MANAGEMENT KYBERNETICKÉ BEZPEČNOSTI

TÉMA Č. 3
SYSTÉM ŘÍZENÍ BEZPEČNOSTI INFORMACÍ

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)

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

OBSAH

- ✓Základní pojmy
- ✓Co jsou informace?
- ✓Co je bezpečnost informací?
- ✓Co je ISMS?
- ✓Model ISMS - PDCA.
- ✓Zavádění a provoz ISMS.
- ✓Monitorování a údržba ISMS.
- ✓Realizace bezpečnostních opatření.
- ✓Norma ČSN ISO/IEC 27001.
- ✓Závěr

Literatura

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.

DOUCEK, Petr; NEDOMOVÁ, Lea; NOVÁK, Luděk; SVATÁ, Vlasta. ***Řízení bezpečnosti informací***. Druhé přepracované vydání, Praha : Professional Publishing, 2011, ISBN 978-80-7431-050-8.

POŽÁR, Josef. *Systém řízení informační bezpečnosti*. In Kný, Milan; Požár, Josef. ***Aktuální pojetí a tendence bezpečnostního managementu a informační bezpečnosti***. Brno : Tribun EU, 2010, s. 93 – 110. ISBN 978-807399-067-1.

ÚVOD

Veškeré informace uchovávané a zpracovávané organizací jsou ohroženy útokem, chybou, přírodními vlivy a jsou vystaveny zranitelnostem souvisícím s jejich používáním.

Ochrana informačních aktiv definováním, dosažením, udržováním a zlepšováním bezpečnosti informací je nezbytná pro to, aby organizace mohla dosáhnout svých cílů a udržovat a zlepšovat soulad s právními normami a svoji image. Tyto koordinované činnosti usměrňující implementaci vhodných kontrolních opatření a ošetřující nepřijatelná rizika bezpečnosti informací jsou všeobecně známa jako prvky **řízení bezpečnosti informací**.

ZÁKLADNÍ POJMY

- **řízení přístupu** (*access control*)
- **aktivum** (*asset*)
- **útok** (*attack*)
- **autentizace** (*authentication*)
- **autenticita** (*authenticity*)
- **dostupnost** (*availability*)
- **důvěrnost** (*confidentiality*)
- **řízení, kontrola** (*control*)
- **efektivnost** (*effectiveness*)
- **událost** (*event*)
- **směrnice** (*guideline*)

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

ZÁKLADNÍ POJMY

- **informační aktivum** (*information asset*)
- **bezpečnost informací** (*information security*)
- **bezpečnostní událost** (*information security event*)
- **bezpečnostní incident** (*information security incident*)
- **řízení bezpečnostního incidentu** (*infonnation security incident management*)
- **systém řízení bezpečnosti informací** (*information security management system*) - ISMS
- **riziko bezpečnosti informací** (*infonnation security risk*)
- **integrita** (*integrity*)
- **systém řízení** (*management system*)
- **nepopiratelnost** (*non-repudiation*)

ZÁKLADNÍ POJMY

- **postup** (*procedure*)
- **proces** (*process*)
- **záznam** (*record*)
- **spolehlivost** (*reliability*)
- **riziko** (*risk*)
- **analýza rizika** (*risk analysis*)
- **kritéria rizika** (*risk criteria*)
- **odhad rizika** (*risk estimation)*
- **hodnocení rizika** (*risk evaluation*)
- **řízení rizika** (*risk management*) - management rizika
- **hrozba** (*threat*)
- **zranitelnost** (*vulnerability*)

Co jsou informace?

1) Informace jsou **aktivum**.
2) Informace mohou být **uchovávány** v mnoha formách.
3) Informace mohou být **přenášeny** různými prostředky.
4) Informace jsou **závislé na informační a komunikační technologii.**

Co je bezpečnost informací?

Bezpečnost informací zahrnuje tři hlavní aspekty:

- důvěrnost,
- dostupnost ,
- integritu.

Bezpečnost informací se dosáhne implementací použitelné sady kontrol, vybraných zvoleným procesem řízení rizik a řízeným pomocí **ISMS**, zahrnujících k ochraně identifikovaných informačních aktiv politiky, procesy, postupy, organizační struktury, software a hardware.

Co je ISMS?

Systém řízení bezpečnosti informací 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.

ISMS – část celkového systému řízení organizace, založená na přístupu (organizace) k rizikům činností, která je zaměřena na ustanovení, zavádění, provoz, monitorování, přezkoumání, údržbu a zlepšování bezpečnosti informací.

Co je ISMS?

ISMS je efektivní dokumentovaný systém řízení a správy informačních aktiv s cílem eliminovat jejich možnou ztrátu nebo poškození tím, že:

- jsou určena aktiva, která se mají chránit,
- jsou zvolena a řízena možná rizika bezpečnosti informací,
- jsou zavedena opatření s požadovanou úrovní záruk a ta jsou kontrolována.

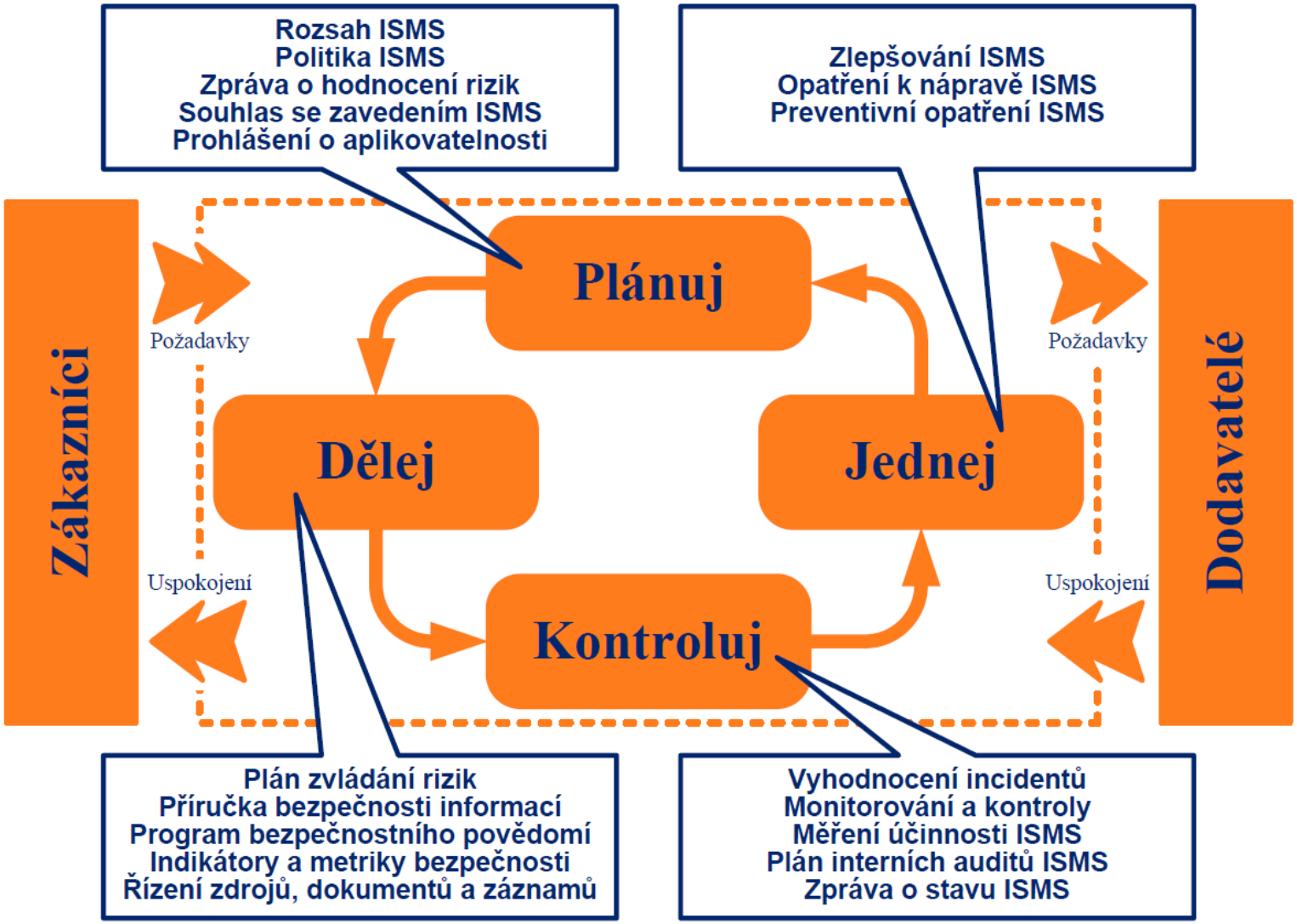
Model ISMS - PDCA

Model ISMS – PDCA (Plánuj – Dělej – Kontroluj – Jednej)

Čtyři etapy celého životního cyklu systému řízení:

- **Ustanovení ISMS –** cílem je upřesnit rozsah a hranice, kterých se řízení bezpečnosti týká, stanovit jasné manažerské zadání a na základě ohodnocení rizik vybrat nezbytná bezpečnostní opatření.
- **Zavádění a provoz ISMS –** cílem je účelně a systematicky prosadit vybraná bezpečnostní opatření do chodu organizace.
- **Monitorování a přezkoumání ISMS –** cílem je zajištění zpětné vazby a pravidelného sledování a hodnocení úspěšných i nedostatečných stránek řízení bezpečnosti informací.
- **Údržba a zlepšování ISMS –** cílem je realizace možností zlepšování systému řízení bezpečnosti informací ať už soustavným zlepšování systému nebo odstraňování zjištěných slabin a nedostatků.

Model ISMS - PDCA



Zavádění a provoz ISMS

- Zavést plánovaná bezpečnostní opatření a zformulovat příručku bezpečnosti informací.
- Definovat program budování bezpečnostního povědomí a provést přípravu a zaškolení všech uživatelů, manažerů a odborných pracovníků.
- Upřesnit způsoby měření účinnosti bezpečnostních opatření a sledovat stanovené ukazatele.
- Zavést postupy a další opatření pro rychlou detekci a reakci na bezpečnostní incidenty.
- Řídit zdroje, dokumenty a záznamy ISMS.

Přínosy zavedení a certifikace ISMS

- Přechod od nesystémového a neuceleného řízení bezpečnosti k bezpečnosti řízené a komplexní.
- Efektivní řízení investic vkládaných do bezpečnosti.
- Inventura vlastních aktiv, jejich ocenění a klasifikace.
- Řízené odstranění nebo snížení rizik v oblasti informačních systémů.
- Zavedení systémového a systematického přístupu při používání IT/IS
- Zvýšení povědomí a odpovědnosti zaměstnanců při práci s informacemi.
- Naplnění legislativních požadavků.
- Zvýšení důvěryhodnosti pro partnery.
- Trvalé monitorování a zlepšování systému řízení bezpečnosti informací.
- Konkurenční výhoda, kultivace Image a firemní kultury.

Monitorování a údržba ISMS

- Monitorovat a ověřit účinnost prosazení bezpečnostních opatření.
- Provést interní audity ISMS, jejichž náplň pokryje celý rozsah ISMS.
- Připravit zprávu o stavu ISMS a na jejím základě přehodnotit ISMS na úrovni vedení organizace.
- Zavádět identifikované možnosti zlepšení ISMS.
- Provádět odpovídající opatření k nápravě a preventivní opatření pro odstranění nedostatků.

Realizace bezpečnostních opatření

- Bezpečnostní politika.
- Organizace bezpečnosti.
- Řízení aktiv.
- Bezpečnost z hlediska lidských zdrojů.
- Fyzická bezpečnost a bezpečnost.
- Řízení komunikací a řízení provozu.
- Řízení přístupu.
- Akvizice, vývoj a údržba informačních systémů.
- Zvládání bezpečnostních incidentů.
- Řízení kontinuity činností organizace.
- Soulad s požadavky.

Realizace bezpečnostních opatření

Norma ČSN ISO/IEC 27001

Norma ČSN ISO/IEC 27001 poskytuje organizacím návod a požadavky na zavedení tzv. Systému managementu bezpečnosti informací (ISMS).

Obsahuje soubor pravidel pro ochranu a bezpečnost informačních aktiv (tedy nejen informací, ale např. klíčového hardwaru, softwaru, zaměstnanců, know-how atd.) uvnitř organizace.

ITIL - Information Technology Infrastructure Library

Information Technology Infrastructure Library (ITIL) je soubor konceptů a postupů, které umožňují lépe plánovat, využívat a zkvalitňovat využití informačních technologií (IT), a to jak ze strany dodavatelů IT služeb, tak i z pohledu zákazníků.

Seznam částí ITIL

- Podnikatelský pohled (*Business Perspectives*)
- Správa aplikací IT (*Application Management*)
- Dodávka IT služeb (*IT Services Delivery*)
- Podpora IT služeb (*IT Services Support*)
- Správa IT infrastruktury (*IT Infrastructure Management*)
- Řízení IT projektů (*IT Project Management*)

ZÁVĚR

Systém řízení bezpečnosti informací (Information Security Management System - ISMS) je dokumentovaný systém, ve kterém jsou chráněna definovaná informační aktiva, jsou řízena rizika bezpečnosti informací a zavedená opatření jsou kontrolována.

ISMS je efektivní dokumentovaný systém řízení a správy informačních aktiv s cílem eliminovat jejich možnou ztrátu nebo poškození.

Systém řízení se opírá o **čtyři hlavní systémové etapy**.

Při zavádění systému řízení bezpečnosti informací v organizaci se postupuje podle normy **ISO/IEC 27001**.

Dotazy?

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

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