Název předmětu: Kybernetická bezpečnost

Téma: 3. Systém řízení bezpečnosti informací (ISMS)

Cíl: Cílem je seznámit studenty se základním pojetím systému řízení bezpečnosti informací (ISMS) podle ISO 27001

Úkoly pro samostatnou práci: zopakovat si základní pojmy z oblasti kybernetické bezpečnosti a pochopit základní procesy řízení bezpečnosti informací.

Studijní literatura:

1. JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.
2. HROMADA, Martin; HRŮZA, Petr; KADERKA, Josef; LUŇÁČEK, Oldřich; NEČAS, Miroslav; PTÁČEK, Bohumil; SKORUŠA, Leopold; SLOŽIL, Richard. *Kybernetická bezpečnost: teorie a praxe.* Praha: Powerprint s.r.o., 2015, 250 s. ISBN 978-80-87994-72-6.
3. HRŮZA, Petr; PITAŠ, Jaromír; ŠANDA, Jaroslav; BRECHTA, Bohumil. *Kybernetická bezpečnost II.* Brno: Univerzita obrany, Brno, 2013, 100 s. ISBN 978-80-7231-931-2.
4. HRŮZA, Petr. *Kybernetická bezpečnost.* Brno: Univerzita obrany, 2012, 90 s. ISBN 978-80-7231-914-5.
5. Vydané normy ISO/ČSN řady 27000, platné zákony a vyhlášky z oblasti kybernetické bezpečnosti

Obsah:

<u>Pojmy</u>

Aktivum (Asset) je cokoliv, co má pro organizaci hodnotu.

Bezpečnost informací (Information security) je ochrana důvěrnosti, integrity a dostupnosti informací.

Dostupnost (Availability) je zajištění toho, že informace a s nimi spojená aktiva jsou uživatelům přístupná v době, kdy je požadují.

Dopad (Impact) je výsledek nežádoucího incidentu.

Důvěrnost (Confidentiality) je zajištění toho, že informace je přístupná jen těm, kteří jsou oprávněni k ní mít přístup.

Hodnocení rizik (Risk assessment) je posouzení pravděpodobnosti selhání bezpečnosti, které by se mohlo vyskytnout působením hrozeb a zranitelností a dopady na konkrétní aktiva.

Hodnocení aktiv (Asset assessment) je stanovení hodnoty aktiva v závislosti na posouzení dopadů na činnost organizace, které by mohly vyplynout ztráty důvěrnosti, integrity nebo dostupnosti aktiv.

Hrozba (Threat) je potenciální příčina nežádoucího incidentu, který může mít za následek poškození systému nebo organizace.

Identifikace aktiva (Asset identification) je proces, který předchází vytvoření seznamu aktiv a určení vlastníka daného aktiva.

Informace (informační aktiva) jsou výsledné, tj. vybrané či jinak zpracované údaje (data), prezentované ve formě snadno čitelné, pochopitelné a využitelné subjektem, jemuž jsou určeny. Mohou být v elektronické formě nebo napsané (vytištěné) v listinné formě, vyřčené při jednání nebo zaznamenané na jiném médiu.

Integrita (Integrity) je zabezpečení přesnosti a kompletnosti informace a metod jejího zpracování.

Riziko (Risk) je potenciální možnost, že daná hrozba způsobí poškození nebo zničení aktiv.

Redukované riziko je riziko, kterému bude organizace čelit po implementaci všech opatření pro snížení rizik, vyplývající z analýzy rizik.

Vlastník aktiva je jednotlivec, jemuž byla vedením přidělena odpovědnost za produkci, vývoj, údržbu, použití a bezpečnost aktiv; neznamená to však, že by byl jejich skutečným vlastníkem a měl k nim vlastnická práva.

Zranitelnost (Vulnerability) je slabé místo aktiva nebo skupiny aktiv, které může být využito jednou nebo více hrozbami.

V dnešní době se již žádná organizace nemůže obejít bez řízení bezpečnosti informací. Bezpečnost informací se stala nedílnou součástí každodenního řízení a vnitřní kultury každé organizace. Abychom byli schopni řízení bezpečnosti informací cíleně, účinně a účelně rozvíjet, je třeba tento prvek řízení vnímat jako systém řízení bezpečnosti informací. Bezpečnost informačního systému je souhrn opatření k zabezpečení provozu informačního systému podle stanovených zásad a pravidel k ochraně jejich dat před neoprávněným narušením, změnou, zneužitím a užíváním.

Systém řízení bezpečnosti informací (ISMS - Information Security Management System) poskytuje model pro ustavení, implementování, zpracovávání, monitorování, přezkoumávání, udržování a zlepšování ochrany informačních aktiv, aby byly dosaženy cíle organizace na základě posouzení rizik a úrovních akceptace rizik organizace navržených k efektivnímu ošetření a řízení rizik. Jednoduše lze říci, že ISMS je efektivní dokumentovaný systém řízení a správy informačních aktiv s cílem eliminovat jejich možnou ztrátu nebo poškození. Úkolem ISMS je zavést pravidla a postupy pro řízení informační bezpečnosti organizace. Pro ISMS v rámci organizace musí být jednoznačně popsána organizace řízení, odpovědnost za informační bezpečnost řídících pracovníků všech stupňů, odborných orgánů a

rolí v systému bezpečnosti informací. Interpretace a implementace jednotlivých doporučení se však může výrazně lišit podle rozsahu systému, počtu uživatelů, způsobu zpracování dat, jejich hodnoty a především podle reálných bezpečnostních rizik. ISMS nebývá v malých a středních firmách popsána tak detailně, jako je tomu ve velkých firmách, zejména nadnárodních organizacích.

Procesy řízení bezpečnosti informací

Pro snazší pochopení základních procesů řízení bezpečnosti informací použijeme následující schéma, které vychází z ITIL (Information Technology Infrastructure Library).

1. Bezpečnostní politika
2. Analýza rizik
3. Plánování opatření
4. Provoz opatření
5. Monitorování a audity
6. Cíle a požadavky

Na základní procesy uvedené ve schématu provedeme mapování požadavků a povinné dokumentace ISMS podle normy ISO/IEC 27001.

1 Bezpečnostní politika

Deklarace cílů a požadavků na úroveň bezpečnosti v organizaci a stanovení rámce co, kdo a jakým způsobem se má dosáhnout.

- **Rozsah ISMS** [ISO/IEC 27001 - 4.2.1 a)]
- **Politika ISMS** [ISO/IEC 27001 - 4.2.1 b)]

2 Analýza rizik

Identifikace a hodnocení aktiv jejich vlastníky, identifikace a hodnocení hrozeb, zranitelností a dopadů na aktiva (ztráta důvěrnosti, integrity a/nebo dostupnosti).

- **Metodika hodnocení rizik** [ISO/IEC 27001 - 4.2.1 c)]
- **Zprávy o hodnocení rizik** [ISO/IEC 27001 - 4.2.1 d) – g)]

3 Plánování opatření

Souhrn rozhodnutí, jakým způsobem bude naloženo s identifikovanými riziky. Vymezení odpovídajících činností, zdrojů, odpovědností a priorit pro zvládání rizik bezpečnosti informací.

- **Prohlášení o aplikovatelnosti** [ISO/IEC 27001 - 4.2.1 j)]
- **Plán zvládání rizik** [ISO/IEC 27001 - 4.2.2 a) – b)]

4 Provoz opatření

Popis toho, jakým způsobem provádět zavedená opatření. Souhrn všech záznamů, které poskytují objektivní důkaz o provozování zavedeného ISMS (typicky systémy pro správu úkolů a schvalování).

- **Dokumentované postupy opatření** (směrnice) [ISO/IEC 27001 - 4.2.2 c)]
- **Záznamy** (listinné i elektronické) [ISO/IEC 27001 - 4.3.3, 5]

5 Monitorování a audity

Pravidelná přezkoumávání účinnosti opatření s ohledem na výsledky bezpečnostních auditů, incidentů, výsledků měření účinnosti opatření, návrhů a podnětů všech zainteresovaných stran.

- **Zprávy z interních auditů** [ISO/IEC 27001 - 6]
- **Přezkoumání ISMS vedením organizace** [ISO/IEC 27001 - 7]
- **Nápravná a preventivní opatření** [ISO/IEC 27001 - 8]

MODEL PDCA (DEMINGŮV CYKLUS)

Cyklus PDCA byl původně vytvořen Walterem Shewhart v roce 1930. Následně PDCA pro zlepšování jakosti využil a rozpracoval Edwards Deming. PDCA model by měl být součástí znalostí každého poradce, jež pracuje v oblastech systémů kvality, ekologických systémů nebo zajištění bezpečnosti.

Jde o metodu postupného zlepšování například kvality výrobků, služeb, procesů, aplikací či dat, která se skládá ze čtyř po sobě následujících a opakujících se kroků.

MODEL PDCA (DEMINGŮV CYKLUS)

- plan (plánuj) – cyklus začíná získáváním informací a popisem řešeného problému, které slouží pro připravení plánu. Plán by měl obsahovat jednotlivé činnosti, které je třeba udělat k odstranění problému nebo zavedení změny
- do (dělej) – realizace plánu stanovených činností,
- check (kontroluj) – následuje sledování dosažených výsledků a jejich porovnání s plánem. Jedná se tedy o kontrolu, zda je původní problém nebo změna začala řešit
- act (jednej) – úpravy záměru i vlastního provedení na základě ověření a plošná implementace zlepšení do praxe, všechny potřebné změny zavést do procesů/systému, přesvědčit se o jejich uplatňování

Plan (plánuj)

V rámci prvního kroku celého Demingova cyklu jde na základě předešlého prověření stávajících podmínek o stanovení cílů (ve většině případů se jedná o napravení dosavadních nedostatků). Zde také nechybí určení nezbytných úkolů, opatření, nástrojů a procesů, které nám budou napomáhat k dosažení právě oněch stanovených cílů.

Při prvním kroku, tedy při tvoření plánu, bychom neměli zapomínat také na návrhy konkrétních způsobů řešení a nejvhodnější z nich připravit k realizaci. V neposlední řadě musí být zajištěno personální obsazení projektu kvalifikovanými pracovníky.

V oblasti IT je proces plánování, dá se říct, nejdůležitější součástí celého procesu. Při zavádění nových systému je plánování nedílnou součástí, bez které by to zkrátka nešlo. Je třeba si předem určit, které systémy budeme zavádět, do kterých oblastí je budeme zavádět a jak už jsme zmínili, nesmíme zapomínat také na kvalifikovaný personál.

Poskytovatel IT služeb musí vytvořit, uplatnit a udržovat plán managementu služeb, který obsahuje:

- cíle, kterých chce poskytovatel služby dosáhnout,
- požadavky na služby,
- známá omezení, která mohou ovlivnit systém managementu služeb (SMS),
- politiky, standardy, zákonné a regulační požadavky a smluvní závazky,
- odpovědnosti a role v rámci procesů,
- lidské, technické, informační a finanční zdroje nezbytné k dosažení cílů SMS,
- další zúčastněné strany v procesu návrhu a přechodu nových nebo změněných služeb,
- rozhraní mezi procesy a jejich integrací s dalšími součástmi SMS,
- přístup k managementu rizik a kritéria pro akceptování rizik,
- technologie využívané pro podporu SMS,
- způsob měření, auditování, vykazování a zlepšování efektivnosti SMS a služeb.

Plán managementu služeb musí být přezkoumáván v plánovaných intervalech a aktualizován podle potřeby.

Do (dělej)

Poskytovatel služeb IT musí implementovat a provozovat SMS pro návrh, přechod, dodávku a zlepšování služeb podle plánu managementu služeb prostřednictvím činností, které zahrnují:

- přidělení a řízení finančních zdrojů a rozpočtů,
- zmocnění, odpovědnosti a role v rámci procesů,
- řízení lidských, technických a informačních zdrojů,
- identifikaci, vyhodnocení a management rizik služeb,
- řízení procesů managementu služeb,
- monitorování a vykazování výkonnosti činností v rámci managementu služeb.

Check (kontroluj)

Krok ověření je krokem kontroly. Nasbíraná data z předešlé fáze podléhají analýze a hlubšímu zkoumání. Reálné výsledky jsou porovnávané s výsledky očekávanými pro zjištění rozdílů. Hledají se odchylky implementace od plánu, přičemž je na reálných výstupech vyhodnocena vhodnost a úplnost plánu pro provedení celkového zdokonalení. Důležitou roli zde hraje i možnost grafického zpracování dat z několika po sobě následujících cyklů. Grafy umožňující

zobrazit trendy v tomto případě zjednodušují vypozorování nastaveného vývoje, z čehož se dají vyvodit důležité informace pro další postup.

Musí existovat dokumentovaný postup, kde budou stanoveny pravomoci a odpovědnosti pro plánování a provádění auditů, vykazování výsledků a udržování záznamů z auditů. Výběr auditorů a provádění auditů musí zajistit objektivitu a nestrannost auditu. Auditoři nesmějí auditovat svoji vlastní práci. Neshody musí být sdělovány, dále u nich musí být stanovena priorita a musí být přidělena odpovědnost za provedení opatření. Management, který je odpovědný za auditované oblasti, musí zajistit, aby jakékoliv nápravy a nápravná opatření byla přijata bez zbytečného prodlení, aby neshody a jejich příčiny byly odstraněny. Činnosti po auditu musí zahrnovat ověření přijatých opatření.

Vrcholový management musí přezkoumávat SMS a služby v plánovaných intervalech pro zajištění jejich trvalé vhodnosti a efektivnosti. Toto přezkoumání musí obsahovat posouzení příležitostí pro zlepšování a potřebu změn SMS, včetně politiky a cílů managementu služeb.

Přezkoumání managementu musí obsahovat přinejmenším informace o:

- zpětné vazbě od zákazníků,
- výkonnosti služeb a procesů,
- současné a budoucí odhadované úrovně lidských, technických, informačních a finančních zdrojů,
- rizicích,
- výsledcích a následných opatření z interních auditů a z přezkoumání managementu,
- změnách, které by mohly ovlivnit SMS a služby,
- příležitostech pro zlepšení.

Záznamy z přezkoumání managementu musí obsahovat rozhodnutí a opatření týkající se zdrojů, zlepšení efektivnosti SMS a zlepšení služeb.

Tento krok spočívá v implementaci vytvořeného plánu z prvního kroku, kdy dochází k realizaci navrženého řešení a zapracování nových procesů. Zároveň se přistupuje ke sběru a měření dat, respektive výsledků realizace pro jejich zpracování v dalších krocích, jimiž budou „zkontroluj“ a „jednej“. Žádná realizovaná změna není provedena bez patřičné dokumentace. A právě takové informace jsou důležité pro následující krok.

Act (jednej)

Krok jednání, nebo také akce, uzavírá celý cyklus. Je založen na jednoduchém a logickém postupu. Bylo-li v kroku ověření prokázáno, že realizace stanoveného plánu přinesla pozitivní výsledky zdokonalující původní standard, pak se tento postup uvedený v plánu stává novým standardem, podle kterého se bude organizace nadále řídit. Může však dojít i k situaci, kdy ověření neprokáže žádný pozitivní přínos nového plánu oproti původnímu standardu. V takovém případě se nepřistupuje na přechod k novému standardu a způsob řízení či realizace pracovního postupu vychází i nadále ze standardu původního.

Musí existovat politika neustálého zlepšování SMS a služeb. Tato politika zahrnuje kritéria hodnocení příležitostí pro zlepšování. Musí existovat dokumentovaný postup včetně pravomocí a odpovědností pro identifikování, dokumentování, vyhodnocení, schválení, stanovení priorit, řízení, měření a hlášení zlepšení. Příležitosti pro zlepšování, včetně nápravných a preventivních opatření musí být dokumentovány. Příčiny identifikovaných neshod musí být napraveny. Nápravná opatření musí být přijata za účelem odstranění příčiny identifikovaných neshod, aby se tak zabránilo jejich opakovanému výskytu. Preventivní opatření musí být přijata za účelem odstranění příčiny potenciálních neshod, aby se tak zabránilo jejich výskytu.

Příležitosti pro zlepšování musí mít stanoveny priority. Poskytovatel služeb musí při rozhodování o příležitostech pro zlepšování využívat kritéria hodnocení z politiky neustálého zlepšování.

Poskytovatel služeb musí řídit činnosti pro zlepšování, které musí obsahovat alespoň:

- stanovení cílů pro zlepšování v jedné nebo více oblastech týkajících se kvality, hodnot, kapacit, nákladů, produktivity, využití zdrojů a snížení rizik,
- zajištění, že schválená zlepšení jsou implementována,
- aktualizace politiky managementu služeb, plánů, procesů a postupů tam, kde je to potřebné,
- měření implementovaných zlepšení oproti stanoveným cílům, tam kde nejsou cíle dosaženy, přijímání potřebných opatření,
- reportování implementovaných zlepšení.

Výjimkou není ani moment, kdy krok ověření přinese něco naprosto neočekávaného, s čím plán nepočítal a nemělo z něj dle předpokladů vyplynout. Nezáleží na tom, jestli je zjištěný fakt pozitivní či negativní, v danou chvíli by neměl být trvale zaveden. Naopak by měl být zahrnut do nového cyklu PDCA tak, aby byl dodatečně detailně prostudován.

Některé zdroje popisující teorii PDCA cyklu uvádějí, že tento poslední krok zahrnuje i provedení úprav (anglický ekvivalent Adjustments). Toto tvrzení je nicméně zavádějící, neboť jde proti základní myšlence PDCA cyklu. Ta totiž říká, že každá změna musí být nejprve detailně naplánována, realizována, ověřena a až po prokázání jejího přínosu uvedena v nový standard. Jakékoli úpravy provedené až v závěrečném kroku tento koloběh tedy zcela porušují.

WILLIAM EDWARDS DEMING

William Edwards Deming byl americký statistik, který se narodil 14. října 1900 v městě Sioux City, ve státě Iowa. Deming proslul svojí průkopnickou prací statistického řízení v Japonsku, která je považována za jeho životní dílo. Podle Deminga byla pojmenována, mimo jiné, jedna z celosvětově nejuznávanějších cen udělovaných za jakost, takzvaná Demingova cena. V roce 1991 se stal členem Automobilové síně slávy (Automotive Hall of Fame), což je organizace založená pro ocenění významných osobností z oblasti vývoje automobilismu.

Pro naši situaci si Deminga připomeneme jakožto autora modelu PDCA. Sám Deming ovšem celé autorství odkazuje svému duchovnímu otci Walteru A. Shewhartovi (od něj také název Shewhartův cyklus). W. E. Deming ve své pozdější kariéře modifikoval model PDCA na model PDSA. Měl totiž dojem, že slovo „check“ zdůrazňuje spíše kontrolu nad celkovou analýzou.

William E. Deming umírá 20. prosince roku 1993 ve věku 93 let. Zemřel ve Washingtonu DC, hlavním městě Spojených států amerických.