MANAGEMENT KYBERNETICKÉ BEZPEČNOSTI

TÉMA Č. 9
METRIKY A MĚŘENÍ PRO HODNOCENÍ ÚČINNOSTI ZAVEDENÉHO ISMS

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.
- ✓Cíle měření bezpečnosti informací.
- ✓Program měření bezpečnosti informací.
- ✓Faktory přispívající k úspěchu.
- ✓Model měření bezpečnosti informací.
- ✓Základní metrika a metoda měření.
- ✓Odvozená metrika a funkce měření.
- ✓Vývoj metrik a měření.
- ✓Provádění měření.
- ✓Analýza dat a hlášení výsledků měření.
- ✓Vyhodnocení a zlepšování PMBI.
- ✓Závěr.

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

PMBI = program měření bezpečnosti informací

Literatura

ČSN ISO/IEC 27004 Datum vydání : 1.1.2011

Informační technologie - Bezpečnostní techniky - Řízení bezpečnosti informací – Měření

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

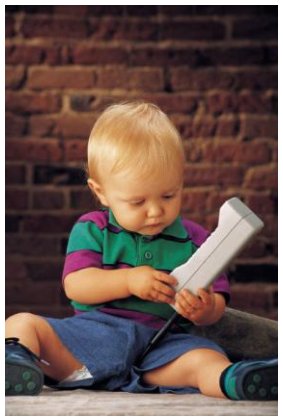
Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky.

ČSN ISO/IEC 27002 / 17799 Datum vydání : 1.8.2006

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

ZÁKLADNÍ POJMY

- analytický model
- atribut
- základní metrika
- data
- rozhodovací kritéria
- odvozená metrika
- indikátor
- informační potřeba
- metrika
- měření
- měření
- funkce měření
- metoda měření
- výsledky měření
- objekt
- měřítko
- jednotka měření
- validace
- ověřování



ZÁKLADNÍ POJMY

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.

ZÁKLADNÍ POJMY

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.

ZÁKLADNÍ POJMY

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.

ZÁKLADNÍ POJMY

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.

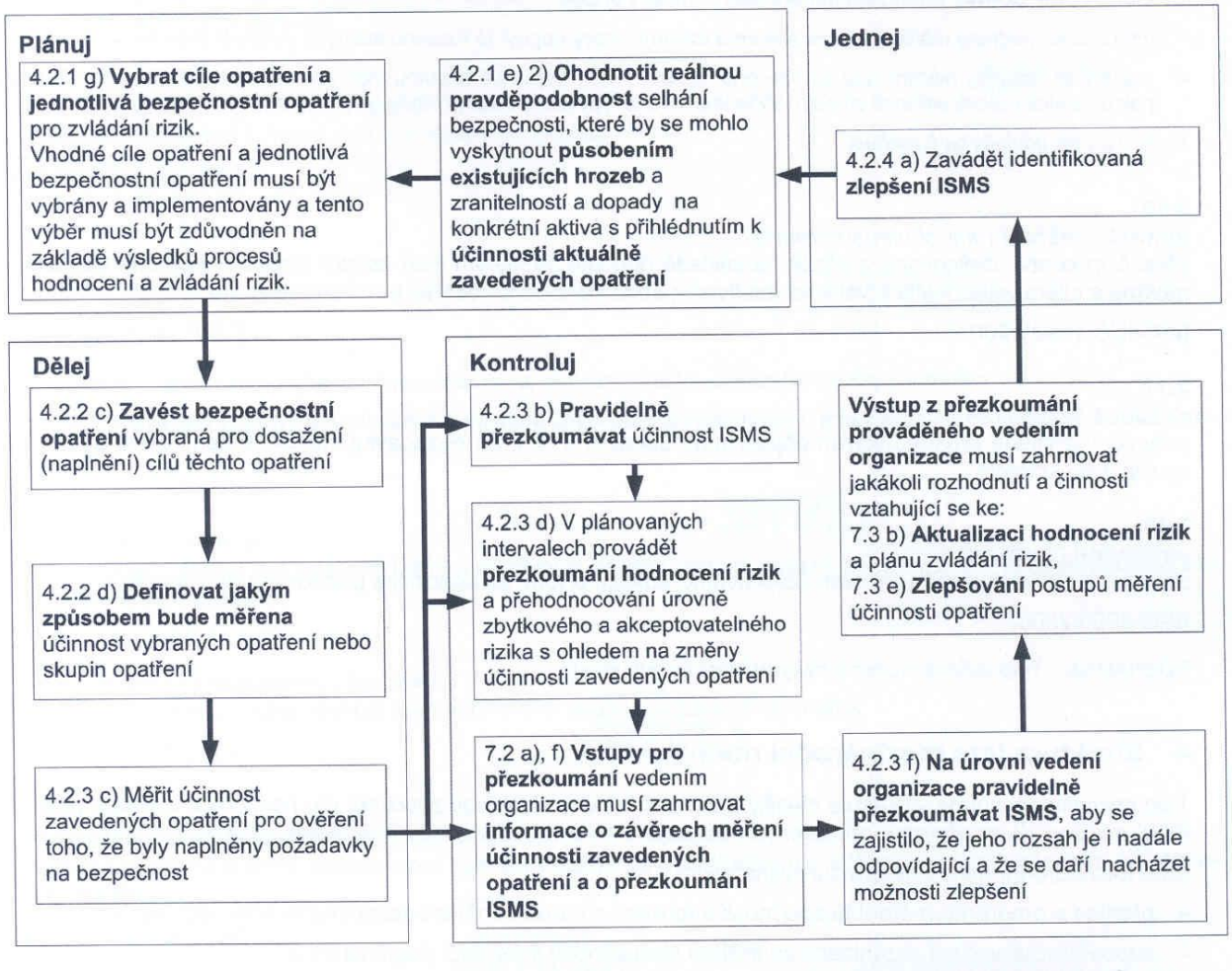
Zranitelnost (Vulnerability) je slabé místo aktiva nebo skupiny aktiv, které může být využito jednou nebo více hrozbami.

Cíle měření bezpečnosti informací

a) vyhodnocení účinnosti zavedených opatření nebo skupin opatření;
b) vyhodnocení účinnosti zavedeného ISMS;
c) ověření míry, do které byly identifikované požadavky na bezpečnost splněny;
d) podpora zlepšování výkonu bezpečnosti informací v rámci celkových rizik činností organizace;
e) poskytování vstupu pro přezkoumání vedením organizace za účelem podpory rozhodování a zdůvodnění zlepšování zavedeného ISMS.

Cíle měření bezpečnosti informací

Vstupy a výstupy měření v ISMS PDCA cyklu řízení bezpečnosti informací



Cíle měření bezpečnosti informací

Faktory ovlivňující cíle měření:

a) role bezpečnosti informací na podporu celkových obchodních činností organizace a rizik, kterým čelí;

b) příslušné právní, regulační a smluvní požadavky;

c) organizační strukturu;

d) náklady a výhody zavedení metrik bezpečnosti informací;

e) kritéria akceptace rizik pro organizaci;

f) potřebu porovnat několik ISMS v rámci samotné organizace.

Program měření bezpečnosti informací

Program měření bezpečnosti informací by měl zahrnovat následující procesy:

a) rozvoj metrik a měření;
b) provádění měření;
c) analýzu dat a hlášení výsledků měření;
d) vyhodnocení a zlepšování programu měření bezpečnosti informací.

Metriky vybrané a zavedené programem měření bezpečnosti informací by se měly přímo vztahovat na provozování ISMS.

Faktory přispívající k úspěchu

Faktory přispívající k úspěchu programu měření bezpečnosti informací:

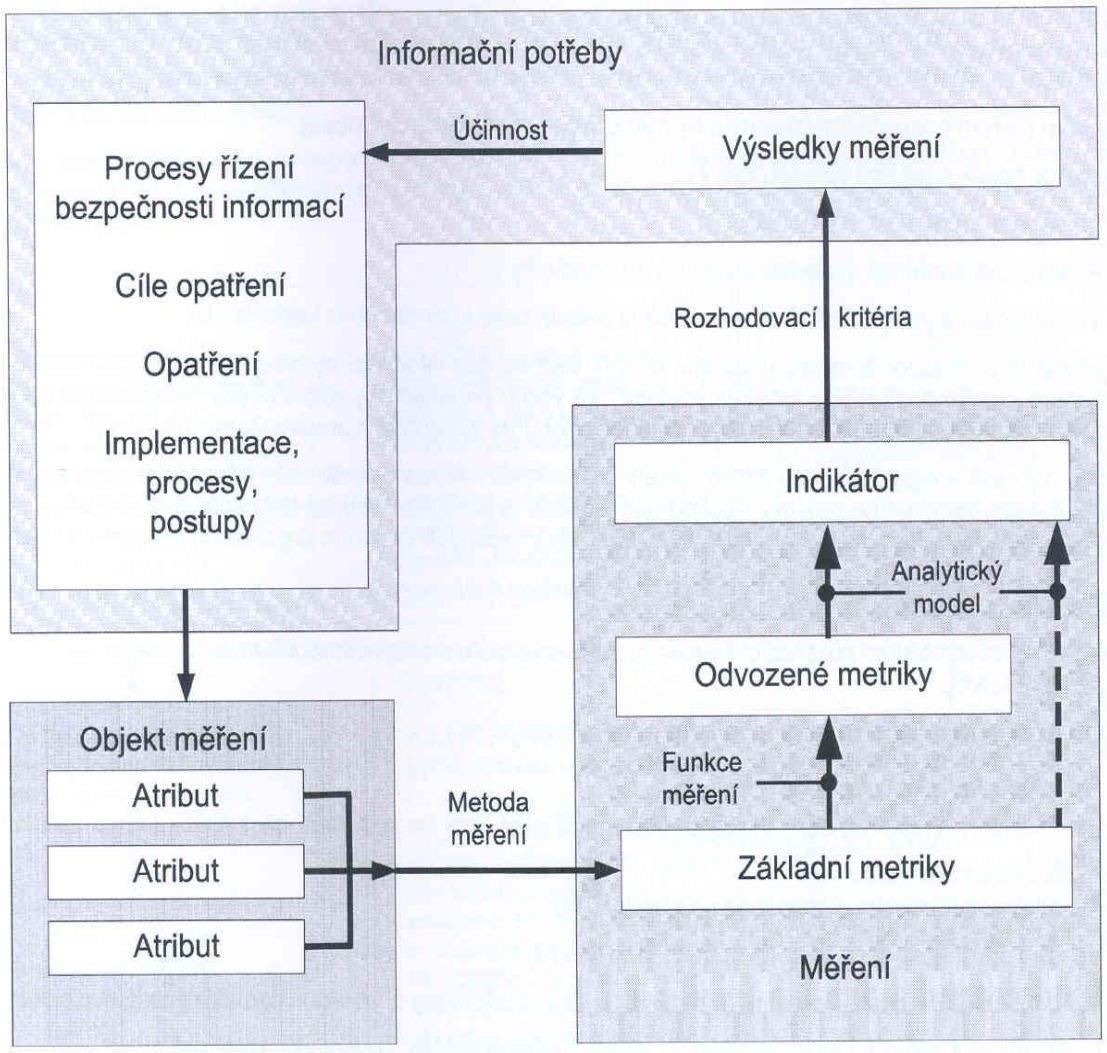
a) existence procesů a postupů ISMS;
b) opakovatelný proces schopný získat a hlásit smysluplná data;
c) kvantifikovatelné metriky založené na cílech ISMS;
d) snadno získatelná data, která lze použít pro měření;
e) vyhodnocení účinnosti programu měření;
f) konzistentní periodický sběr, analýza a hlášení o datech měření;
g) využití výsledků měření příslušnými zainteresovanými stranami;
h) akceptace zpětné vazby na výsledky měření;
i) vyhodnocení užitečnosti výsledků měření.

Model měření bezpečnosti informací

Model měření bezpečnosti informací je struktura spojující informační potřebu s příslušnými objekty měření a jejich atributy. Objekty měření mohou zahrnovat plánované nebo zavedené procesy, postupy, projekty a zdroje.

Model měření bezpečnosti informací popisuje, jak jsou příslušné atributy kvantitativně určeny a převedeny na indikátory, které poskytují základ pro rozhodování.

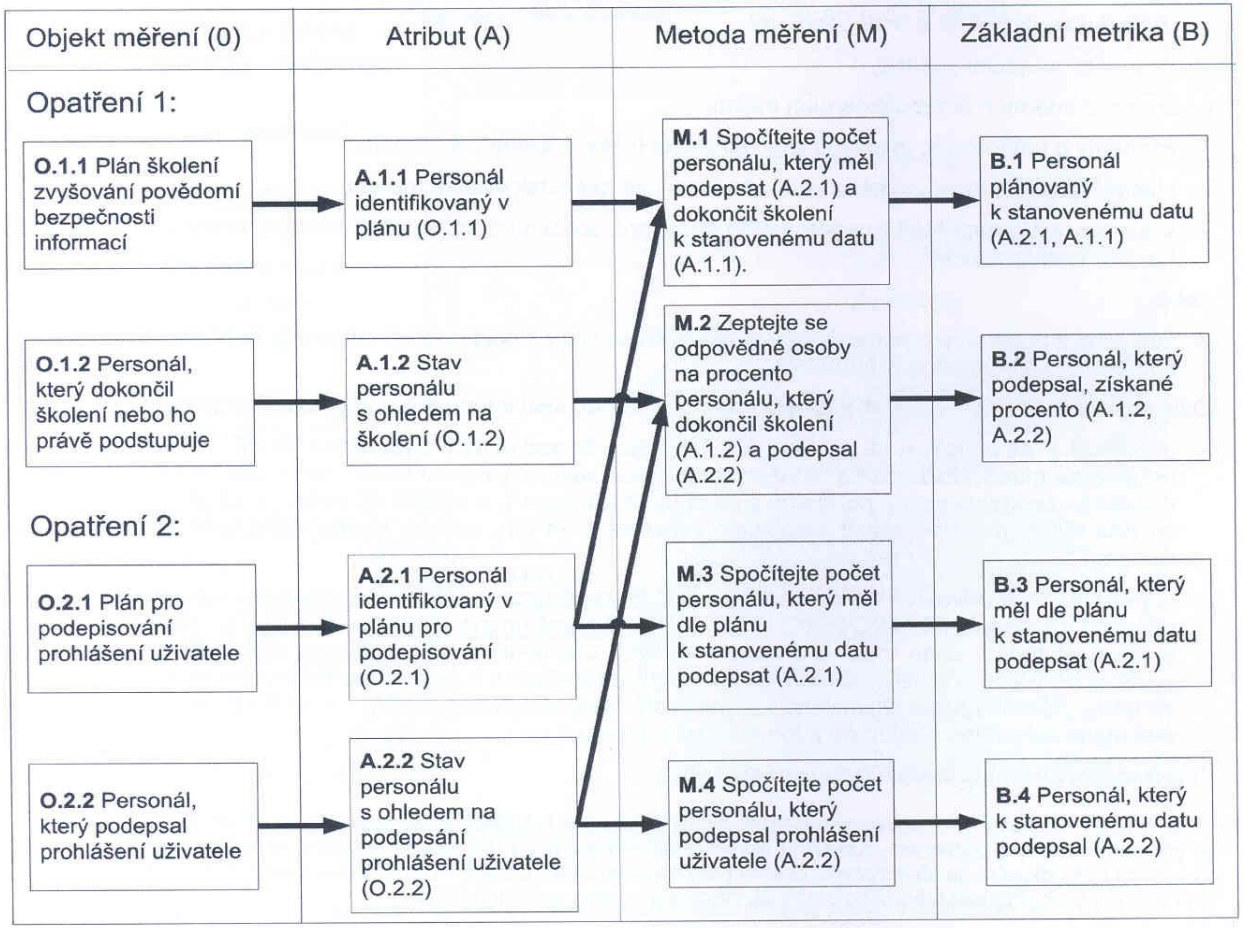
Model měření bezpečnosti informací



Základní metrika a metoda měření

- Základní metrika je **nejjednodušší metrika**, která může být získána.
- Základní metrika vyplývá z použití **metody měření** na atributy vybrané u objektu měření.
- Objekt měření může mít mnoho **atributů**.
- Daný **atribut** lze použít pro **několik** různých základních metrik.
- **Metoda měření** je logická posloupnost operací použitá při kvantitativním určení atributu s ohledem na stanovené měřítko.

Základní metrika a metoda měření

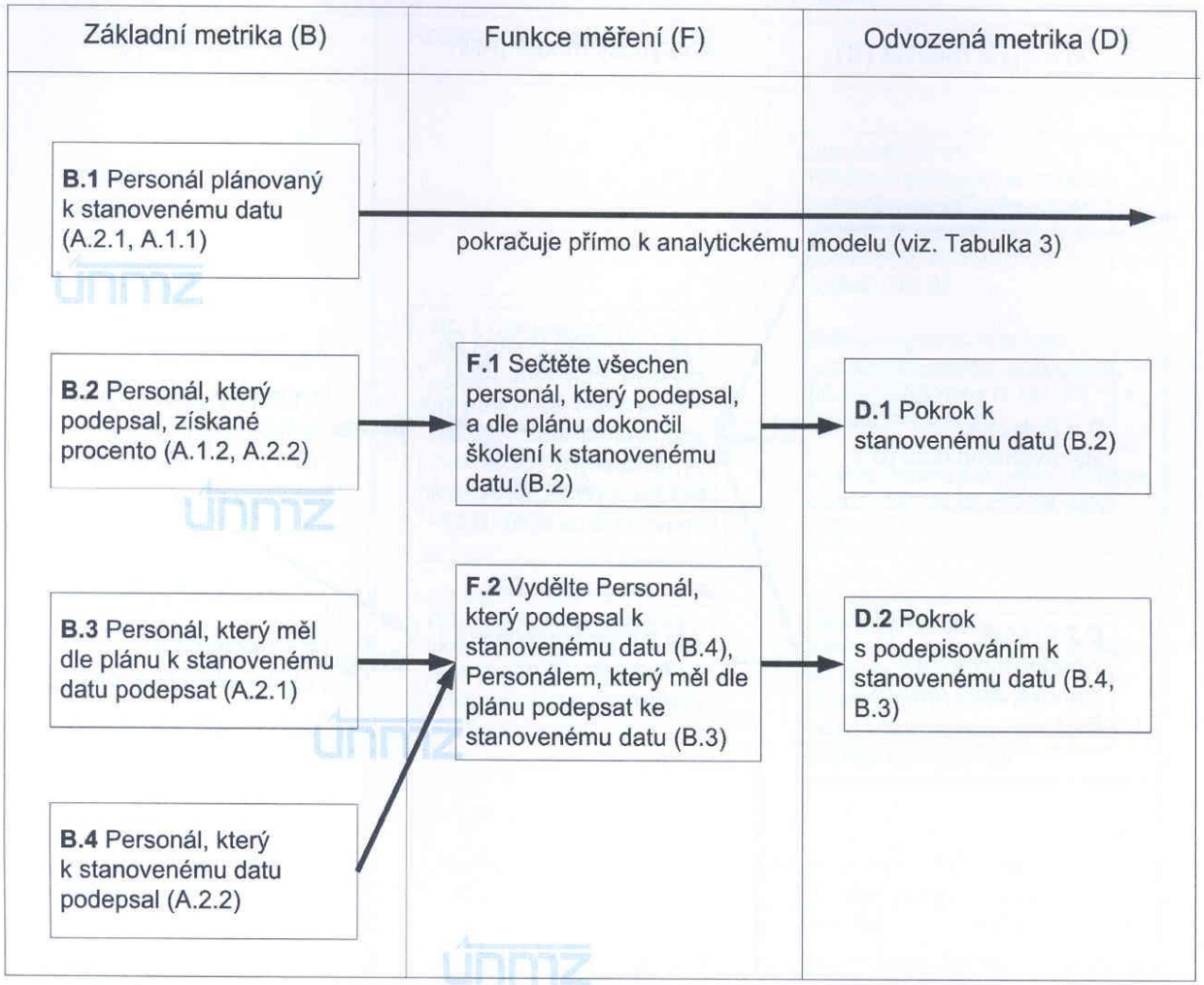


Příklad vztahu mezi objektem měření, atributem, metodou měření a základní metrikou pro měření objektů ustanovených pro zavedená opatření.

Odvozená metrika a funkce měření

- Odvozená metrika je souhrn dvou nebo více základních metrik. Daná základní metrika může sloužit jako vstup pro několik odvozených metrik.
- Funkce měření je výpočet používaný pro kombinování základních metrik dohromady za účelem vytvoření odvozené metriky.
- Měřítko a jednotka odvozené metriky závisí na měřítkách a jednotkách základních metrik, z nichž jsou složeny, i na tom, jak jsou kombinovány funkcí měření.
- Funkce měření může obsahovat celou škálu technik.
- Funkce měření může kombinovat základní metriky za použití různých měřítek.

Odvozená metrika a funkce měření



Odpovědnosti vedení organizace

Vedení organizace je odpovědné za ustanovení programu měření bezpečnosti informací.

Vedení organizace by mělo:

- stanovit cíle pro PMBI;
- ustanovit politiku pro PMBI;
- stanovit role a odpovědnosti pro PMBI;
- zajistit dostatečné zdroje pro provádění měření, včetně personálu, financování, nástrojů a infrastruktury;
- zajistit dosažení cílů PMBI;
- zajistit, aby nástroje a zařízení používané ke sběru dat byly řádně udržovány;
- stanovit účel měření pro každý koncept měření;
- zajistit, aby měření poskytovalo dostatek informací pro příslušné zainteresované strany.

PMBI = program měření bezpečnosti informací

Vývoj metrik a měření

Měly by být ustanoveny a dokumentovány činnosti potřebné k vývoji metrik a měření, včetně:

- definování rozsahu měření;
- identifikování informační potřeby;
- výběru objektu měření a jeho atributů;
- vývoj konceptů měření;
- používání konceptů měření;
- ustanovení sběru dat a analytických procesů a nástrojů,
- stanovení přístupu k implementaci měření a k dokumentaci.

Provádění měření

Měly by být ustanoveny a dokumentovány činnosti potřebné k vývoji metrik a měření, včetně:

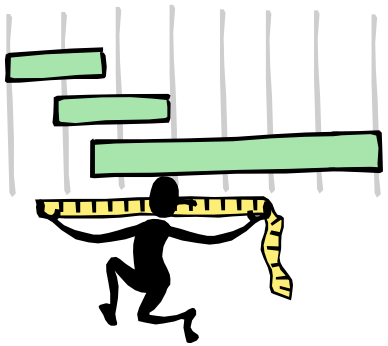
- definování rozsahu měření;
- identifikování informační potřeby;
- výběru objektu měření a jeho atributů;
- vývoj konceptů měření;
- používání konceptů měření;
- ustanovení sběru dat a analytických procesů a nástrojů,
- stanovení přístupu k implementaci měření a k dokumentaci.

Analýza dat a hlášení výsledků měření

Sebraná data by měla být analyzována za účelem získání výsledků měření a získané výsledky měření by měly být sděleny.

Tato činnost zahrnuje:

a. analýzu dat a získání výsledků měření;
b. sdělení výsledků měření příslušným zainteresovaným stranám.



PMBI = program měření bezpečnosti informací

Vyhodnocení a zlepšování PMBI

Nejpravděpodobnějšími kritérii, kdy by organizace měly vyhodnotit a zlepšit zavedený PMBI, jsou:

- změny obchodních cílů organizace;
- změny právních nebo regulačních požadavků a smluvních závazků s dopadem na bezpečnost informací;
- změny požadavků organizace na bezpečnost informací;
- změny rizik bezpečnosti informací pro organizaci;
- zvýšená dostupnost vytříbenějších nebo vhodnějších dat a/nebo metod sběru dat pro účely měření;
- změny objektu měření a/nebo jeho atributů.

PMBI = program měření bezpečnosti informací

ZÁVĚR

Organizace by měla ustavit a řídit program měření bezpečnosti informací.

Model měření bezpečnosti informací popisuje, jak jsou příslušné atributy kvantitativně určeny a převedeny na indikátory, které poskytují základ pro rozhodování.

Vedení organizace je odpovědné za ustanovení programu měření bezpečnosti informací.

Organizace by měla definovat kritéria pro hodnocení účinnosti programu měření bezpečnosti informací.

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

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