Standardy a definice pojmů bezpečnosti informací

Robert Gogela, CISA, CISM

Lidská společnost se snaží na vše vytvořit normy a potom trestat ty, kdo normy porušují. Nikdo již ale nekontroluje, zda nám normy vyhovují a zda odpovídají situaci, ve které se nacházíme. Normální je normy dodržovat, proč ale lidé neustále normy porušují? Je to snad tím, že lidé nejsou normální, nebo je to tím, že normy nejsou normální a neodpovídají situaci? é Často dochází k tomu, že ten, kdo normy vytváří, je tvořit tak, aby vyhovovaly jemu, a je mu jedno, že nevyhovují druhým lidem!

Vít Kouba

1 Standardy bezpečnosti informací

1.1 Mezinárodní normy ISMS řady ISO/IEC 27xxx

1.1.1 Normy vydané ÚNMZ v českém jazyce

ČSN ISO/IEC 27000:2010
Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník

ČSN ISO/IEC 27001:2006
Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací ï Požadavky

ČSN ISO/IEC 17799:2006 (oprava označení na ISO/IEC 27002 vydána UNMZ v roce 2008)
Informační technologie - Bezpečnostní techniky - Soubor postupů pro management bezpečnosti informací

ČSN ISO/IEC 27004:2011
Informační technologie - Bezpečnostní techniky - ř ízení bezpečnosti informací - Měření

ČSN ISO/IEC 27005:2009
Informační technologie - Bezpečnostní techniky - ř ízení rizik bezpečnosti informací

ČSN ISO/IEC 27006:2008
Informační technologie - Bezpečnostní techniky - Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací

ČSN EN ISO 27799:2010
Zdravotnická informatika - Systémy řízení bezpečnosti informací ve zdravotnictví využívající ISO/IEC 27002

1.1.2 Další normy vydané v angličtině

ISO/IEC 27011:2008
Information technology ð Security techniques ð Information security management guidelines for telecommunications organizations based on ISO/IEC 27002

ISO/IEC 27031:2011
Information technology ð Security techniques ð Guidelines for information and communications technology readiness for business continuity

ISO/IEC 27033-1:2009
Information technology ð Security techniques ð Network security overview and concepts

ISO/IEC 27035:2011
Information technology ð Security techniques ð Information security incident management

1.2 Standardy pouğívané v USA

Federal Information Security Management Act of 2002 (ĂFISMAń)
Federální zákon o managementu bezpeļnosti informací. Vyğaduje, aby kağdý federální úŚad zavedl program bezpeļnosti informací a informaļních systémŢ, vļetnĎsluğeb poskytovaných nebo Śízených jiným úŚadem nebo dodavatelem.

FIPS PUB 199
Standardy pro kategorizaci bezpeļnosti federálních informací a informaļních systémŢ

FIPS PUB 200
Minimální poğadavky na bezpeļnost federálních informací a informaļních systémŢ

NIST Special Publications 800 series (NIST SP 800 series)
PŚíruļky pro posuzování, výbĎr a implementaci bezpeļnostních opatŚení v informaļních systémech a ICT technologiích

Zdroje: http://csrc.nist.gov/publications/PubsSPs.html

1.3 Standardy pouğívané ve Spolkové republice NĎmecko

BSI Standard 100-1: Information Security Management Systems (ISMS)

BSI-Standard 100-2: IT-Grundschutz Methodology

BSI-Standard 100-3: Risk Analysis based on IT-Grundschutz

BSI-Standard 100-4: Business Continuity Management

Zdroje: https://www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandards_node.html

2 Definice pojmŢ bezpeļnosti informací

Kapitola si klade za cíl seznámit ļtenáŚe se základními a ļasto pouğívanými pojmy bezpeļnosti informací, na jejichğ významu a obsahu se nezŚídka nedokáğe shodnout ani odborná veŚejnost.

2.1 Základní pojmy

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

Bezpeļnost informací (Information security) je ochrana dŢvĎrnosti, integrity a dostupnosti informací.

Dostupnost (Availability) je zajiğtĎní toho, ğe informace a s nimi spojená aktiva jsou uğivatelŢm pŚístupná v dobĎ, kdy je poğadují.

Dopad (Impact) je výsledek neğádoucího incidentu.

DŢvĎrnost (Confidentiality) je zajiğtĎní toho, ğe informace je pŚístupná jen tĎm, kteŚí jsou oprávnĎni k ní mít pŚístup.

Hodnocení rizik (Risk assessment) je posouzení pravdĚpodobnosti selhání bezpeļnosti, které by se mohlo vyskytnout pŢsobením hrozeb a zranitelností a dopady na konkrétní aktiva.

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

Hrozba (Threat) je potenciální pŠíļina neģádoucího incidentu, který mŢģe mít za následek poģkození systému nebo organizace.

Identifikace aktiva (Asset identification) je proces, který pŠedchází vytvoŠení seznamu aktiv a urļení vlastníka daného aktiva.

Informace (informaļní aktiva) jsou výsledné, tj. vybrané ļi jinak zpracované údaje (data), prezentované ve formĚ snadno ļitelné, pochopitelné a využitelné subjektem, jemuģ jsou urļeny. Mohou být v elektronické formĚ nebo napsané (vytištĚné) v listinné formĚ, vyŠļené pŠi jednání nebo zaznamenané na jiném médiu.

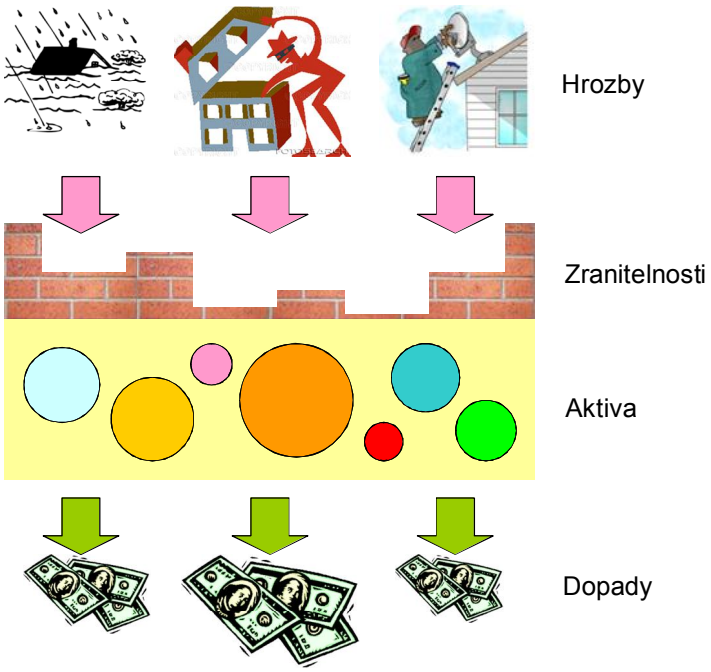
Integrita (Integrity) je zabezpeļení pŠesnosti a kompletnosti informace a metod jejího zpracování.

Riziko (Risk) je potenciální moģnost, ģe daná hrozba zpŢsobí poģkození nebo zniļení aktiv.

Redukované riziko je riziko, kterému bude organizace ļelit po implementaci vģech opatŠení pro sníģení rizik, vyplývající z analýzy rizik.

Vlastník aktiva je jednotlivec, jemuģ byla vedením pŠidĚlena odpovĚdnost za produkci, vývoj, údrģbu, použití a bezpeļnost aktiv; neznamená to vģak, ģe by byl jejich skuteļným vlastníkem a mĚl k nim vlastnická práva.

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

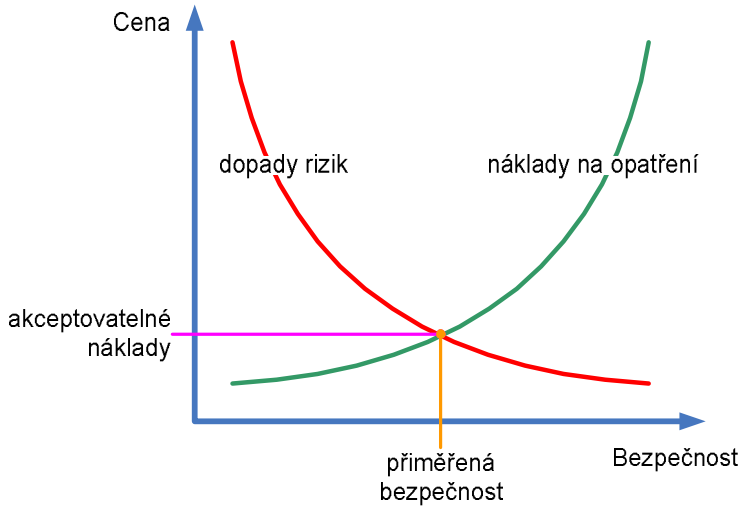


Základní pojmy bezpeļnosti informací

2.2 PŘimĚřená úroveň bezpečnosti

Zajištění bezpečnosti není hledáním dokonalého způsobu ochrany, ale aplikací takových opatření, která jsou přiměřená hodnotě předmětu ochrany (aktiv).

Primárním předmětem ochrany jsou informace (nikoliv jejich nosiče nebo prostředky pro zpracování). Čím vyšší hodnotu pro nás informace mají, tím vyšší pozornost musíme věnovat bezpečnosti jejich nosičů. Každá organizace by si proto měla provádět alespoň základní hodnocení a kategorizaci svých informací a tomu přizpůsobit i způsob jejich ochrany.



Zvažování rizik a opatření (analýza nákladů a přínosů)

Velikost úsilí a investic do bezpečnosti musí odpovídat hodnotě aktiv a míře možných rizik. Změny v procesech organizace při zavádění ISMS a při aplikaci opatření v ICT systémech musí dostatečně redukovat dopady možných rizik za akceptovatelných nákladů.

2.3 Procesy řízení bezpečnosti informací

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

Základní procesy řízení bezpečnosti informací dle ITIL

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

2.3.1 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)]

2.3.2 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)]

2.3.3 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)]

2.3.4 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]

2.3.5 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]