MANAGEMENT KYBERNETICKÉ BEZPEČNOSTI

TÉMA Č 2
ZÁKLADNÍ VÝCHODISKA A NORMY INFORMAČNÍHO MANAGEMENTU

pplk. Ing. Petr HRŮZA, Ph.D.
Univerzita obrany, Fakulta ekonomiky a managementu
Katedra vojenského managementu a taktiky
E-mail.: petr.hruza@unob.cz

Operační program Vzdělávání pro konkurenceschopnost

Projekt: ***Vzdělávání pro bezpečnostní systém státu***

(reg. č.: CZ.1.01/2.2.00/15.0070)

esf evropský sociální fond v ČR | EVROPSKÁ UNIE | MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY | OP Vzdělávání pro konkurenceschopnost | UNIVERZITA OBRANY

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

OBSAH

- ✓Základní pojmy.
- ✓Co je bezpečnost informací?
- ✓Proč je nezbytná bezpečnost informací.
- ✓Jak stanovit bezpečnostní požadavky.
- ✓Hodnocení bezpečnostních rizik.
- ✓Výběr opatření.
- ✓Východiska bezpečnosti informací.
- ✓Kritické faktory úspěchu.
- ✓Vytváření vlastních směrnic.
- ✓Struktura normy.
- ✓Normy rodiny 27k.
- ✓Závěr.

Literatura

Základní

- LUKÁŠ Luděk, HRŮZA Petr, KNÝ *Milan. Informační management v bezpečnostních složkách*. 1. vydání. Praha : Ministerstvo obrany České republiky, 2008. 214 s. ISBN: 978-80-7278-460-8

ČSN ISO/IEC 27000 Datum vydání : 1.5.2010

Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník.

ČSN ISO/IEC 27001 Datum vydání : 1.10.2006

Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky.

ČSN ISO/IEC 27002 / 17799 Datum vydání : 1.8.2006

Informační technologie - Bezpečnostní techniky - Soubor postupů pro management bezpečnosti informací.

ZÁKLADNÍ POJMY

- **aktivum** *(asset)*
- **opatření** *(control)*
- **prostředky pro zpracování informací** *(information processing facilities)*
- **bezpečnost informací** *(information security)*
- **bezpečnostní událost** *(information security event)*
- **bezpečnostní incident** *(information security incident)*
- **riziko** *(risk)*
- **analýza rizik** *(risk analysis)*
- **hodnocení rizik** *(risk assessment)*
- **vyhodnocení rizik** *(risk evaluation)*
- **management rizik** *(risk management)*
- **zvládání rizik** *(risk treatment)*
- **hrozba** *(threat)*
- **zranitelnost** (*vulnerability)*

Co je bezpečnost informací?

Informace jsou **aktiva**, která mají pro organizaci hodnotu. Je tedy nutné je vhodným způsobem chránit.

Informace mohou existovat v různých podobách. Mohou být **vytištěny** nebo **napsány na papíře**, uloženy v **elektronické podobě**, **posílány poštou** nebo **elektronickou cestou**, zachyceny na **film** nebo **vyřčeny** při konverzaci.

Proč je nezbytná bezpečnost informací?

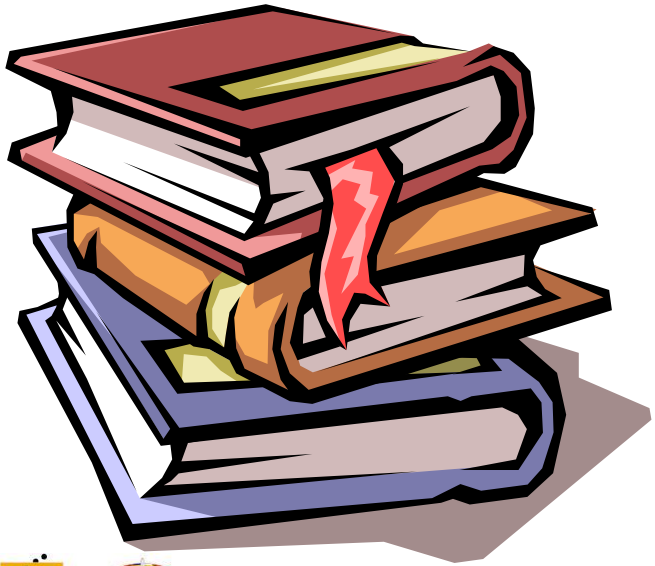
Bezpečnost informací je zaměřena na širokou škálu hrozeb a zajišťuje tak kontinuitu činností organizace, minimalizuje obchodní ztráty a maximalizuje návratnost investic a podnikatelských příležitostí.

Bezpečnosti informací lze dosáhnout implementací soustavy opatření, která mohou existovat ve formě pravidel, postupů, procedur, organizační struktury, programových a hardwarových funkcí.

Jak stanovit bezpečnostní požadavky?

Tři hlavní zdroje:

- hodnocení rizik,
- požadavky zákonů a podzákonných norem, smluvní ujednání a místní zvyklosti,
- konkrétní principy.



Hodnocení bezpečnostních rizik

Požadavky na bezpečnost jsou stanoveny za pomoci metodického hodnocení bezpečnostních **rizik**.

Výsledky hodnocení rizik pomohou určit vedení organizace odpovídající kroky i priority pro řízení bezpečnostních rizik u informací a pro realizaci opatření určených k zamezení jejich výskytu.

Hodnocení rizik by mělo být prováděno periodicky, aby bylo možné včas reagovat na jakékoliv změny v bezpečnostních požadavcích.

Výběr opatření

Pro pokrytí specifických potřeb mohou být vytvořena **zcela nová opatření**. Výběr konkrétních opatření je na rozhodnutí každé organizace.

Rozhodnutí je založeno na **kritériích** určujících akceptaci nebo zvládání rizika a celkovém přístupu organizace k řízení rizik.

Při výběru opatření by měla být zohledněna příslušná **národní a mezinárodní legislativa a regulace**.

Východiska bezpečnosti informací

Řada opatření může být považována za základní principy představující dobrá východiska pro implementaci bezpečnosti informací.

Opatření, která by měla být pro organizaci podstatná z pohledu legislativy, jsou:

a)ochrana osobních údajů;

b)ochrana důležité dokumentace organizace, jako například účetních záznamů;

c)ochrana duševního vlastnictví.

Východiska bezpečnosti informací

Opatření, považovaná za základ nejlepších praktik pro zajištění bezpečnosti informací, jsou:

a)dokument bezpečnostní politiky informací;

b)přidělení odpovědností v oblasti bezpečnosti informací;

c)vzdělávání, školení a zvyšování povědomí v oblasti bezpečnosti informací;

d)bezchybné zpracování v aplikačních systémech;

e)řízení technických zranitelností;

f)řízení kontinuity činností organizace;

g)zvládání bezpečnostních incidentů a kroky k nápravě.

Kritické faktory úspěchu

Pro úspěšnou implementaci bezpečnosti informací v organizaci jsou často kritické následující faktory:

a) bezpečnostní politika, bezpečnostní cíle a činnosti, které respektují cíle činností organizace;

b) přístup k zavádění, udržování, monitorování a zlepšování bezpečnosti informací v souladu s kulturou organizace;

c) zřetelná podpora a angažovanost ze strany vedení organizace;

d) dobré pochopení bezpečnostních požadavků, hodnocení a managementu rizik;

Kritické faktory úspěchu - pokračování

e) účinný marketing bezpečnosti vůči vedení organizace, zaměstnancům a jiným stranám;

f) rozšíření směrnic a norem bezpečnostní politiky informací mezi všechny zaměstnance, vedení organizace a třetí strany;

g) zdroje na financování činností souvisejících s řízením bezpečnosti informací;

h) realizace odpovídajících školení, vzdělávání a programů zvyšování povědomí;

i) zavedení procesu zvládání bezpečnostních incidentů;

j) komplexní a vyvážený systém pro ohodnocení míry účinnosti řízení bezpečnosti informací a získávání návrhů ke zlepšení na základě zpětné vazby.

Vytváření vlastních směrnic

Tento soubor postupů může být chápán jako východisko pro vytváření **specifických směrnic organizace.**

Ne všechna doporučení a opatření postupů mohou být použitelná.

Kromě toho mohou být nezbytná i další opatření.

Základní dokumenty IM

Základním koncepčním dokumentem informačního managementu je **Informační strategie**.

Informační strategie je vizí informačního systému organizace. Je promyšleným cílem, jehož by chtěla firma v oblasti výstavby a provozu informačního systému dosáhnout.

Základem zpracování informační strategie je zhodnocení **současného stavu informačního systému organizace, finančních a jiných možností organizace, obecného stavu informačních a komunikačních technologií.**

Struktura Informační strategie

- Úvod.
- Zdroje a východiska.
- Legislativní rámec a požadavky na IS.
- Výchozí stav – analýza stavu IS.
- Analýza veškerých vnitřních i vnějších podnikových procesů.
- Analýza pokrytí všech procesů automatizovaným zpracováním pomocí IS.

Struktura Informační strategie

- Analýza technologického zabezpečení IS.
- Analýza informačních potřeb.
- Cílový stav.
- Transformace do cílového stavu (navrhnout postup, jak dosáhnout cílového stavu ze současných podmínek).
- Závěr.

Cíle Informační strategie

Cílem dokumentu je stanovení globální strategie v oblasti informačních a komunikačních technologií, které se mají stát výkonným nástrojem pro podporu dosahování strategických cílů organizace. Informační strategie je rovněž základním nástrojem systémové integrace.

Vypracování Informační strategie je obvykle završeno oponentním řízením, kde se k předkládanému dokumentu vyjadřuje vedení organizace.

Informační strategie

Pokud vytvořením Informační strategie je pověřena externí organizace, musí vždy dojít k velmi těsné součinnosti mezi ní a zadávající společností. Externí organizace nemůže být totiž nikdy schopná sama o sobě (bez součinnosti) Informační strategii vytvořit.

Pokud v organizaci je již zaveden jakýkoliv informační systém, **musí** vlastnímu vytvoření Informační strategie předcházet audit IS/ICT. V každém případě pak Informační strategii předchází audit informačních potřeb.

Informační strategie

Na vlastní dokument by dále měla navázat **implementace Informační strategie:**

- rozpracování Informační strategie do cílového uspořádání IS/ICT,
- stanovení plánu, jak cílového stavu dosáhnout,
- vlastní realizace plánu.

Informační manager

Pro důsledné zajišťování informační strategie je potřebné určit jejího **zodpovědného reprezentanta** ve firmě. Roli reprezentanta zodpovědného za informační strategii firmy zastává obvykle **informační manažer**.

Monitoruje situaci uvnitř i vně firmy a na základě důkladné analýzy svých poznatků dokáže posoudit riziko jednotlivých akcí celé informační strategie firmy.

Informační manažer nebo jiný subjekt, odpovědný za informační strategii (například externí firma) pak odpovídá za kvalitu specifikace klíčových informací pro podporu rozhodování řídících pracovníků firmy a výběr standardů, které chce firma uplatňovat při budování informačního systému.

Shrnutí - Informační strategie

- Je klíčovým podkladem ke směřování rozvoje firmy v oblasti IS/ICT.
- Je důležitým podkladovým materiálem pro zpracování dokumentů, kterými firma oslovuje externí dodavatele IS/ICT.
- Definuje vazby mezi všemi projekty ve firmě, včetně projektů pro rozvoj informačních technologií.
- Urychluje řešení zavádění IS/ICT.
- Obsahuje koncepční podklady pro plánování nezbytných investic v oblasti IS/ICT na její pravidelnou údržbu.

Bezpečnostní politika

Bezpečnostní politika je souhrn požadavků, potřeb, pravidel, směrnic, předpisů a zásad, které jsou definovány pro zabezpečení všech prvků informačního systému na všech úrovních přístupu odpovídajících potřebám a možnostem firmy. Bezpečnostní politika informačního systému musí definovat hlavní cíle při ochraně informací, stanovit způsob řešení bezpečnosti a určit pravomoc zodpovědnosti. Definuje východiska pro všechny další aktivity firmy v oblasti informační bezpečnosti. Musí pokrývat všechny významné oblasti informační bezpečnosti.

Bezpečnostní politika

Při vytváření **bezpečnostní politiky** je potřeba stanovit úroveň detailu, faktografický rozsah a rozsah dokumentu, úroveň podrobnosti, definovat základní principy, odpovědnosti a pravomoci. Vytvořením bezpečnostní politiky práce nekončí. Tuto politiku je potřeba přijmout a vyhlásit. Po schválení vrcholovým managementem je důležité, aby byli všichni zaměstnanci s dokumentem seznámeni.

Informační politika

Informační politika je dlouhodobá koncepce rozvoje informačních a komunikačních technologií. Informační politika je nikdy nekončící a stále se vyvíjející proces, který ovlivňují technologické, ekonomické, sociální, kulturní a organizační faktory. Základním kritériem dělení jednotlivých informačních politik je způsob budování a provozování informačního systému organizace jako celku, případně autonomnost dílčích subsystémů (informačních systémů jednotlivých prvků organizace) a schopnost jejich vzájemné spolupráce.

Informační politika

V konečném důsledku se jedná o způsob budování informačního systému organizace, organizační strukturu zajišťující toto budování, způsob financování výstavby a provozu informačních systémů a schopnost spolupráce jednotlivých informačních systémů. Možnost či nemožnost sdílení dat je jedním znaků informační politiky uplatněné v dané organizaci. Míra definování a uplatnění informační politiky je odrazem kvality informačního managementu v organizaci. Je-li informační politika trvale pěstována a prosazována, zlepšuje se vlastní informační podpora řízení a postupně vzniká informačně založená organizace.

Monitoring a audit

Monitoring a audit informační bezpečnosti je nedílnou součástí procesu řízení informační bezpečnosti. Nedostatečná úroveň a absence monitoringu bývá příčinou, že bezpečnostní incidenty zůstávají dlouhou dobu neodhaleny a vzniklé škody pak mohou několikanásobně převýšit případné škody těchto incidentů odhalených včas. Monitoring stejně jako celý proces řešení bezpečnosti musí začít u analýzy největších rizik a sledování bezpečnostních událostí. Dodržování bezpečnostních standardů musí být tedy soustředěno do oblastí s největším rizikem.

Monitoring a audit

Společnost FreeDivision má na svých internetových stránkách velice výstižný citát:

„*I nejspolehlivější bezpečnostní systém je pouze teoretickou obranou proti útokům, dokud není vyzkoušen v praxi. Samozřejmě nemá smysl čekat na skutečný útok, ideální je řízená zkouška robustnosti a spolehlivosti bezpečnostních opatření, kterými firma chrání citlivá data*“.

FreeDivision s.r.o. , www.freedivision.com

Monitoring

K provádění účinného **monitoringu** informačního systému je nejprve nezbytné vydefinovat celkový rozsah monitoringu.

Je potřeba určit jaké informace, zdroje a citlivá místa mají být monitorována.

Dále je důležité vydefinovat a rozdělit odpovědnosti za monitoring. Kdo co bude dělat a za co bude odpovídat vedení firmy, bezpečnostní manažer, vlastní a externí zaměstnanci.

Penetrační testy

Mezi způsoby monitoringu informačního systému patří **penetrační testování**, které je založeno na aktivním zjišťování a odhalování bezpečnostních slabin systému.

Penetrační test je součást bezpečnostní analýzy. Je možné odhalit chyby v zabezpečení informačních systémů či aplikací a je možné zabránit úniku informací, poškození či zneužití. Výstupem penetračních testů je podrobná zpráva, která popisuje nalezené zranitelnosti, rizika s odhadem jejich míry dopadu. Penetrační testy je dobré pravidelně opakovat.

Audit - obecně

Audit obecně chápeme jako kritickou analýzu nebo hloubkovou kontrolu se zaměřením na zlepšení procesů v organizaci. Audit může pomoci při stanovení a případně dosažení cílů organizace, pokud je prováděn jako systematicko-metodický přístup k systému řízení, kontroly a správy organizace. V dnešní době je audit chápán jako synonymum hloubkové kontroly pro specifické oblasti.

Audit informačního systému

Audit informačního systému můžeme chápat jako **analýzu** informačního systému, jejímž cílem je posoudit, zda je systém ve shodě se stanovenými požadavky. Audit provádí nezávislá autorizovaná osoba nebo instituce, která nemá přímou odpovědnost za funkce prověřovaného systému. Audit můžeme vnímat také jako **záznam událostí a činností** vykonaných uživatelem nebo jeho jménem, důležitých z hlediska bezpečnosti informačního systému (tzv. bezpečnostní audit). Spolu s identifikací a autentizací slouží k určení zodpovědnosti při vyšetřování bezpečnostních incidentů.

Bezpečnostní audit

Bezpečnostní audit je zhodnocení stavu bezpečnosti vůči vybranému standardu.

Audit je prováděn **fyzicky přímo** na zkoumaném zařízení (např. serveru), nikoli vzdáleně po síti.

Audit vyžaduje **plný přístup** ke zkoumaným zařízením a je prováděn za asistence administrátora.

Hlavním cílem bezpečnostního auditu je zmapování aktuálního stavu bezpečnosti v rámci firmy, odhalení možných rizik a vytvoření základu pro případné ucelené bezpečnostní řešení (audit IS, penetrační testy, analýza rizik).

Bezpečnostní audit

Základem bezpečnostního auditu je pasivní sběr informací o konfiguraci a nastavení informačního systému. Posléze následuje vyhodnocení těchto informací a vyvození závěrů.

Výsledkem bezpečnostního auditu je porovnání zjištěných hodnot vůči hodnotám doporučeným a samostatná zpráva o každém zařízení.

Informační audit

Cílem **informačního auditu** je zhodnocení stavu informační podpory organizace jako takové, abstrahující od hodnocení informačního systému.

V jeho rámci se identifikují **informace**, které jsou **nezbytné k řízení organizace**, jsou-li poskytovány informačními zdroji, nedochází-li k **duplicitě zdrojů** v poskytování informací případně jejich **absenci**.

Informační audit

Informační audit by měl zahrnovat následující **kroky nebo fáze**:

- plánování,
- sběr údajů,
- analýzu údajů,
- hodnocení údajů,
- komunikační doporučení,
- implementační doporučení.

Informační audit

Firma by měla provádět audit informačního systému v plánovaných intervalech tak, aby si vždy minimálně dokázala odpovědět na následující otázky:

1. Vyhovuje stávající IS všem našim požadavkům?
2. Je náš IS zaveden a udržován efektivně?
3. Funguje nám IS tak, jak se od něho očekává?

Existují ještě **technický audit, audit informační strategie a legislativní audit**.

Plánování auditů

Program auditů musí být naplánován s ohledem na stav a význam auditovaných procesů a oblastí a také s ohledem na výsledky předchozích auditů.

Musí být definována **kritéria auditů, jejich rozsah, četnost a metody.**

Výběr auditorů a vlastní provedení auditů musí zajistit objektivitu a nestrannost procesu auditu.

Auditoři nesmí auditovat (prověřovat) svou vlastní práci.

Audit

Odpovědnosti a požadavky na plánování a provedení auditů, na hlášení výsledků a udržování záznamů musí být definovány dokumentovaným postupem.

Vedoucí zaměstnanci odpovědní za oblast, která je předmětem auditu, musí zajistit, že kroky na odstranění zjištěných nedostatků a jejich příčin budou prováděny bez zbytečného odkladu.

Norma ČSN ISO 19011, *Směrnice pro auditování systému managementu jakosti a/nebo systému environmentálního managementu*, může být dobrým zdrojem doporučení, jak provádět audity IS.

Monitoring a audit

Bez monitoringu a auditu není celkové řízení bezpečnosti komplexní.

Řada firem ale na tuto skutečnost často zapomíná a podceňuje ji.

Provozní řád

Co by určitě měl Provozní řád obsahovat?

Kdo všechno se jím musí ve firmě řídit a kdo ne?

Neměl by být každý uživatel vyškolen a neměl by prokázat způsobilost s užíváním IT a podepsat Provozní řád informačního systému dané firmy dříve, než mu bude přidělen přístup do informačního systému?

Může zaměstnanec pracovat s informačním systémem, aniž by absolvoval aspoň základní školení a podepsal, že byl obeznámen s Provozním řádem informačního systému?

Provozní řád informačního systému

1. ÚVODNÍ USTANOVENÍ

- Definice základních pojmů
- Správce informačního systému
- Provozovatel informačního systému
- Nakládání s informacemi
- Struktura informačního systému
- Odpovědnost organizačních a řídících struktur

Provozní řád informačního systému

2. PROVOZNÍ ŘÁD

- Obecné zásady práce s výpočetní technikou
- Práva a povinnosti uživatele
- Bezpečnostní zásady
- Provozní doba sítí
- Pohotovost pro uživatele
- Semináře, školení
- Archivace datových souborů
- Elektronická pošta
- Antivirová bezpečnost
- Používání Internetu
- Vytváření přístupů uživatelů k informačnímu systému
- Změna a rušení přístupů uživatelů k informačnímu systému
- Publikování informací

Provozní řád informačního systému

3. ZÁVĚREČNÁ USTANOVENÍ

- Určuje většinou platnost Provozního řádu, jeho novelizaci atp.

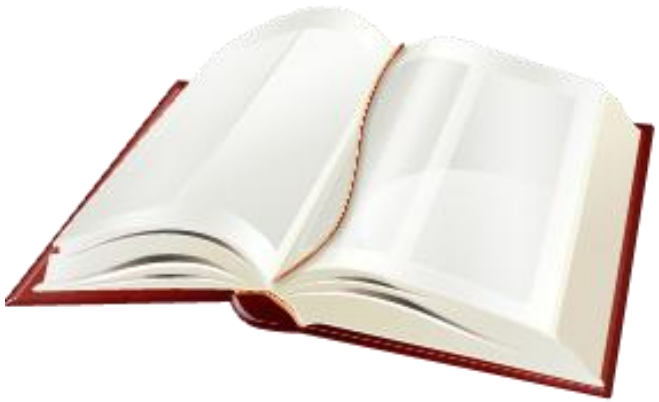
4. PŘÍLOHY

- Soupis případných příloh k Provoznímu řádu (Například: Výkladový slovník IS, Předávání dat IS, Protokol o instalaci klientského počítače, Protokol operativní evidence, Evidenční list, Požadavek na vytvoření přístupu k informačnímu systému pracovníka, Požadavek na zrušení přístupu a převod dat).

Struktura normy

Norma obsahuje celkem **11 základních oddílů**, které jsou dále rozděleny do **39 kategorií bezpečnosti.**

Každý z oddílů obsahuje jednu nebo více kategorií bezpečnosti.



Struktura normy

a) Bezpečnostní politika (1);
b) Organizace bezpečnosti (2);
c) Klasifikace a řízení aktiv (2);
d) Bezpečnost lidských zdrojů (3);
e) Fyzická bezpečnost a bezpečnost prostředí (2);
f) Řízení komunikací a řízení provozu (10);
g) Řízení přístupu (7);
h) Nákup, vývoj a údržba informačního systému (6);
i) Zvládání bezpečnostních incidentů (2);
j) Řízení kontinuity činností organizace (1);
k) Soulad s požadavky (3).

Struktura normy

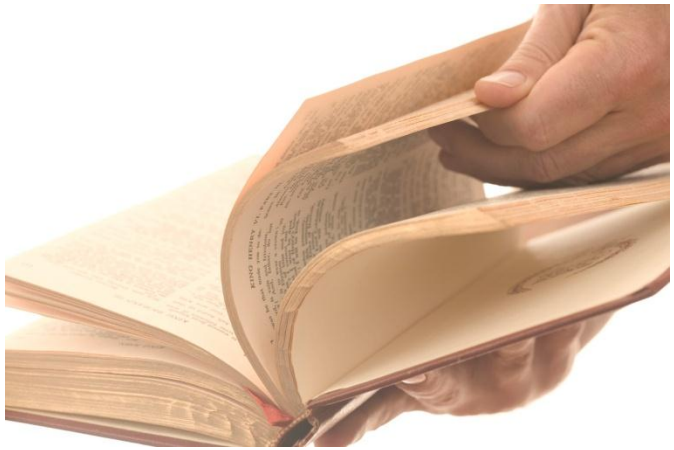
Každá z kategorií bezpečnosti obsahuje:

a) cíl opatření, určující čeho má být dosaženo;

b) jedno nebo více opatření, která lze použít k dosažení stanoveného cíle opatření.

Popis opatření je strukturován následovně:

- Opatření
- Doporučení k realizaci
- Další informace



ČSN ISO/IEC normy

Rodina **ČSN ISO/IEC norem 27k** je roztříděna na:

a) normy obsahující **přehled a terminologii,**

b) normy specifikující **požadavky**,

c) normy popisující **všeobecné směrnice**,

d) normy popisující **směrnice specifické podle sektorů**.

Normy obsahující přehled a terminologii

ISO/IEC 27000

Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník

Tato mezinárodní norma poskytuje organizacím a jednotlivcům:

a) přehled rodiny norem ISMS;

b) úvod k systémům řízení bezpečnosti informací (ISMS);

c) stručný popis procesu Plánuj - Prováděj (Dělej) – Kontroluj - Jednej (PDGA);

d) termíny a definice použité v rodině norem ISMS.

Normy specifikující požadavky

ISO/IEC 27001

Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky

Tato mezinárodní norma specifikuje **požadavky na ustavení, implementaci, provozování, monitorování, přezkoumávání a zlepšování formálně schválených systémů řízení bezpečnosti informací (ISMS)** v kontextu celkových obchodních rizik organizace.

Poskytuje normativní požadavky na vývoj a provoz ISMS, včetně sady kontrolních opatření pro řízení a zmírnění rizik spojených s informačními aktivy, které organizace vyhledává, aby je chránila provozováním ISMS.

Normy specifikující požadavky

ISO/IEC 27006

Informační technologie - Bezpečnostní techniky - Požadavky na orgány poskytující audit a certifikaci systémů řízení bezpečnosti informací

Tato mezinárodní norma specifikuje požadavky a poskytuje návod pro orgány poskytující audit a certifikaci ISMS

Normy popisující všeobecné směrnice

ISO/IEC 27002

Informační technologie - Bezpečnostní techniky - Soubor postupů pro řízení bezpečnosti informací

Tato mezinárodní norma poskytuje obecně akceptované kontrolní cíle a kontrolní opatření nejlepších praktik.

Poskytuje návod na implementaci kontrol bezpečnosti informací.

Normy popisující všeobecné směrnice

ISO/IEC 27003

Informační technologie - Bezpečnostní techniky - Návod k implementaci systému řízení bezpečnosti informací

Tato mezinárodní norma poskytuje praktický návod k implementaci a dále informace pro ustavení, implementaci, provozování, monitorování, přezkoumávání, udržování a zdokonalování ISMS .

Normy popisující všeobecné směrnice

ISO/IEC 27004

Informační technologie - Bezpečnostní techniky - Řízení bezpečnosti informací - Měření

Tato mezinárodní norma poskytuje návod a doporučení pro vývoj a použití měření za účelem posouzení efektivnosti ISMS, kontrolních cílů a kontrolních opatření použitých k implementaci a řízení bezpečnosti informací.

Normy popisující všeobecné směrnice

ISO/IEC 27005

Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací

Tato mezinárodní norma poskytuje směrnice pro řízení rizik bezpečnosti informací.

Poskytuje návod pro implementaci procesně orientovaného přístupu k řízení rizik, aby tak pomohla uspokojivě implementovat a naplnit požadavky na řízení rizik bezpečnosti informací.

Normy popisující všeobecné směrnice

ISO/IEC 27007

Informační technologie - Bezpečnostní techniky - Směrnice pro provádění auditu systémů řízení bezpečnosti informací

Tato mezinárodní norma poskytuje návod pro provádění auditů ISMS a poučení o pravomocích auditorů systému řízení bezpečnosti informací.

Poskytuje návod o rganizacím, které potřebují provádět interní a externí audity ISMS nebo řídit program auditu ISMS požadavků.

Normy popisující směrnice specifické pro sektory

ISO/IEC 27011

Informační technologie - Bezpečnostní techniky - Směrnice pro řízení bezpečnosti informací pro telekomunikační organizace na základě ISO/IEC 27002

Tato mezinárodní norma poskytuje směrnice podporující implementaci Řízení bezpečnosti informací v telekomunikačních organizacích.

Poskytuje telekomunikačním organizacím úpravu směrnic ISO/IEC 27002, týkajících se výhradně jejich průmyslového sektoru.

Normy popisující směrnice specifické pro sektory

ISO/IEC 27799

Informační technologie – Řízení bezpečnosti informací ve *zdravotnictví využívající ISO/IEC 27002*

Tato mezinárodní norma poskytuje směrnice podporující implementaci Řízení bezpečnosti informací ve zdravotnických organizacích.

Poskytuje zdravotnickým organizacím úpravu směrnic ISO/IEC 27002, týkajících se výhradně jejich průmyslového sektoru.

ZÁVĚR

Informace jsou **aktiva**, která mají pro organizaci hodnotu. Je tedy nutné je vhodným způsobem chránit.

Požadavky na bezpečnost jsou stanoveny za pomoci metodického hodnocení bezpečnostních rizik.

Norma obsahuje celkem **11 základních oddílů**, které jsou dále rozděleny do **39 kategorií bezpečnosti.**

Dotazy?

pplk. Ing. Petr HRŮZA, Ph.D.
Univerzita obrany, Fakulta ekonomiky a managementu
Katedra vojenského managementu a taktiky
E-mail.: petr.hruza@unob.cz