOT analýzy bezpečnosti IT v podniku XY. Zdroj: autor.

		Vnitřní analýza	
Vnější analýza	Příležitosti (O)	**Silné stránky (S)**	**Slabé stránky (W)**
		Řeší + ZKB a ISO 27001 - roční in. plánování + ZKB a ISO 27001 - know-how IT + tablet PC - kiosky na výrobě + QR kódy - kiosky na výrobě + mobilní klient ERP - kiosky na výrobě + proj./proces. řízení - funkční ERP + plán. výr. kapacit - funkční ERP + DMS a worflow - funkční ERP + cloud. služby - servery a zálohy **Neřeší** - zvyšující se IT gramotnost absolventů - technologie podnikové sociální sítě - sofistikovaná technologie Safetica - přechod na Active Directory	**Řeší** + přístup ke kon. dok. - správa kon. dok. + absence z. server. - cloud. služby + absence politiky IT - ISO 27001 + popis procesů - procesní řízení + říz. domény - přechod na AD + outsoursing - přechod na AD + fyzická bezpečnost – Safetica **Neřeší** - absence IDS - outsoursing - závěsná páteřní optika - vytíženost IT oddělení - absence školení zaměstnanců - dokumentace strukt. kabeláže
	Hrozby (T)	**Silné stránky (S)**	**Slabé stránky (W)**
		Řeší + dod. IT zdrojů - záz. holdingu, inv. plánování, oper. schválení + rychlý růst - záz. holdingu, oper. schválení, felx. prostředí pro servery + odchod odborníků - zázemí holdingu + únik os. informací - řízení př. v ERP **Neřeší** - únik nebo ztráta citlivých dat podniku - odchod odborníků - útok pomocí virů a malwarů - sociální útoky - útoky na síťovou infrastrukturu - výpadky elektřiny - přepětí v el. síti zp. bleskem - výpadek internetu - živelná katastrofa	**Významně ohrožují** - dod. IT zdrojů - absence z. serverovny, outsoursing - rychlý růst - SW správy kon. dok., absence politiky IT, popis procesů, fyzická bezpečnost, vytížení IT oddělení, pravidelná školení, dok. str. kabeláže - únik citl. dat - řízení kon. dokum., absence politiky IT, zast. říz. domény, absence IDS, outsoursing pro doménu, fyzická bezpečnost - únik os. infor. - absence politiky IT, outsoursing, fyzická bezpečnost - útok viry - řízení kon. dokum., absence politiky IT, zast. říz. domény, absence IDS, vytížení IT oddělení, absence školení - sociální útoky - absence politiky IT, absence školení - útoky s. infras. - absence IDS, vytíženost IT - výpadky elektřiny - absence z. serv., absence politiky IT, vytíženost IT - přepětí bleskem - absence z. serv., absence politiky IT, vytíženost IT - výpadek internetu - outsoursing - živelná katastrofa - absence z. serv., absence politiky IT, vytíženost IT

Syntéza podmínek SWOT analýzy má úzký vztah k podniku XY a v této fázi je nezbytné okomentovat jednotlivá spojení a dále rozvinout zmíněné strategie.

Strategie SO (Strenght - Opportunity)

- ZKB a ISO 27001 - roční investiční plánování: získané znalosti ze zákona o kybernetické bezpečnosti a ISO/IEC 27001 vedou k fundovanější definici požadavků na investice do bezpečnostních opatření.
- ZKB a ISO 27001 - know-how IT pracovníků: znalost ZKB a ISO/IEC 27001 pomůže IT pracovníkům v mnoha aspektech IT bezpečnosti (více kapitoly 3. a 4.).
- Tablet PC - kiosky na výrobě: mobilní tablet PC opatřený čtečkou čárových a QR kódů může plně nahradit stacionární kiosek na výrobě.
- QR kódy - kiosky na výrobě: prověřené QR kódy mohou oproti čárovým kódům nést mnohem více informací včetně bezpečnostních prvků.
- Mobilní klient ERP - kiosky na výrobě: použití mobilního klienta na zařízeních typu tablet PC nebo smartphone zařídí bezpečnější komunikaci s aplikačním serverem ERP systému.
- Projektové a procesní řízení, plánování výrobních kapacit, implementace DMS a workflow - funkční ERP: metodiky řízení a plánování obecně mají příznivý vliv na čistotu a efektivitu toku informací v podniku nejen prostřednictvím ERP.
    - Cloudové služby - servery a zálohy: využití cloudových služeb přináší mnoho bezpečnostních výhod pro podnik. Patří mezi ně obvykle dobré IT zázemí (SW, HW, znalosti) poskytovatele služeb. Může nést ale také bezpečnostní hrozby, například výpadek konektivity do datového centra.

Strategie ST (Strenght - Threat)

- Ohrožení dodávek IT zdrojů - zázemí holdingu: síla holdingu podporuje postavení podniku na trhu a má příznivý vliv na dodavatelský řetězec obecně.

- Ohrožení dodávek IT zdrojů – roční investiční plánování: schválení ročního plánu investic umožňuje pravidelnou obměnu strojů, platbu SW licencí a plánování IT projektů.
- Ohrožení dodávek IT zdrojů – možnost operativního schválení investice v případě nouze: v případě vzniku významného neočekávaného problému lze projednat případnou investici do IT bez potřeby složitého schvalovacího procesu.
- Rychlý růst podniku – zázemí holdingu a operativní schválení investice: zvládnutí případného rychlého růstu podniku jistě velmi pomůže silné postavení holdingu na trhu, stejně jako možnost operativního schválení investice v případě nouze.
- Rychlý růst podniku – flexibilní prostředí pro servery a zálohy: VMware je velmi flexibilní prostředí a poskytuje široké možnosti rozšíření jak po výkonové, tak funkční stránce.
- Odchod odborníků - zázemí holdingu: finanční zázemí poskytuje možnost udržet si významné odborníky z řad zaměstnanců, kteří by mohli svým odchodem odnést část know-how podniku.
- Únik osobních informací - řízení přístupů v ERP: součástí ERP je dostatečně propracované a nakonfigurované řízení přístupů (práv) k osobním informacím, stejně tak jako k citlivým datům podniku (ty jsou však k dispozici i v jiném systému, který není dostatečně zabezpečen).

Strategie WO (Weakness - Opportunity)

- Nedostatečné řízení přístupu ke konstrukční dokumentaci řeší právě nepoužívaný SW pro správu dat konstrukční dokumentace.
- Absence záložní serverovny - cloudové služby: jedním z řešení, kam zálohovat důležitá firemní data, je cloudové úložiště.
- Absence politiky IT bezpečnosti – implementace ISO/IEC 27001: vlastní implementace ISMS obsahuje tvorbu politiky a cílů bezpečnosti informací (více kapitola 3).
- Chybějící popis firemních procesů - procesní řízení: procesnímu řízení předchází analýza firemních procesů.

- Zastaralé řízení podnikové domény - přechod na Active Directory (AD): systém řízení podnikové domény nemá již několik let k dispozici aktualizace, nasazení poslední verze AD představuje velký skok v modernizaci podnikové bezpečnosti.
- Outsoursing pro doménu, mailserver, firewall a VPN - přechod na AD: nasazením AD je možné přesunout podnikovou doménu pod správu podniku. Součástí toho by bylo vhodné provést i přesun a modernizaci mailserveru. Podnikový firewall a VPN však neřeší.
- Fyzická bezpečnost – Safetica: nedostatečnou fyzickou bezpečnost lze řešit například technologií Safetica, která umí třeba kontrolovat připojená externí úložiště, komunikaci po síti i mailem nebo reportovat chování zaměstnance.

Strategie WT (Weakness - Threat)

- Dodávky IT zdrojů - absence z. serverovny: v situaci, kdy nebude možné použít infrastrukturu stávající serverovny (například routery, switche, kabeláž), nelze použít jinou variantu. Podnik bude odkázán na flexibilitu dodavatelů.
- Dodávky IT zdrojů - outsoursing pro doménu: v případě potíží s podnikovou doménou je nutné kontaktovat dodavatele a čekat na jeho odezvu.
- Rychlý růst podniku - nepoužívaný SW správy konstrukční dokumentace: současné nedostatečné řízení přístupu ke konstrukční dokumentaci představuje riziko, které z velké části řeší specializovaný SW, který se však nepoužívá. Pokud by došlo k rychlejšímu růstu podniku, zprovoznění specializovaného SW pro správu dat by bylo daleko náročnější.
- Rychlý růst podniku - absence politiky IT: rychlý růst podniku představuje větší příliv zaměstnanců a více potencionálních potíží s bezpečností informačního systému a informací obecně. Předem připravená bezpečnostní pravidla, postupy a směrnice, stejně jako

reporting a konfigurace podléhající politice bezpečnosti (více kapitola 3), by celou situaci měla výrazně usnadnit.

- Rychlý růst podniku - popis procesů: chybějící popis procesů přímo znemožňuje efektivní změny v procesech informačního systému.
- Rychlý růst podniku - fyzická bezpečnost: při rychlém růstu podniku bývá kladen důraz na vlastní funkčnost podniku, to sebou nese krádeže, případně únik firemních dat.
- Rychlý růst - vytížení IT oddělení: příliš vytížené IT oddělení není schopno poskytovat podniku služby v potřebné kvalitě, stejně jako se řádně starat o citlivá firemní data.
- Rychlý růst – absence pravidelných školení: absence pravidelných školení způsobuje neefektivitu nebo chybovost při práci zaměstnanců. Při rychlém růstu podniku se tyto rizika zvyšují.
- Rychlý růst – neúplná dokumentace strukturované kabeláže: neúplnost dokumentace zpomaluje plánování a vlastní rozšíření strukturované kabeláže.
- Únik citlivých dat – nedostatečné řízení přístupu ke konstrukční dokumentaci: špatně řízený přístup k datům umožňuje vznik rizika z jejich zneužití.
- Únik citlivých dat - absence politiky IT: politika informační bezpečnosti předepisuje kdo a jak smí citlivá data využívat, její absence vyvolává riziko zneužití.
- Únik citlivých dat - zastaralé řízení podnikové domény: nedostatečné možnosti konfigurovat globální i uživatelská pravidla přispívají velkou mírou k úniku podnikových dat.
- Únik citlivých dat - absence IDS: nemožnost monitorovat a reportovat síťový provoz (IDS) vede k riziku úniku dat elektronickou cestou.
- Únik citlivých dat - outsoursing pro doménu: v outsoursingu podnikové domény a mailserveru má k citlivým datům podniku přístup poskytovatel služeb, z pozice administrátora.
- Únik citlivých dat - fyzická bezpečnost: zaměstnanci a hosté mohou vynést z podniku citlivá firemní data na přenosných médiích.

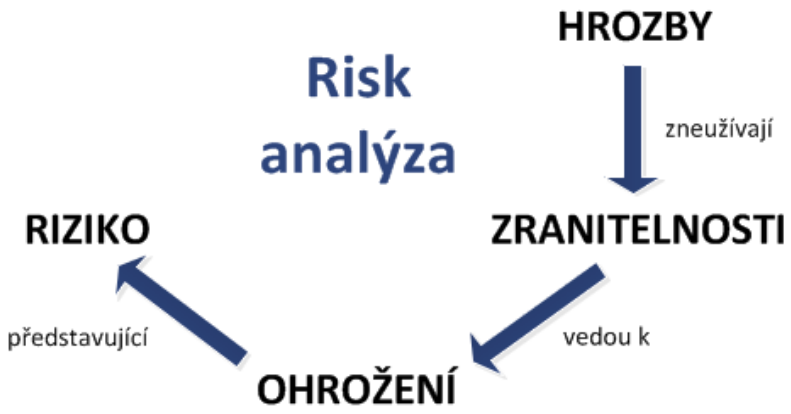
- Únik osobních informací - absence politiky IT: stejný případ jako u úniku citlivých dat - absence politiky IT.
- Únik osobních informací - outsoursing pro doménu: outsoursing podnikové domény umožňuje přístup dodavateli i k osobním informacím zaměstnanců.
- Únik osobních informací - fyzická bezpečnost: stejný případ jako únik citlivých dat - fyzická bezpečnost.
- Útok viry - nedostatečné řízení přístupů ke konstrukční dokumentaci: špatné řízení přístupů k datům dává příležitost pro vznik rizika poškození virem či malwarem.
- Útok viry - absence politiky IT: politika IT bezpečnosti nepředepisuje plánování testů, aktualizací a jednání v případě napadení virem.
- Útok viry - zastaralé řízení podnikové domény: doména se díky outsoursingu a zastaralému řízení tváří z pohledu podnikového IT jako blackbox, což přispívá riziku napadení i nedostatečné obrany proti virům.
- Útok viry - absence IDS: škodlivé programy komunikující po podnikové síti není snadné odhalit, pomocí IDS by to bylo snadnější.
- Útok viry - vytížení IT oddělení: vytíženost pracovníků IT zpomalý celý proces odstranění virů. Pokud jde například o viry, které provádějí šifrování citlivých dat, vzniká další riziko z jejich ztráty, kde je nutná obnova ze zálohy.
- Útok viry - absence školení: absence školení vede ke špatnému zacházení s viry a antiviry.
- Sociální útoky - absence politiky IT: absence politiky nedává jasný návod, jak správně reagovat na útoky typu podvodný e-mail, war dialing, krádež dokumentů nebo běžné vyzrazení hesla či hesla na lístečku. Politika tím také nedefinuje hranici zodpovědností mezi zaměstnancem a podnikem.
- Sociální útoky - absence školení: neexistence školení znamená chybné reakce na útoky, případně neznalost politiky IT bezpečnosti.

- Útoky na síťovou infrastrukturu - absence IDS: časově náročnější odhalení kolizí IP, přehlcení pakety a celkově jakýchkoliv anomálií v podnikové síti.
- Útoky na síťovou infrastrukturu - vytíženost IT: nedostatek prostoru pro řešení potíží se projeví na delším čase diagnostiky sítě a následné opravy i na vzniku příležitosti k chybám.
- Výpadky elektřiny - absence záložní serverovny: výpadkem elektřiny v jedné budově (v jednom rozvaděči) se přeruší dodávka elektřiny všem páteřním síťovým prvkům a serverům.
- Výpadky elektřiny - absence politiky IT: součástí politiky IT není recovery plán.
- Výpadky elektřiny - vytíženost IT: krátkodobé výpadky prověřují především HW a záložní zdroje, v případě dlouhodobého výpadku je třeba řádně vypnout kritické části infrastruktury (servery, routery, tel. ústřednu, BTS, WiFi spoje, atd.).
- Přepětí bleskem - absence záložní serverovny: pokud blesk způsobí přepětí v síti, kde je umístěna kritická část IT infrastruktury, hrozí poškození všem těmto prvkům.
- Přepětí bleskem - absence politiky IT: stejně jako u výpadku elektřiny, součástí politiky IT není recovery plán.
- Přepětí bleskem - vytíženost IT: poškození síťových prvků vždy vytíží pracovníky IT.
- Výpadek internetu – outsoursing: mezi outsoursované služby patří (mimo jiné) internet a mailserver, které při výpadku internetu nefungují. Pro internet není k dispozici záložní spoj, ani poskytovatel (kromě internetu poskytovaného mobilními operátory).
- Živelná katastrofa - absence záložní serverovny: pokud katastrofa postihne serverovnu, není jiná infrastruktura, kterou by šlo využít k fungování podniku.
- Živelná katastrofa - absence politiky IT: podobně jako u předchozích bodů není k dispozici recovery plán.

- Živelná katastrofa - vytíženost IT: obnova IT po živelné katastrofě je závislá na IT zdrojích.

6.2.4. Významná rizika vyplývající ze SWOT analýzy

Ohrožení je zneužití zranitelnosti hrozbou, což představuje konkrétní riziko.



Obr. 4: Definice rizik. Zdroj: upraveno autorem dle (Čermák, 2013).

Zjištěná rizika mohou být významná buď tím, že ohrožují významné (důležité, cenné) aktivum podniku nebo svou vysokou pravděpodobností, že hrozby zneužijí zranitelnosti.

Tab. 5: Významná rizika výsledků SWOT analýzy v podniku XY. Zdroj: autor.

Rizika vyplývající z	Rizika
Absence politiky IT; Pravidelných školení; Řešení fyzické bezpečnosti	- čím vyšší bude růst podniku, tím bude více bezpečnostních incidentů - únik citlivých dat podniku a osobních dat zaměstnanců - špatné jednání zaměstnanců při ochraně proti škodlivým programům - špatné jednání zaměstnanců při ochraně proti sociálním útokům - neexistence postupů a záruk obnovení provozu (recovery plán)
Absence IDS	- únik citlivých dat elektronickou cestou - neodhalení škodlivých programů komunikujících po podnikové síti - časově náročné řešení incidentů v podnikové síti
Absence záložní serverovny	- poškození kritického HW výpadkem elektřiny - poškození kritického HW bleskem - nemožnost obnovení provozu po živelné katastrofě
Chybějící popis podnikových procesů	- neefektivní změny v procesech informačního systému
Nedostatečné řízení přístupu; Nepoužívaný SW pro data konstrukční dokumentace	- čím vyšší bude růst podniku, tím větší problém bude nasadit SW - únik citlivých dat podniku - poškození dat škodlivými programy (viry, malware)
Outsoursing podnikové domény, mailserveru, firewallu, antiviru a VPN; Zastaralé řízení podnikové domény	- odkázanost na služby dodavatele v kritické oblasti IT - únik citlivých dat podniku a osobních dat zaměstnanců externí firmě - poškození dat škodlivými programy (viry, malware)
Vytíženost IT oddělení	- zhoršení IT služeb - vyšší ohrožení podnikových dat

6.3. Penetrační testy

Před rozhodnutím, jestli provést penetrační testování, je třeba se zabývat otázkou, zda jde o vhodnou metodou k provedení detekce rizik podnikového informačního systému. Dle Mika (2013, s. 3) jsou časté důvody k provedení penetračních testů následující: „Ověření reálné odolnosti systému. Lze zhodnotit efektivitu procesů dohledu/monitoringu. Může obsahovat netradiční metody. Lze najít chyby v custom kódu.“.

Náklady na penetrační testování jsou obvykle dány rozsahem, hloubkou a specifikami konkrétního podniku. V případě prvního provedení, nemusí být předem jasné přínosy podniku z penetračních testů. V případě podniku XY byl tedy stanoven takový finanční limit, který byl podnik schopen akceptovat, a přitom příliš neutrpěla kvalita výsledků testů.

6.3.1. Zadání a příprava penetračního testování

Zadání penetračního testování

Předmětem poptávky je provedení vnitřních penetračních testů informačního systému v podniku XY, včetně stanoveného finančního limitu. Podnik XY požaduje v souvislosti s penetračním testováním zachování plné funkčnosti všech systémů a neporušení veškerých firemních dat. Dále podnik XY požaduje po zhotoviteli penetračních testů zachování úplné mlčenlivosti tak, aby nemohlo dojít během, i po provedení, testů k jakémukoliv vyzrazení informací patřících podniku XY nebo jiným způsobem k poškození společnosti. V průběhu penetračního testování chceme být pravidelně informováni o začátku a konci testování a o jakýchkoliv vzniklých potížích. Penetrační testování bude rozděleno na dvě fáze.

První fáze testování: realizace základního screeningového penetračního testování pomocí automatizovaných nástrojů. Výstupem penetračního testování bude soupis jednotlivých zařízení v síti dostupných v době testování, včetně identifikovaných zranitelností ke každému konkrétnímu systému, tříděných dle

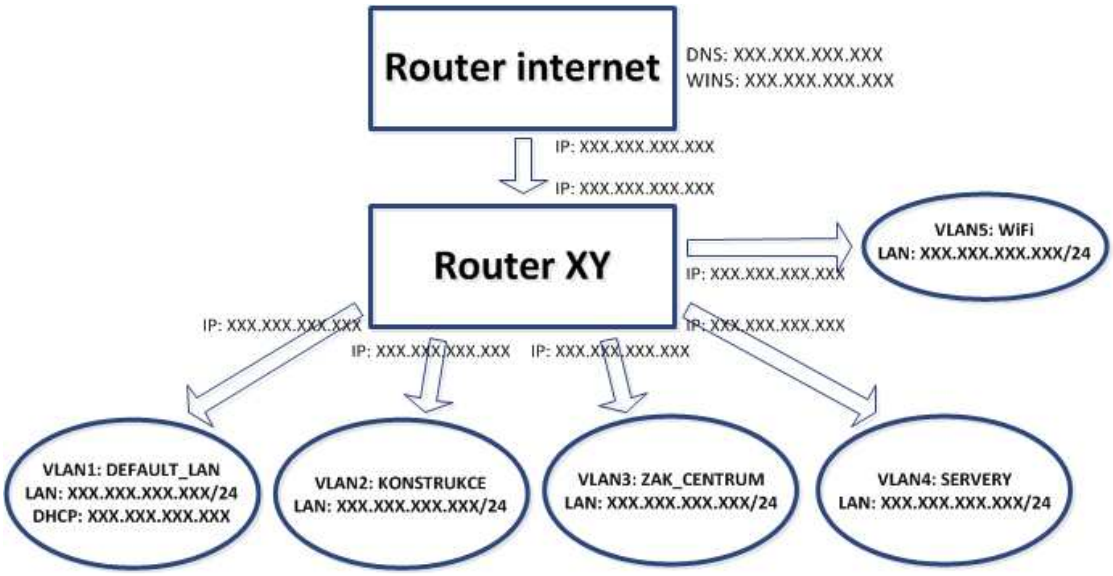
závažnosti nálezu. Rozsah testování je omezen na 4 subnety, každý o velikosti /24 (prefix).

Druhá fáze testování: na základě výstupů z první fáze testování bude realizováno jednání, které definuje další postup v případě nálezu kritických zranitelností a dalšího zaměření budoucího testování.

Příprava penetračního testování

Podnikové směrnice rozdělují nákup zboží a služeb do několika kategorií, ke kterým jsou popsány nutné podmínky pro provedení nákupu. Jedná se především o finanční limity, které určují, od které částky je třeba uspořádat výběrové řízení, v jakém rozsahu a kdo musí být členem hodnotící komise. Penetrační testování spadalo do nejnižší finanční kategorie, nebylo tedy třeba uspořádat výběrové řízení. K jednání byly přizvány společnosti AutoCont CZ a.s. a Unicorn Systems a.s. Obě společnosti prokázaly potřebné znalosti, odbornost a zkušenosti pomocí svých referencí. Pro provedení penetračních testů byla vybrána společnost Unicorn Systems.

Před dalším jednáním byla podepsána „Smlouva o utajení“ (vzor této smlouvy je uveden v příloze 10.4). Následně byly upřesněny technické detaily, například topologie sítě (Obr. 5) a časový plán provedení testů.



Obr. 5: Topologie sítě. Zdroj: autor.

6.3.2. Výsledky penetračních testů

Manažerské shrnutí

Tento dokument popisuje výsledek penetračního testování infrastruktury podniku XY pomocí automatizovaných nástrojů Tenable Nessus a OpenVAS.

Jako cíl testování byly zvoleny sítě „DEFAULT_LAN, SERVERY, KONSTRUKCE a ZAK_CENTRUM“, kde bylo celkem prověřeno 186 spuštěných koncových zařízení a serverů.

Z důvodu definice časového okna pro realizaci penetračních testů nedošlo k plnému prověření programem OpenVAS, nicméně vzhledem k množství nálezů programem Tenable Nessus to nepovažujeme za nedostatek, naopak – absencí realizace druhým programem vznikl větší prostor pro konzultace a případnou nápravu stavu, což považujeme za prioritnější.

Celkově bylo nalezeno v síti podniku XY následující množství zranitelností (s výskytem na více koncových zařízení):

- 13x critical zranitelnost (na více stanicích)
- 22x high zranitelnost (na více stanicích)
- 64x medium zranitelnost (na více stanicích)
- 28x low zranitelnost (na více stanicích)

Kritická (critical) zranitelnost je uvedena u chyb umožňující plné převzetí cílového operačního systému (práva administrátora). Mezi tuto úroveň zranitelnosti lze zařadit i provozování nepodporovaných operačních systémů ze strany výrobce (v tomto případě Windows® NT a Windows® XP).

Vysoká (high) zranitelnost je většinou ukazatel chybné konfigurace přístupů (například výchozí jméno a heslo, absence aplikace major aktualizace provozované služby) nebo zranitelnost mající za určitých okolností potenciál k plnohodnotnému převzetí systému nebo jeho kompromitaci s využitím nižších práv.

Střední (medium) zranitelnost je většinou chyba ve formě méně závažné aktualizace mající za následek omezení přístupu ke službě, případně její nedostupnost.

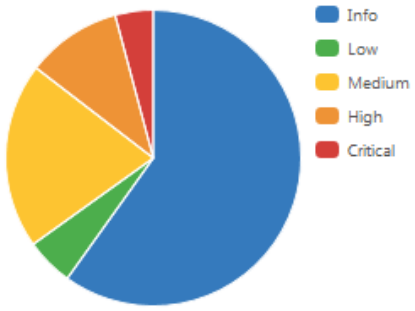
Nízké (low) zranitelnosti indikují drobné pochybení v konfiguraci umožňující zjištění podrobnějších informací o operačním systému, jež je možné dále využít pro mapování prostředí.

Informativní (info) zranitelnosti představují obecné informace, které by mohly být využity spíše jako doplňující. Např. verze http serveru, verze SSH a podobně.

Je nezbytné si uvědomit, že zranitelnost celého prostředí je stejná jako nejméně chráněný prvek. Bezpečnost domény může být například velice úspěšně narušena instalací specifických programů na méně významné servery, pak pouze vyčkat na přihlášení privilegovaného doménového uživatele, čímž dojde ke krádeži plných administrátorských práv. Celková úroveň zranitelnosti je tedy kritická.

Zhodnocení zranitelnosti pro síť DEFAULT_LAN

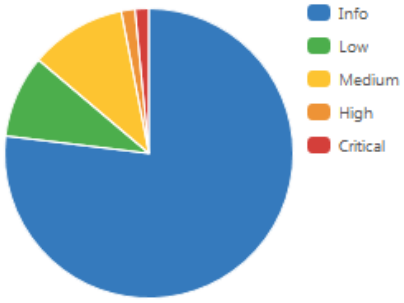
- 8x critical zranitelnost
- 20x high zranitelnost
- 39x medium zranitelnost
- 10x low zranitelnost



Graf 1: Zranitelnosti VLAN1. Zdroj: autor.

Zhodnocení zranitelnosti pro síť KONSTRUKCE

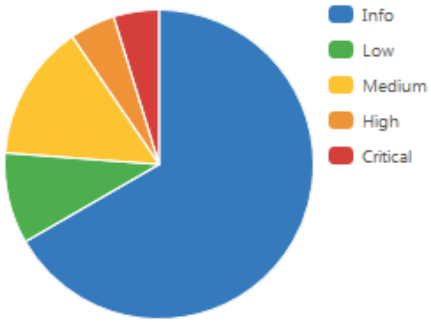
- 1x critical zranitelnost
- 1x high zranitelnost
- 7x medium zranitelnost
- 6x low zranitelnost



Graf 2: Zranitelnosti VLAN2. Zdroj: autor.

Zhodnocení zranitelnosti pro síť ZAK_CENTRUM

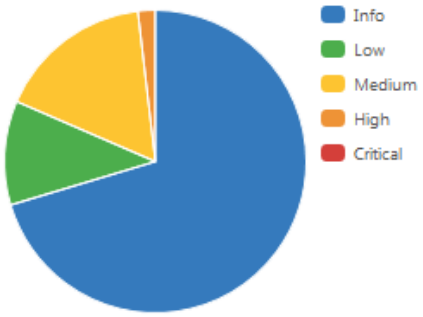
- 3x critical zranitelnost
- 1x high zranitelnost
- 9x medium zranitelnost
- 6x low zranitelnost



Graf 3: Zranitelnosti VLAN3. Zdroj: autor.

Zhodnocení zranitelnosti pro síť SERVERY

- 1x high zranitelnost
- 9x medium zranitelnost
- 6x low zranitelnost



Graf 4: Zranitelnosti VLAN4. Zdroj: autor.

Celkové zhodnocení

Vzhledem k výskytu kritických chyb v obou testovaných segmentech je celková bezpečnost na velice nízké úrovni. Bezpečnost celého ICT prostředí je odvislá od nejvíce zranitelného koncového zařízení nebo serveru. Jisté zmírnění stavu by bylo možné, pokud bychom předpokládali, že Windows XP (označené jako kritická zranitelnost díky absenci podpory ze strany výrobce) nejsou z pohledu bezpečnosti prozatím kritické. Avšak i přes tento předpoklad existuje dále velké množství zranitelností, které celkovou klasifikaci drží na úrovni kritická. Je to mimo jiné díky využívání starších verzí programů, použití výchozích hesel nebo nevhodně zvolenými certifikáty. Další závažná zranitelnost byla objevena v síti SERVERY, kde je využívána zastaralá verze virtualizačního serveru a přítomnost nedávno objevené chyby zranitelnosti Shellshock.

V prostředí, které bylo analyzováno, je reálné očekávat ze strany interních, případně i externích útočníků (bezpečnost centrální brány nebyla testována) zdárný

útok na ICT prostředí mající za následek např. ztrátu, krádež či kompromitaci dat, případně výrazné ovlivnění provozu.

Všeobecná doporučení

S ohledem na nálezy zranitelností doporučuji realizovat následující kroky:

- Podrobnou analýzu reportů s cílem odhalit jaké konkrétní servery obsahují jakou zranitelnost.
- Povýšit prostředí VMware na nejvyšší verzi.
- Povýšit OpenSSL v prostředích kde je to možné a deaktivovat nepoužívané služby.
- Opravit community stringy, případně deaktivovat SNMP.
- Zvážit nasazení interní CA pro vyšší zabezpečení certifikátů.
- Povýšení stanic s instalovanými Windows XP na vyšší verzi operačního systému.
- Zavedení centrálního WSUS serveru a přenastavit systém aplikace záplat na automatickou (včetně automatického schvalování).
- Revize využívaných starších verzí aplikací a služeb, zajistit povýšení na nejvyšší možnou verzi (především Apache a OpenSSL).
- Přenastavení výchozích hesel v aplikacích.
- Revidovat nastavení certifikační autority.
- Povýšit verzi řídících systému SIMATIC (případně omezit přístupy na tato zařízení pouze z omezeného množství počítačů – využití další segmentace sítě s definovanými přístupy).
- Opakovaně realizovat penetrační testy k identifikaci dalších potenciálních hrozeb.

6.3.3. Rizika vyplývající z penetračních testů

Přílohou k výsledkům penetračních testů jsou velice podrobné informace, popisující veškerá síťová zařízení (která byla v čase testů aktivní), k nim jednotlivé klasifikované zranitelnosti, včetně doporučení k jejich odstranění, nebo zmírnění případného dopadu při pokusu o zneužití. Podobně jako u SWOT analýzy, jsou i v případě penetračních testů vybrána pouze významná rizika. V případě penetračních testů jsou to high zranitelnosti v síti SERVERY, critical zranitelnosti v ostatních sítích, a to vše s přihlédnutím k všeobecným doporučením.

Tab. 6: Významná rizika výsledků penetračních testů v podniku XY. Zdroj: autor.

Rizika vyplývající z	Rizika
Neaktuální verze ESXi 5.5 Build 1746974 Update 1	- možnost zneužití GNU Bash Environment Variable Handling Code Injection (Shellshock)
Neaktuální verze OpenSSL	- možnost zneužití OpenSSL 'ChangeCipherSpec' MiTM Vulnerability - možnost zneužití OpenSSL Heartbeat Information Disclosure
Neaktuální verze Apache	- možnost zneužití HTTP serveru pro řízení domény a přístupu k mailserveru
Na hlavním routeru je pro SNMP nastaven výchozí community string	- možnost zneužití informací o podnikové síti
Slabě zabezpečený certifikát pro mailserver	- možnost zneužití slabého šifrování
Používání stanic s Windows XP	- zneužití zranitelností zastaralého operačního systému (podpora skončila 8.9.2014)
Absence WSUS (centrální řízení aktualizací pro operační systémy Microsoft)	- možnost neaktuálnosti verze operačního systému Windows může vést k případnému zneužití
Absence politiky IT	- zneužití slabých nebo výchozích hesel
Zastaralé verze řídících systémů SIMATIC	- možnost zneužití informací o některých strojích a zařízeních ve výrobě

6.4. Hodnocení rizik

V kapitolách 6.2.4. a 6.3.3. byla méně významná rizika akceptována a ta významná identifikována a popsána. Před tím, než dojde k navržení opatření k těmto významným rizikům, je vhodné získat jakýsi žebříček důležitosti, a to ohodnocením závažnosti jednotlivých rizik. Dle kapitoly 3.3.4. se rizika bezpečnosti informací hodnotí dle těchto kritérií:

a) potencionální následky, které by nastaly, pokud by se realizovala rizika;
b) reálná pravděpodobnost výskytu rizika.

K hodnocení rizik dle doporučení ISO/IEC 27003 je třeba vybrat vhodnou metodu, která je reprodukovatelná a porovnatelná v čase. Mezi takové metody může patřit analýza dopadů na aktiva, pravděpodobnosti scénářů, hodnota finanční ztráty způsobené výpadkem aktiva a další. ISO/IEC 27003 (ÚNMZ, 2011, s. 28) také říká: "Hodnocení rizik by se měli účastnit jedinci, kteří velmi dobře znají cíle organizace a chápou bezpečnost (proniknutí do podstaty věci, co je v současné době důležité)."

Hodnocení rizik v této práci vychází z výše uvedených kritérií a) a b) a využívá dlouholetou znalost prostředí a zkušenosti autora. Hodnocení je popsáno níže v Tab. 7 pomocí bodů od 1 do 10, přičemž riziko ohodnocené 10 je nejvýznamnější.

..

Tab. 7: Hodnocení rizik IT v podniku XY. Zdroj: autor.

Rizika vyplývající z	Rizika	Závažnost
Absence politiky IT;	- čím vyšší bude růst podniku, tím více bezpečnostních incidentů	8
Pravidelných školení;	- únik citlivých dat podniku a osobních dat zaměstnanců	7
Řešení fyzické bezpečnosti	- špatné jednání zam. při ochraně proti škodlivým programům	4
	- špatné jednání zam. při ochraně proti sociálním útokům	5
	- neexistence postupů a záruk obnovení provozu (recovery plán)	3
Absence IDS	- únik citlivých dat elektronickou cestou	5
	- neodhalení škodlivých programů v podnikové síti	3
	- časově náročné řešení incidentů v podnikové síti	2
Absence záložní serverovny	- poškození kritického HW výpadkem elektřiny	7
	- poškození kritického HW bleskem	4
	- nemožnost obnovení provozu po živelné katastrofě	2
Chybějící popis podnikových procesů	- neefektivní změny v procesech informačního systému	7
Nedostatečné řízení přístupu;	- čím vyšší růst podniku, tím větší problém bude nasadit SW	5
Nepoužívaný SW pro data	- únik citlivých dat podniku	7
konstrukční dokumentace	- poškození dat škodlivými programy (viry, malware)	3
Outsoursing domény	- odkázanost na služby dodavatele v kritické oblasti IT	6
mailserveru, firewallu,	- únik citlivých dat podniku a osobních dat zam. externí firmě	3
antiviru a VPN; Zastaralé	- poškození dat škodlivými programy (viry, malware)	3
řízení podnikové domény		
Vytíženost IT oddělení	- zhoršení IT služeb	4
	- vyšší ohrožení podnikových dat	7
Neaktuální verze ESXi 5.5 Build 1746974 Update 1	- zneužití GNU Bash Environment Variable Handling Code Injection (Shellshock)	2
Neaktuální verze OpenSSL	- zneužití OpenSSL 'ChangeCipherSpec' MiTM Vulnerability	2
	- zneužití OpenSSL Heartbeat Information Disclosure	2
Neaktuální verze Apache	- zneužití HTTP serveru pro řízení domény a mailserveru	4
Výchozí community string na hlavním routeru pro SNMP	- možnost zneužití informací o podnikové síti	2
Slabý certifikát mailserver	- možnost zneužití slabého šifrování	2
Používání stanic s Windows XP	- zneužití zranitelností zastaralého operačního systému (podpora skončila 8.9.2014)	2
Absence WSUS (centrální řízení aktualizací Microsoft)	- možnost neaktuálnosti verze operačního systému Windows může vést k případnému zneužití	2
Absence politiky IT	- zneužití slabých nebo výchozích hesel	10
Zastaralé verze řídících systémů SIMATIC	- možnost zneužití informací o některých strojích a zařízeních	2

Hodnocení závažnosti jednotlivých rizik je třeba podložit podrobnějšími informacemi:

- Čím vyšší bude růst podniku, tím více bezpečnostních incidentů – růst podniku je často plánován z pohledu potřeb a kapacit výroby. Nepřipravenost nebo nedostatek kapacit pro zvládání incidentů mnohonásobně zvyšuje pravděpodobnost vzniku dalších rizik. Právě díky této návaznosti je to velmi závažné riziko.
- Únik citlivých dat podniku a osobních dat zaměstnanců – odcizení dat hosty, ale především zaměstnanci, je díky mnoha aspektům poměrně snadné a přitom může představovat vážný dopad na podnik.
- Špatné jednání zaměstnanců při ochraně proti škodlivým programům – vzhledem k velkému množství škodlivých programů je to v podstatě denní problém. Na druhou stranu podnik XY riziko zmírňuje opatřeními typu firewall, dvěmi úrovněmi antivirové ochrany, atd.
- Špatné jednání zaměstnanců při ochraně proti sociálním útokům – četnost sociálních útoků není příliš velká, jedná se ale o poměrně účinnou hrozbu.
- Neexistence postupů a záruk obnovení provozu (recovery plán) – postupy, jak obnovit činnost systémů a mít k tomu prostředky, mohou být v případě nouze velmi užitečné. Jiné riziko to ale představuje pro výrobní podniky a například datová centra.
- Únik citlivých dat elektronickou cestou – únik citlivých dat představuje riziko v obecné rovině. Absence IDS představuje pouze částečné řešení.
- Neodhalení škodlivých programů v podnikové síti – prostřednictvím počítačové sítě dochází k distribuci mnoha škodlivých programů. Toto riziko částečně řeší firewall, antivir a aktualizace OS.
- Časově náročné řešení incidentů v podnikové síti – řešení chyb síťového provozu může být velmi časově náročné. Četnost takových incidentů je ale v posledních několika letech nižší.

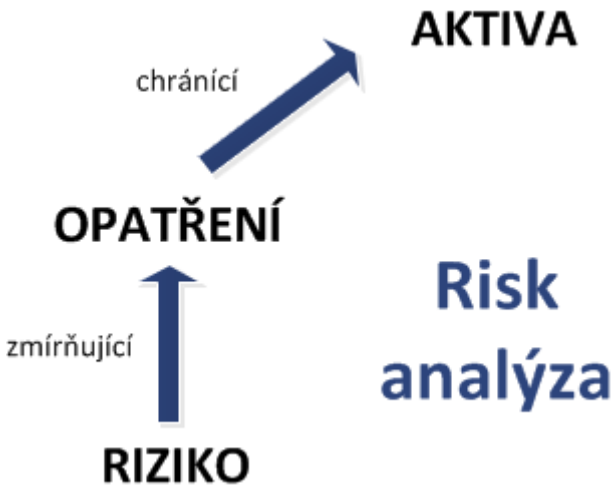
- Poškození kritického HW výpadkem elektřiny – k výpadkům elektřiny dochází v lokalitě podniku velmi často a jsou téměř vždy zdrojem HW potíží, naštěstí ne příliš často potíží s kritickými HW prvky.
- Poškození kritického HW bleskem - blesk představuje podobné riziko jako výpadek elektřiny, k potížím ale nedochází tak často.
- Nemožnost obnovení provozu po živelné katastrofě – dopad tohoto rizika je velmi vážný a může představovat úplnou ztrátu některých dat. Lokalita podniku ale není v oblasti s vyšší možností vzniku živelné katastrofy.
- Neefektivní změny v procesech informačního systému – neefektivní změny ve firemních procesech a špatné nasazení nových procesů vedou k neefektivitě a špatnému fungování podniku. Toto riziko je reálné a představuje nedostatek a neucelené informace pro rozhodování i na vyšších postech podniku.
- Čím vyšší růst podniku, tím větší problém bude nasadit SW – riziko, že nebude systém pro správu konstrukční dokumentace správně a efektivně fungovat, se zvyšuje s růstem podniku a časem odkládání tohoto projektu.
- Únik citlivých dat podniku – k úniku citlivých dat velmi přispívá současný stav řízení přístupu ke konstrukční dokumentaci a představuje tedy velké riziko odcizení.
- Poškození dat škodlivými programy (viry, malware) – základní řízení přístupu a zálohování toto riziko zmírňuje, nicméně existují případy, kdy i přesto může dojít k nenávratnému poškození či ztrátě dat.
- Odkázanost na služby dodavatele v kritické oblasti IT – obecný problém s outsoursingem znamená riziko spolehnout se (i přes smlouvu) na ochotu a pomoc dodavatele. V tomto případě i na jeho pracovní dobu.
- Únik citlivých dat podniku a osobních dat zaměstnanců externí firmě – toto riziko zmírňuje smlouva o utajení.
- Poškození dat škodlivými programy (viry, malware) – toto riziko zmírňuje antivir, firewall a aktualizace OS.

- Zhoršení IT služeb – zhoršení služeb IT představuje zpomalení a neefektivitu práce zaměstnanců, může mít ale mnohem horší dopady.
- Vyšší ohrožení podnikových dat – nedostatkem času na vyřízení požadavků, incidentů, projektů a podobně velmi zvyšuje riziko chybovosti. Je jen otázkou času, kdy chyba či přehlédnutí bude mít dopad na data a způsobí podniku újmu.
- Zneužití GNU Bash Environment Variable Handling Code Injection (Shellshock) – riziko zneužití této chyby je tím menší, čím vyšší problém je pro útočníka dostat se do podnikové sítě.
- Zneužití OpenSSL 'ChangeCipherSpec' MiTM Vulnerability – možnost zneužití nepředstavuje příliš velkou motivaci pro útočníka.
- Zneužití OpenSSL Heartbeat Information Disclosure – možnost zneužití nepředstavuje příliš velkou motivaci pro útočníka.
- Zneužití HTTP serveru pro řízení domény a mailserveru – zneužití některých mailů by mohlo mít dopad na podnik.
- Možnost zneužití slabého šifrování - možnost zneužití nepředstavuje příliš velkou motivaci pro útočníka. Jsou jiné způsoby, jak snadněji získat potřebné informace.
- Zneužití zranitelností zastaralého operačního systému – Windows XP na několika stanicích je chráněn i jinými prostředky. Navíc dochází k postupnému nahrazení novějšími stroji dle plánu pravidelné obnovy.
- Možnost neaktuálnosti verze operačního systému Windows – obecně aktualizace Windows jsou jedním z nástrojů pro ochranu. Potřeba centrálně monitorovat a spravovat tyto aktualizace není prioritou.
- Zneužití slabých nebo výchozích hesel – asi největší riziko představuje zneužití přihlašovacích údajů, protože toto riziko může být jednoduše zneužito a vede k mnoha negativním dopadům. Zaměstnanci se nechovají zodpovědně ke svým přístupům a zastaralý systém pro řízení podnikové domény neumožňuje tvorbu rozumné politiky.
- Možnost zneužití informací o některých strojích a zařízeních – riziko zneužití tohoto typu informací je sníženo tím, že tyto informace nejsou příliš žádány potencionálními útočníky.

7. Případová studie – návrh zabezpečení podnikové infrastruktury

Případová studie se zaměřuje na kvalitativní stránku problematiky, což z pohledu zvládání rizik bezpečnosti informací znamená detailní popis rizik a k nim hledání opatření na základě porozumění podobným případům.

Podrobný popis rizik, včetně ohodnocení, je vypracován v předchozí kapitole 6. V návaznosti na analýzu rizik je tedy předmětem případové studie hledání vhodných opatření ke zmírnění rizik a ochraně aktiv.



Obr. 6: Zvládání rizik. Zdroj: upraveno autorem dle (Čermák, 2013).

7.1. Požadavky

Obecným požadavkem je zvýšení bezpečnosti informací v podniku XY. Jelikož informační systém je poměrně rozsáhlý a prostupuje v podstatě do všech zásadních procesů podniku, je třeba celou problematiku řešit z mnoha úhlů pohledu. K tomu výborně poslouží výsledky analýzy rizik tvořené dvěma metodami.

Dílčí požadavky:

- Zvýšit povědomí o ochraně informací.

- Efektivní práce s daty.
- Zvýšit ochranu dat proti odcizení.
- Zvýšit schopnost řídit bezpečnost informací.

7.2. Popis řešení

Komplexní řešení nabízí implementace ISO/IEC 27001, která popisuje tvorbu a fungování Systému řízení bezpečnosti informací (ISMS). Vlastní proces nasazení ISMS je popsán pomocí normy ISO/IEC 27003 a zvládání rizik je jeho součástí. Zmírnění konkrétních rizik pomocí opatření je součástí této podkapitoly.

Jako pomoc s hledáním vhodných opatření se nabízí první sloupeček Tab. 7 s názvem „Rizika vyplývající z“ v kapitole 6.4.

Zavedení politiky bezpečnosti informací

Dle ISMS je politika bezpečnosti informací dokument, který vychází ze záměrů organizace, v obecné rovině je popsána v kapitole 3.3.3. Pro zavedení základní politiky bezpečnosti informací v podniku XY není v současnosti potřeba splnit všechny podmínky ISO/IEC 27001.

Doporučený postup:

1) Souhrn cílů a požadavků organizace (lze vyjít z této případové studie).
2) Identifikace aktiv.
3) Analýza a hodnocení rizik (lze využít kapitolu 6.).
4) Výběr opatření k významným rizikům (lze vyjít z této případové studie).
5) Vytvoření a schválení vrcholového projektu ke zlepšení bezpečnosti informací (lze vyjít z této případové studie).
6) Stanovení periody opakování.

Toto opatření zmírňuje rizika: opatření má návaznost na všechna rizika bezpečnosti informací.

Tvorba IT směrnic

Tvorba IT směrnic navazuje na zavedení politiky bezpečnosti informací. Je více než vhodné vytvořit v podniku XY směrnice IT alespoň v takovém rozsahu, aby popisovala nejdůležitější pravidla pro chování zaměstnanců k podnikovému IT.

Doporučení:

- Směrnice stanovující základní role a odpovědnosti v IT (administrátor, supervizor, uživatel, host, odpovědnost za svěřenou IT techniku a podniková data).
- Směrnice pro identifikaci uživatele heslem, čipovou kartou a biometrikou (včetně minimální síly hesla, chování při vyzrazení a podobně).
- Směrnice pro nástup a ukončení pracovního poměru zaměstnance (tvorba a rušení účtů, úvodní školení, podpis zaměstnance o seznámení s IT směrnicemi).

Toto opatření zmírňuje rizika:

- Čím vyšší bude růst podniku, tím více bezpečnostních incidentů.
- Únik citlivých dat podniku a osobních dat zaměstnanců.
- Únik citlivých dat elektronickou cestou.
- Zneužití slabých nebo výchozích hesel.

IT školení zaměstnanců

Úvodní školení zaměstnanců při nástupu do zaměstnaneckého poměru je již zmíněno v IT směrnicích. Pravidelné školení zaměstnanců ale zvyšuje povědomí o zacházení s IT technikou, informacemi a zvyšuje efektivitu práce.

Doporučení:

- Pravidelné roční školení IT (obecné školení, ERP, provede IT).
- Pravidelné roční školení konstruktérů (CAD software, provede dodavatel).

- Jednorázová školení na změny v systémech (legislativa, mzdy, účetnictví, nová verze CAD software, provede dodavatel).

Toto opatření zmírňuje rizika:

- Čím vyšší bude růst podniku, tím více bezpečnostních incidentů.
- Únik citlivých dat podniku a osobních dat zaměstnanců.
- Špatné jednání zaměstnanců při ochraně proti škodlivým programům.
- Špatné jednání zaměstnanců při ochraně proti sociálním útokům.
- Únik citlivých dat elektronickou cestou.
- Zhoršení IT služeb.
- Zneužití slabých nebo výchozích hesel.

Modernizace řízení podnikové domény

Modernizace systému pro řízení podnikové domény představuje nákup a implementaci MS Active Directory nebo podobného moderního unixového řešení. Součástí stávajícího řešení je i mailserver, proto je nutné modernizovat i tuto funkcionalitu.

Doporučení:

- Pořízení licencí MS pro Active Directory (Windows Server 2012 R2 Standard + potřebný počet CAL licencí).
- Pořízení licencí MS Exchange server 2013 nebo podobného konkurenčního řešení (nový mailserver nebo pronájem).
- Přechod na AD a Exchange.

Toto opatření zmírňuje rizika:

- Odkázanost na služby dodavatele v kritické oblasti IT.
- Únik citlivých dat podniku a osobních dat zaměstnanců externí firmě.
- Poškození dat škodlivými programy (viry, malware).
- Zneužití HTTP serveru pro řízení domény a mailserveru.
- Možnost zneužití slabého šifrování.
- Zneužití slabých nebo výchozích hesel.

Pořízení a konfigurace podnikového firewallu

Současné řešení podnikové domény zahrnuje mimo mailserver také podnikový firewall a VPN. V případě modernizace bude potřeba počítat i s těmito funkcionalitami. Navíc toto zařízení může obsahovat IDS (systém pro detekci průniku a anomálií sítě) a IPS (IDS + prevence proti průniku, blokování škodlivé činnosti).

Doporučení:

- Pořízení a implementace podnikového firewallu s VPN, antivirem a dalšími funkcemi (Cisco ASA, Kerum, Fortinet a podobně).
- Toto řešení může obsahovat i IDS.
- Toto řešení může obsahovat i IPS.
- Pokud je využit systém IDS nebo IPS, je nezbytné zajistit automatickou aktualizaci databáze pro detekci stavových značek (řetězce specifické pro daný typ útoku).

Toto opatření zmírňuje rizika:

- Opatření může mít vliv na většinu rizik vyplývajících z penetračních testů.
- Čím vyšší bude růst podniku, tím více bezpečnostních incidentů.
- Únik citlivých dat podniku a osobních dat zaměstnanců.
- Únik citlivých dat elektronickou cestou.
- Odkázanost na služby dodavatele v kritické oblasti IT.
- Poškození dat škodlivými programy (viry, malware).
- S IDS nebo IPS, neodhalení škodlivých programů v podnikové síti.
- S IDS nebo IPS, časově náročné řešení incidentů v podnikové síti.

Přechod na systém správy konstrukční dokumentace

V souborovém systému nejsou citlivá data konstrukční dokumentace řádně chráněna a řízena (přístupy, logování). Systém pro správu konstrukční dokumentace je již zakoupen a implementován v rámci projektu EU, není však používán.

Doporučení:

- Projednání potřeb konstrukce.
- Stanovení časového plánu pro přechod.
- Nové školení o přechodu a používání systému pro správu konstrukční dokumentace (provede dodavatel).

Toto opatření zmírňuje rizika:

- Čím vyšší bude růst podniku, tím více bezpečnostních incidentů.
- Únik citlivých dat podniku a osobních dat zaměstnanců.
- Únik citlivých dat elektronickou cestou.
- Čím vyšší růst podniku, tím větší problém bude nasadit SW.
- Poškození dat škodlivými programy (viry, malware).

Zřízení záložní serverovny

Produkční a zálohovací servery jsou umístěny v jedné serverovně. Pro ochranu dat je potřeba tyto dva typy serverů umístit do jiné lokality.

Doporučení:

- Zřízení záložní serverovny v jiné budově.
- Přestěhování zálohovacího serveru a záložního produkčního serveru.
- Sepsání základní verze recovery plánu.

Toto opatření zmírňuje rizika:

- Neexistence postupů a záruk obnovení provozu (recovery plán).
- Poškození kritického HW výpadkem elektřiny.
- Poškození kritického HW bleskem.
- Nemožnost obnovení provozu po živelné katastrofě.

Analýza podnikových procesů

Pomocí analýzy procesů je možné určit a ucelit informace o fungování podniku. Tato analýza také odhalí slabá místa, neefektivitu a finanční ztráty. Dále při

budování či růstu podniku poskytne možnost efektivně rozvíjet stávající procesy nebo implementovat nové. Analýzou procesů v podniku musí vzniknout ucelená znalost (dokumentace), která bude dále aktualizována, a to pravidelně při každé změně jakéhokoliv procesu. Je také vhodné tuto dokumentaci periodicky prověřovat proti skutečnosti.

Doporučení:

- Projednání rozsahu analýzy s vedením podniku s ohledem na ISO 9001.
- Provedení analýzy ERP (dle rozsahu provede IT nebo ext. firma).
- Dle stanoveného rozsahu je možné provést analýzu procesů mimo ERP (provede ext. firma).
- Dle stanoveného rozsahu je možné předat procesní dokumentaci na jednotlivá oddělení (jen s ohledem na ISO 9001).
- Pravidelná aktualizace procesní dokumentace.

Toto opatření zmírňuje rizika:

- Čím vyšší bude růst podniku, tím více bezpečnostních incidentů.
- Neefektivní změny v procesech informačního systému.

Posílení IT oddělení

Procentuální počet IT pracovníků z celkového počtu zaměstnanců v podniku XY je 0,23%. Dle statistiky (*Gartner*, 2013) je ve výrobních podnicích tato hodnota (IT FTE as a % of Total Employees) v průměru 1,8% (u českých firem se obvykle uvádí 1%).

Doporučení:

- Přijmout alespoň 2 IT pracovníky na plný úvazek.
- Rozdělit odpovědnosti jednotlivým IT pracovníkům.

Toto opatření zmírňuje rizika:

- Toto opatření má nepřímý vliv na všechna rizika.
- Čím vyšší bude růst podniku, tím více bezpečnostních incidentů.

- Únik citlivých dat podniku a osobních dat zaměstnanců.
- Únik citlivých dat elektronickou cestou.
- Neefektivní změny v procesech informačního systému.
- Zhoršení IT služeb.
- Vyšší ohrožení podnikových dat.

7.3. Přínosy

Přínosy jednotlivých opatření jsou konkrétně popsány seznamy rizik, které zmírňují. To, že zmíněná rizika jsou skutečná a mají nebo s velmi reálnou pravděpodobností mohou mít vliv na chod podniku, dokládá metodicky zpracovaná analýza rizik v kapitole 6.

Opatření jsou vybrána tak, aby měla efektivní vliv na daná rizika a zároveň dokázala zmírnit co nejvíce rizik. Zavedení každého ze zmíněných opatření bude mít pozitivní vliv na bezpečnost cenných informací podniku a bude také efektivní jako prevence do budoucna.

Vzhledem k dílčím požadavkům, opatření:

- Zvyšují povědomí o ochraně informací.
- Zvyšují efektivitu práce s daty.
- Zvyšují ochranu dat proti odcizení.
- Zvyšují schopnost řídit bezpečnost informací.

8. Závěr

Obecným cílem práce byl návrh komplexního zabezpečení podnikové IT infrastruktury. Mezi klíčové zdroje informací byly vybrány normy řady ISO/IEC 27000 a zákon o kybernetické bezpečnosti, který z těchto norem čerpá. Pro detekci zranitelností byla zvolena analýza rizik, která byla provedena dvěma metodami. Jako první byla vytvořena SWOT analýza a následně penetrační testování. Výsledky z obou metod byly ohodnoceny. Na základě předchozího byla představena případová studie zabývající se konkrétními opatřeními, které vedou ke zmírnění nalezených rizik.

K popisu norem byly vybrány a podrobně popsány podnormy ISO 27000, jako obecný přehled, definice pojmů a seznam všech navazujících podnorem a ISO 27001, pro představení systému řízení bezpečnosti informací (ISMS). Pro úplnost byly obecnou formou zmíněny i podnormy ISO 27002 (souboru postupů a opatření), ISO 27003 (směrnice pro implementaci ISMS), ISO 27004 (měření) a ISO 27005 (řízení rizik). Ke každé části norem byl přidán popis využití, jako vysvětlení vztahu norem k této práci.

V návaznosti na normy byl představen nový zákon o kybernetické bezpečnosti. Zde byly vysvětleny důvody jeho vzniku a v několika hlavních bodech shrnut stručný popis zákona. Pro definici organizací podléhajících zákonu byla zmíněna vyhláška o významných informačních systémech a nařízení vlády č. 432/2010 Sb. Podnik, jenž byl cílem této práce, zákonu nepodléhá, to však neznamená, že na tyto typy organizací nemá zákon žádný vliv. Proto bylo následně zpracováno i toto téma. Pro úplnost byly doplněny informace o hlášení kybernetického bezpečnostního incidentu.

Další teoretická kapitola byla věnována penetračnímu testování. Ta popisuje důležité pojmy a metody penetračního testování, hledání slabých míst, red teamingu a systémových testů. S ohledem na praktickou použitelnost obsahuje kapitola informace o správné přípravě a průběhu penetračního testování. Tato podkapitola definuje právní rámec české legislativy, postup tvorby, způsoby a nástroje používané při testování a vlastní využití penetračních testů pro detekci IT zranitelností organizace.

Hlavním úkolem praktické části bylo sestavit analýzu rizik v konkrétní organizaci, s využitím doporučení popsaných v normě ISO 27000. Z důvodů obav o možné zneužití citlivých informací byla organizace popsána obecnou formou pod názvem „podnik XY“, výsledky analýzy tím však nebyly nijak ovlivněny.

Jako první metoda byla zvolena SWOT analýza, která definovala silné a slabé stránky jako vnitřní podmínky podniku, příležitosti a hrozby jako podmínky působící na podnik zvenčí. Tyto podmínky byly dále zpracovány pomocí syntézy, čímž vznikly strategie SO (Strenght - Opportunity), ST (Strenght - Threat), WO (Weakness - Opportunity) a WT (Weakness - Threat). Všechny tyto kroky byly detailně popsány a okomentovány. Výsledkem SWOT analýzy je tabulka významných rizik, doplněná o vodítka k jejím zdrojům.

Druhou metodou analýzy rizik bylo provedení penetračních testů IT infrastruktury podniku. Ta začíná zadáním pro provedení testů z pohledu podniku, které je rozděleno na dvě fáze: „obecné provedení testů celé infrastruktury“ a „cílené testy“, které jsou provedeny následně na základě informací získaných z obecných testů. Následuje příprava testů, ta ve zkratce popisuje výběr partnera s ohledem na podnikové směrnice a zdůrazňuje důležitost sepsání smlouvy o utajení. Další podkapitola se věnuje výsledkům penetračních testů. Ty odhalují, mimo jiné, 13 kritických nálezů a 22 nálezů s vysokým hodnocením zranitelnosti. Všechny výsledky jsou kategorizovány dle jednotlivých virtuálních sítí podniku. Jsou také podrobněji popsány významné zranitelnosti. Následuje celkové zhodnocení a všeobecná doporučení. Závěrem penetračních testů je opět tabulka významných rizik včetně jejich zdrojů.

Výsledkem analýzy rizik je hodnocení důležitosti jednotlivých rizik vyplývajících ze SWOT analýzy a penetračního testování, vše s přihlédnutím k doporučením normy ISO 27000. Rizika s nejvýznamnějším ohodnocením se týkají témat zneužití slabých hesel, vzrůstající množství bezpečnostních incidentů vzhledem k růstu podniku, úniku a ohrožení citlivých dat a neefektivity podnikových procesů. Vše je opět detailně popsáno a okomentováno.

Závěrem této práce byla provedena případová studie, jejímž cílem je nalezená významná rizika významně ošetřit. Byla tedy navržena vhodná opatření, která zmíněná rizika co nejvíce zmírňují a zároveň mají významný vliv na větší množství těchto rizik. Jednotlivá opatření jsou popsána včetně upřesňujícího doporučení a obsahují také seznam rizik, která mají za úkol zmírnit. Mezi navržená opatření patří například zavedení politiky bezpečnosti informací, tvorba IT směrnic, modernizace podnikové domény, přechod na systém správy konstrukční dokumentace a analýza podnikových procesů.

Obecný cíl práce je naplněn pomocí metodicky zpracované analýzy rizik a následnou případovou studií, která doporučuje provést několik více či méně náročných změn vedoucích k poměrně výraznému zlepšení informační bezpečnosti podniku. Logickou návazností na tuto práci je tedy projednání výsledků práce s vedením podniku. Jako další se nabízí zavedení prvního zmíněného opatření, politiky bezpečnosti informací, která může představovat první reálný krok směrem k získání certifikátu ISO/IEC 27001.

9. Seznam informačních zdrojů

1. ALEBRAHIM, Azadeh, et al. 2014. Pattern-based and ISO 27001 compliant risk analysis for cloud systems: treaties and international agreements registered or filed and recorded with the Secretariat of the United Nations. 2014 IEEE 1st International Workshop on Evolving Security and Privacy Requirements Engineering (ESPRE). Boston, MA: IEEE, 2014, vol. 26, 5-6, s. 42-47. DOI: 10.1109/ESPRE.2014.6890527.
2. An Introduction to ISO 27001, ISO 27002....ISO 27008. 2013. The ISO 27000 Directory [online]. [cit. 2014-12-03]. Dostupné z: http://www.27000.org/
3. BECKERS, et al. 2014. ISMS-CORAS: A structured method for establishing an ISO 27001 compliant information security management system. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). Switzerland: Springer International Publishing Switzerland, 2014, s. 315-344. 8431. ISSN 03029743.
4. BECKERS, Kristian, et al. 2011. Pattern-Based Support for Context Establishment and Asset Identification of the ISO 27000 in the Field of Cloud Computing. Sixth International Conference on Availability, Reliability and Security. IEEE, 2011, s. 327-333. DOI: 10.1109/ARES.2011.55.
5. Businessballs. 2012. SWOT analysis: SWOT analysis method and examples, with free SWOT template. Businessballs.com [online]. [cit. 2015-03-30]. Dostupné z: http://www.businessballs.com/swotanalysisfreetemplate.htm
6. CSIRT. 2015. Zákon o kybernetické bezpečnosti. Csirt.cz [online]. [cit. 2015-03-22]. Dostupné z: https://www.csirt.cz/page/2630/zakon-o-kyberneticke-bezpecnosti/
7. ČERMÁK, Miroslav. 2013. Analýza rizik: Jemný úvod do analýzy rizik [online]. [cit. 2015-03-20]. Dostupné z:

http://www.cleverandsmart.cz/analyza-rizik-jemny-uvod-do-analyzy-rizik/

8. ČESKO. 2015. Zákon č. 101/2000 Sb., o ochraně osobních údajů. In: Sbírka zákonů České republiky. Dostupné z: https://www.uoou.cz/zakon-c-101-2000-sb-o-ochrane-osobnich-udaju-a-o-zmene-nekterych-zakonu-ve-zneni-ucinnem-od-1-ledna-2015/ds-3109/
9. ČESKO. 2014. Zákon 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů. In: Sbírka zákonů České republiky. Dostupné z: http://portal.gov.cz/app/zakony/download?idBiblio=82522&nr=181~2F2014~20Sb.&ft=pdf
10. DOUCEK, Petr et al., 2011. Řízení bezpečnosti informací: 2. rozšířené vydání o BCM. 2., přeprac. vyd. Praha: Professional Publishing, 286 s. ISBN 978-80-7431-050-8.
11. FAL', A. M., el al. 2010. Standardization in information security management: Compliance, governance and risk management. Cybernetics and Systems Analysis. Boston, MA: Springer US, 2010, vol. 46, issue 3, s. 512-515. DOI: 10.1007/s10559-010-9227-9.
12. FENZ, Stefan, et al. 2007. Information Security Fortification by Ontological Mapping of the ISO/IEC 27001 Standard. 13th Pacific Rim International Symposium on Dependable Computing (PRDC 2007). IEEE, 2007, s. 381-388. DOI: 10.1109/PRDC.2007.29.
13. GARTNER. 2013. Gartner IT Key Metrics Data: 2013 IT enterprise summary report [online]. [cit. 2015-03-20]. Dostupné z: http://itsurvey.gartner.com/itsurveydocs/itkmd13enterprisesummaryreport.pdf
14. GIKAS, Constantine, et al. 2010. A General Comparison of FISMA, HIPAA, ISO 27000 and PCI-DSS Standards. Information Security Journal: A Global Perspective. IEEE, 2010-06-08, vol. 19, issue 3, s. 132-141. DOI: 10.1080/19393551003657019.

15. GUTIÉRREZ-MARTÍNEZ, Josefina, et al. 2010. Business Model for the Security of a Large-Scale PACS, Compliance with ISO/27002: 2013 Standard. Journal of Digital Imaging. Boston, MA: Springer US, 2010, vol. 30, issue 6, s. -. DOI: 10.1007/s10278-014-9746-4.
16. HARRIS, Shon et al., 2008. Hacking: manuál hackera. 1. vyd. Praha: Grada, 399 s. ISBN 978-80-247-1346-5.
17. HLAVA, Tomáš. 2011. Testování bílé a černé skříňky (white box, black box, grey box). Testování softwaru [online]. [cit. 2015-01-09]. Dostupné z: http://testovanisoftwaru.cz/druhy-typy-a-kategorie-testu/testovani-bile-a-cerne-skrinky-white-box-black-box-grey-box/
18. HOY, Zoé, et al. 2014. A structured approach to integrating audits to create organisational efficiencies: ISO 9001 and ISO 27001 audits. Total Quality Management. Boston, MA: Springer US, 2014-01-08, vol. 26, 5-6, s. 690-702. DOI: 10.1080/14783363.2013.876181.
19. HUMPHREYS, Edward, et al. 2008. Information security management standards: Compliance, governance and risk management. Information Security Technical Report. Boston, MA: Springer US, 2008, vol. 13, issue 4, s. 247-255. DOI: 10.1016/j.istr.2008.10.010.
20. Legislativní pohled na napadání sítí v České republice. 2010. Security-portal.cz [online]. [cit. 2015-02-19]. Dostupné z: http://www.security-portal.cz/clanky/legislativní-pohled-na-napadání-sítí-v-české-republice
21. MIKO, Karel. 2013. Interpretace výsledků penetračních testů. DCIT [online]. [cit. 2015-02-01]. Dostupné z: http://www.dcit.cz/cs/system/files/CIMIB_Penetracni-testy.pdf
22. NCKB. 2011. Co je NCKB. Národní Centrum Kybernetické Bezpečnosti [online]. [cit. 2015-01-09]. Dostupné z: https://www.govcert.cz/cs/
23. NEUBAUER, Thomas, et al. 2008. Interactive Selection of ISO 27001 Controls under Multiple Objectives. Proceedings of The Ifip Tc 11 23rd International Information Security Conference. Boston, MA: Springer US, 2008, vol. 19, issue 3, s. 477. DOI: 10.1007/978-0-387-09699-5_31.

24. OZKAN, Sevgi, et al. 2010. Collaborative risk method for information security management practices: A case context within Turkey. International Journal of Information Management. Boston, MA: Springer US, 2010, vol. 30, issue 6, s. 567-572. DOI: 10.1016/j.ijinfomgt.2010.08.007.
25. PŘIBYL, Tomáš. 2010. Penetrační testy a webové aplikace. ICTSecurity.cz [online]. [cit. 2015-03-13]. Dostupné z: http://www.ictsecurity.cz/10/11/1-webova-bezpecnost/penetracni-testy-a-webove-aplikace.html
26. SAKÁL, Peter, Libor PAŠEK a Juraj JAKUBIČKA. 2010. SWOT analýza [online]. Trnava, [cit. 2015-03-25]. Dostupné z: Ústavu priemyselného inžinierstva a manažmentu a kvality. Semestrálna práca. Slovenská Technická Univertiza Bratislava.
27. SHOJAIE, Bahareh, et al. 2014. Evaluating the Effectiveness of ISO 27001: 2013 Based on Annex A. 2014 Ninth International Conference on Availability, Reliability and Security. Boston, MA: IEEE, 2014, vol. 26, 5-6, s. 259-264. DOI: 10.1109/ARES.2014.41.
28. SO, Idris Gautama, et al. 2014. Action Design of Information Systems Security Governance for Bank Using COBIT 4.1 and Control Standard of ISO 27001: treaties and international agreements registered or filed and recorded with the Secretariat of the United Nations. Advanced Materials Research. Boston, MA: IEEE, 2014, vol. 905, 5-6, s. 663-668. DOI: 10.4028/www.scientific.net/AMR.905.663.
29. ŠPIDLA, Aleš. 2014. Zákon o kybernetické bezpečnosti. Ness.com [online]. [cit. 2014-12-19]. Dostupné z: http://web.ness.com/zokb-download?elq=f3e2f8f72256451ea6151b3d77cf43e3&elqCampaignId=209
30. ŠUTÁK, Martin a Dušan MACEK. 2008. GITY, a.s. Gity: Bezpečnost v kostce [online]. [cit. 2015-03-17]. Dostupné z: http://www.chrantesidata.cz/cs/art/1146-isms/

31. The history of ISO/IEC 27001. 2013. Gamma Secure Systems Limited [online]. [cit. 2015-12-22]. Dostupné z: http://www.gammassl.co.uk/27001/history.php
32. ÚNMZ. 2014. ČSN ISO/IEC 27000: Informační technologie – Bezpečnostní techniky - Systém řízení bezpečnosti informací - Přehled a slovník. Praha: ÚNMZ.
33. ÚNMZ. 2014. ČSN ISO/IEC 27001: Informační technologie – Bezpečnostní techniky - Systém řízení bezpečnosti informací - Požadavky. Praha: ÚNMZ.
34. ÚNMZ. 2014. ČSN ISO/IEC 27002: Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací. Praha: ÚNMZ.
35. ÚNMZ. 2011. ČSN ISO/IEC 27003: Informační technologie – Bezpečnostní techniky – Směrnice pro implementaci systému řízení bezpečnosti informací. Praha: ÚNMZ.
36. ÚNMZ. 2011. ČSN ISO/IEC 27004: Informační technologie – Bezpečnostní techniky – Řízení bezpečnosti informací - měření. Praha: ÚNMZ.
37. ÚNMZ. 2013. ČSN ISO/IEC 27005: Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací. Praha: ÚNMZ.
38. VYMAZAL, Michal a Jiří RICHTER. 2012. Penetrační testy. LINUXServices.cz [online]. [cit. 2015-03-17]. Dostupné z: http://www.linuxservices.cz/penetracni-testy
39. WANG, Chi-Hsiang a Dwen-Ren TSAI. 2009. Integrated installing ISO 9000 and ISO 27000 management systems on an organization. International Carnahan Conference on Security Technology. IEEE, 2009, s. 265-267. DOI: 10.1109/CCST.2009.5335527.

10. Přílohy

10.1. Seznam ilustrací

10.2. Seznam tabulek

10.3. Seznam grafů

10.4. Smlouva o utajení

Smlouva o utajení

1. Smluvní strany

a

- dále souhrnně jako „smluvní strany“

uzavírají níže uvedeného dne, měsíce a roku

smlouvu o utajení tohoto obsahu:

2. Úvodní ustanovení

Smluvní strany spolu spolupracují za účelem uzavření obchodní smlouvy. V rámci obchodních vztahů si smluvní strany poskytují důvěrné informace – tj. informace technického i netechnického charakteru, ať už souvisí s podnikáním či nikoliv, získané stranami v písemné, ústní nebo jiné hmotné či nehmotné formě.

Důvěrné informace mimo jiné zahrnují i obchodní tajemství, obchodní záznamy a plány, cenové struktury, objevy, nápady, koncepty, know-how, technické specifikace a informace o konstrukčním řešení výrobku, výkresy, náčrtky, modely, vzorky, výrobky, vývojové diagramy, počítačové programy a sestavy, diskety, jména zákazníků či dodavatelů, výsledky zkoušek a jiné majetkové informace.

Důvěrné informace nezahrnují:

a) Informace veřejně dostupné a známé v okamžiku obdržení nebo informace, které se později stanou takto dostupnými bez zavinění smluvní strany, která je obdrží.
b) Informace, které již smluvní strana má ještě před jejich získáním od smluvní strany, která je poskytuje, pod podmínkou, že informace nejsou získány protiprávním jednáním té smluvní strany, která informace získává, a že takové informace nejsou vázané podmínkou utajení.
c) Informace výslovně schválené druhou smluvní stranou ke zveřejnění.
d) Informace nezávisle vytvořené některou smluvní stranou jinak než v souvislosti s touto smlouvou.
e) Informace, které jsou vyžádány soudem, státním zastupitelstvím, věcně příslušným správním orgánem, vždy na základě zákona.

Důvěrné informace, uvedené výše v této smlouvě, jsou důvěrné a považovány za obchodní tajemství ve smyslu ust.§ 504 zák.č. 89/2012 Sb., Občanského zákoníku (dále jen „NOZ“). Proto uzavřeli účastníci tuto smlouvu o podmínkách, za kterých si smluvní strany v tomto rozsahu zpřístupní své obchodní tajemství a důvěrné informace (dále v textu smlouvy označované souhrnně též jen jako „důvěrné informace“ nebo „obchodní tajemství“).

Obchodní tajemství a důvěrné informace, dle ust.§ 504 NOZ touto smlouvou chráněné, tvoří veškeré skutečnosti technické, ekonomické, právní a výrobní povahy ve hmotné či nehmotné formě, které byly smluvní stranou takto řádně označeny a byly poskytnuty druhé smluvní straně. Tyto skutečnosti nejsou v příslušných obchodních kruzích zpravidla běžně dostupné a obě strany smlouvy mají zájem na jejich utajení a na odpovídajícím způsobu jejich ochrany.

3. Předmět smlouvy

3.1. Smluvní strany se zavazují v rámci své obchodní spolupráce nakládat s důvěrnými informacemi druhé smluvní strany tak, že budou respektovat a dodržovat jejich důvěrný charakter ve smyslu ust.§ 504 NOZ, jakož i respektovat a chránit obchodní tajemství druhé smluvní strany. V této souvislosti se zavazují, že veškeré skutečnosti, spadající do oblasti obchodního tajemství a důvěrné informace nebudou dále rozšiřovat nebo reprodukovat. Smluvní strany se zejména zavazují:

a) Nesdělit třetím osobám důvěrné informace druhé smluvní strany ani údaje, které jsou předmětem obchodního tajemství druhé smluvní strany.
b) Zajistit, aby důvěrné informace a obchodní tajemství nebyly zpřístupněny třetím osobám.
c) Zabezpečit listiny, včetně jejich fotokopií, obsahující informace, na které se vztahuje tato smlouva, před zneužitím třetími osobami.
d) Nevyužívat know how a podkladů předaných druhé smluvní straně pro vlastní obchodní činnost, která má konkurenční charakter vůči dotčené smluvní straně.

3.2. Smluvní strany jsou oprávněny použít důvěrných informací, na které se vztahuje tato smlouva, pouze za účelem plnění závazků a oprávnění v souladu se smlouvou uzavřenou s druhou smluvní stranou. Ve všech případech jsou smluvní strany oprávněny chráněné informace zpřístupnit pouze subjektu, který prokáže své oprávnění příslušnou informaci obdržet, případně subjektu, který s dotčenou smluvní stranou má uzavřenu obdobnou smlouvu o utajení informací, nebo na podkladě předchozího písemného souhlasu od této smluvní strany a za podmínek v něm specifikovaných. Pokud smluvní strana poskytnutí informací třetí straně povolí, je příslušná smluvní strana povinna zajistit utajení informací v souladu s touto smlouvou.

3.3. Smluvní strany přejímají povinnost zavázat k respektování a dodržování obchodního tajemství a utajování důvěrných informací druhé smluvní strany své zaměstnance a přijmout účinná opatření pro zamezení úniku chráněných informací.

4. Ostatní práva a povinnosti a důsledky porušení smlouvy

4.1. Oba účastníci smlouva se zavazují, že zabezpečí, aby dokumenty, obsahující obchodní tajemství nebo důvěrné informace, byly řádně evidovány.

4.2. Nedodržení této dohody kteroukoli ze smluvních stran se považuje za podstatné porušení této smlouvy a porušení povinnosti zachovávat důvěrné informace a porušení práva na ochranu obchodního tajemství.

4.3. Pokud se některá smluvní strana dozví o neoprávněném poskytnutí, úniku nebo zneužití majetkových informací, je povinna bez prodlení informovat druhou smluvní stranu.

4.4. V případě jakéhokoliv prokázaného porušení této smlouvy se porušující smluvní strana zavazuje zaplatit poškozené smluvní straně smluvní pokutu ve výši 500.000 Kč (slovy pětsettísíckorunčeských) za každý jednotlivý případ porušení povinností a to k vyúčtování poškozené smluvní strany, v době splatnosti ve vyúčtování uvedené. Tím není dotčeno právo poškozené smluvní strany na náhradu škody, a to v plné výši vedle smluvní pokuty, včetně ušlého zisku, z důvodu porušení závazku ze strany smluvní strany či osob, které ke spolupráci přizvala, a za které vůči této smluvní straně odpovídá.

5. Ostatní ujednání

5.1. Poskytnutí informací tvořících obchodní tajemství nebo důvěrných informací nezakládá právo na licenci, ochrannou známku, patent, právo užití nebo šíření autorského díla, ani jakékoliv jiné právo duševního nebo průmyslového vlastnictví. Chráněné informace, které mohou být zveřejněny smluvní stranou postupem a v souladu s touto smlouvou, nesmí obsahovat žádné údaje, záruky, jistiny nebo ručení, které by byly v rozporu s právy ochranných známek, patentovými právy, autorskými právy nebo dalšími právy duševního vlastnictví.

5.2. Veškeré chráněné informace, které dle této smlouvy smluvní strany poskytnou, jsou a zůstanou vlastnictvím dané smluvní strany a budou druhé smluvní straně vráceny po ukončení jejich smluvního vztahu.

5.3. Smluvní strany berou na vědomí, že jsou oprávněny použít prostředky právní ochrany proti nekalé soutěži.

6. Trvání a ukončení smlouvy

6.1. Tato smlouva vstupuje v platnost dnem jejího podpisu a končí v okamžiku, kdy budou všechny získané informace veřejně dostupné. To platí i v případě, že smluvní vztah mezi smluvními stranami skončí dříve.

7. Závěrečná ustanovení

7.1. Účastníci této smlouvy tímto vzájemně prohlašují a stvrzují svými podpisy, že si tuto smlouvu řádně zvážili, jejímu obsahu porozuměli, a že vyjadřuje jejich pravou, skutečnou a svobodnou vůli.

Smlouva je sepsána ve dvou vyhotoveních, z nichž každá ze stran obdrží po jednom z nich. V případě sporu, se účastníci budou řídit platným právem České republiky

7.2. Smlouva je uzavřena a nabývá účinnosti okamžikem jejího podpisu smluvními stranami.

10.5. Zadání práce

FIM UHK
UNIVERZITA HRADEC KRÁLOVÉ
Fakulta informatiky a managementu
Rokitanského 62, 500 03 Hradec Králové, tel: 493 331 111, fax: 493 332 235

Zadání k závěrečné práci

Jméno a příjmení studenta: **Tomáš Stránský**

Obor studia: Aplikovaná informatika (2)
Jméno a příjmení vedoucího práce: **Josef Horálek**

Název práce:
Bezpečnost podnikové IT infrastruktury a implementace ISO 2700

Název práce v AJ:
Cyber security IT infrastructure ISO 27000 for company

Podtitul práce:

Podtitul práce v AJ:

Cíl práce: Cílem práce je navrhnout komplexní zabezpečení podnikové infrastruktury s využitím doporučení a požadavků ISO 27000.

Osnova práce:
1. Úvod
2. Představení normy ISO 27000
3. Využití penetračních testů pro detekci bezpečnostních hrozeb
4. Analýza bezpečnostních rizik ve firemním prostředí
5. Případová studie - komplexní návrh zabezpečení podnikové infrastruktury
6. Závěr

Projednáno dne:

Podpis studenta Podpis vedoucího práce