MANAGEMENT KYBERNETICKÉ BEZPEČNOSTI

TÉMA Č. 4
SOUBOR POSTUPŮ PRO MANAGEMENT BEZPEČNOSTI INFORMACÍ – POLITIKA A ORGANIZACE 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)

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.
- ✓Politika bezpečnosti informací.
- ✓Organizace bezpečnosti informací.
- ✓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.

ČSN ISO/IEC 27002 / 17799 Datum vydání : 1.8.2006

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

ZÁKLADNÍ POJMY

- Bezpečnost informací
- Politika bezpečnosti informací
- Dokument bezpečnostní politiky informací
- Přezkoumání bezpečnostní politiky informací

Politika bezpečnosti informací

- Určit směr a vyjádřit podporu bezpečnosti informací ze strany vedení v souladu s požadavky organizace, příslušnými zákony a směrnicemi.

- Vedení organizace by mělo stanovit jasný směr postupu v oblasti bezpečnosti informací, ukázat její podporu vydáním a aktualizací bezpečnostní politiky informací platné v celé organizaci.

Dokument bezpečnostní politiky informací

- Dokument bezpečnostní politiky informací by měl být schválen vedením organizace, publikován a dán na vědomí všem zaměstnancům a relevantním externím stranám.

- Dokument bezpečnostní politiky informací by měl obsahovat vyjádření podpory vedení organizace a měl by stanovit zamýšlený přístup k budování bezpečnosti informací.

Dokument bezpečnostní politiky informací

Dokument by měl obsahovat následující body:

- definici bezpečnosti informací, její cíle, rozsah a její význam;
- prohlášení vedení organizace o záměru podporovat cíle a principy bezpečnosti informací;
- rámec pro stanovení cílů opatření a opatření včetně jednotného přístupu k hodnocení a řízení rizik;
- stručný výklad bezpečnostních zásad (politik), principů, standardů a norem a požadavků na soulad, kterým organizace přikládá zvláštní význam, například:
- stanovení obecných a konkrétních odpovědností pro oblast řízení bezpečnosti informací včetně hlášení bezpečnostních incidentů;
- odkazy na dokumentaci, která může bezpečnostní politiku podporovat.

Dokument bezpečnostní politiky informací

Dokument by měl obsahovat následující body:

- definici bezpečnosti informací, její cíle, rozsah a její význam;
- prohlášení vedení organizace o záměru podporovat cíle a principy bezpečnosti informací;
- rámec pro stanovení cílů opatření a opatření včetně jednotného přístupu k hodnocení a řízení rizik;
- stručný výklad bezpečnostních zásad (politik), principů, standardů a norem a požadavků na soulad, kterým organizace přikládá zvláštní význam, například:
- stanovení obecných a konkrétních odpovědností pro oblast řízení bezpečnosti informací včetně hlášení bezpečnostních incidentů;
- odkazy na dokumentaci, která může bezpečnostní politiku podporovat.

Dokument bezpečnostní politiky informací

S dokumentem by měli být seznámeni uživatelé v rámci organizace, a to formou, která je relevantní, přístupná a pochopitelná všem potenciálním příjemcům.

Bezpečnostní politika informací může být součástí (hierarchicky podřízena) dokumentu nejvyšší politiky organizace. V případech, kdy je bezpečnostní politika šířena mimo organizaci, by měla být zajištěna ochrana citlivých informací před vyzrazením.

Přezkoumání bezpečnostní politiky informací

- Měla by být přezkoumávána v plánovaných intervalech a vždy když nastane významná změna.
- Měla by mít vlastníka odpovědného za její vytvoření, přezkoumání a aktualizaci.
- Při přezkoumání by měly být zohledněny závěry z přezkoumání provedeného vedením organizace. Měl by být vytvořen postup a plán pravidelného přezkoumání vedení organizace.

Vstupy pro přezkoumání

1. zpětná vazba od zainteresovaných stran;
2. výsledky nezávislých přezkoumání;
3. stav preventivních a nápravných činností;
4. výsledky z předchozích přezkoumání vedením organizace;
5. výkonnost procesu a soulad s bezpečnostní politikou;
6. změny, které mohou mít vliv na přístup organizace k řízení bezpečnosti informací,;
7. trendy v oblasti hrozeb a zranitelností;
8. hlášení bezpečnostních incidentů;
9. doporučení orgánů veřejné správy.

Výstupy z přezkoumání

Výstupy by měly obsahovat:

- změny a zlepšení přístupu organizace k řízení bezpečnosti informací a procesům organizace;
- změny cílů opatření a jednotlivých opatření;
- změny v přidělení zdrojů a odpovědností.

O provedených přezkoumáních bezpečnostní politiky vedením organizace by měly být udržovány záznamy.

Od vedení organizace by mělo být získáno schválení aktualizované verze bezpečnostní politiky.

Organizace bezpečnosti informací

1 Interní organizace

- Řídit bezpečnost informací v organizaci.
- Měl by být vytvořen řídící rámec pro zahájení a řízení implementace bezpečnosti informací v organizaci.

2 Externí subjekty

- Zachovat bezpečnost informací organizace a prostředků pro zpracování informací, které jsou přístupné, zpracovávané, sdělované nebo spravované externími subjekty.
- Bezpečnost informací a prostředků pro zpracování informací by neměla být snížena při zavedení produktů a služeb třetích stran.

Organizace bezpečnosti informací
Interní organizace

Vedení organizace by mělo určit potřebnost konzultací od odborníka na bezpečnost informací a přezkoumat a koordinovat výsledky konzultací v rámci organizace.

Vedení organizace by mělo stanovit jasný směr a aktivně podporovat bezpečnost v rámci organizace.

Organizace bezpečnosti informací
Interní organizace

- Koordinace bezpečnosti informací
- Přidělení odpovědností v oblasti bezpečností informací
- Schvalovací proces prostředků pro zpracování informací
- Dohody o ochraně důvěrných informací
- Kontakt s orgány veřejné správy
- Kontakt se zájmovými skupinami
- Nezávislá přezkoumání bezpečností informací

Organizace bezpečnosti informací
Externí subjekty

Cílem je zachovat bezpečnost informací organizace a prostředků pro zpracování informací, které jsou přístupné, zpracovávané, sdělované nebo spravované externími subjekty.

Bezpečnost informací a prostředků pro zpracování informací by neměla být snížena při zavedení produktů a služeb třetích stran.

Přístup externích subjektů k prostředkům pro zpracování informací a k informacím by měl být kontrolován.

Organizace bezpečnosti informací
Externí subjekty

- Identifikace rizik vyplývajících z přístupu externích subjektů
- Bezpečnostní požadavky pro přístup klientů
- Bezpečnostní požadavky v dohodách se třetí stranou

ZÁVĚR

Bezpečnostní politika informací může být součástí (hierarchicky podřízena) dokumentu nejvyšší politiky organizace. V případech, kdy je bezpečnostní politika šířena mimo organizaci, by měla být zajištěna ochrana citlivých informací před vyzrazením.

Dotazy?

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