MANAGEMENT KYBERNETICKÉ BEZPEČNOSTI

TÉMA Č. 2 - SOUBOR POSTUPŮ PRO MANAGEMENT BEZPEČNOSTI INFORMACÍ – ZVLÁDÁNÍ BEZPEČNOSTNÍCH INCIDENTŮ

pplk. Ing. Richard SLOŽIL
CIRC - MO
Email: Richard.Slozil@army.cz

Operační program Vzdělávání pro konkurenceschopnost

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

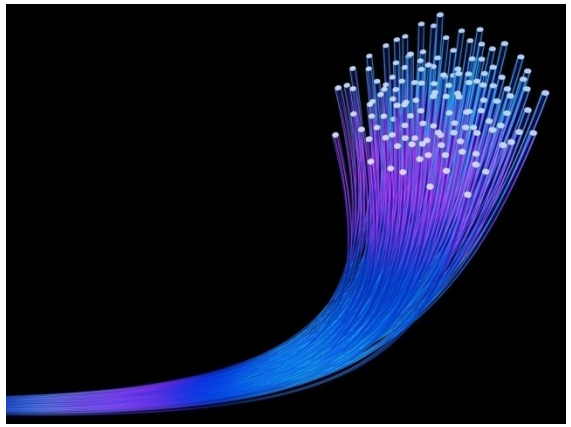
(reg. č.: CZ.1.01/2.2.00/15.0070)

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.
- ✓Hlášení bezpečnostních událostí a slabin.
- ✓Zvládání bezpečnostních incidentů a kroky k nápravě.
- ✓Odpovědnosti a postupy.
- ✓Ponaučení z bezpečnostních incidentů.
- ✓Shromažďování důkazů.
- ✓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.

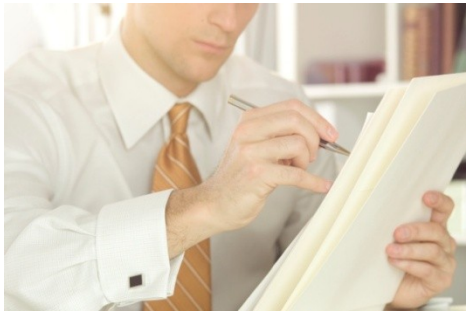
Základní pojmy

- incident
- bezpečnost informací
- bezpečnostní událost
- bezpečnostní incident
- riziko
- třetí strana
- zranitelnost

Hlášení bezpečnostních událostí a slabin

Cílem je zajistit nahlášení bezpečnostních událostí a slabin informačního systému způsobem, který umožní včasné zahájení kroků vedoucích k nápravě.

Měly by být ustaveny formální postupy pro hlášení bezpečnostních událostí a pro zvyšování stupně jejich důležitosti. Všichni zaměstnanci, smluvní strany a uživatelé třetích stran by měli znát postupy hlášení různých typů událostí a slabin, které mohou mít dopad na bezpečnost aktiv organizace. Zjištěné bezpečnostní události a slabiny by měli zaměstnanci ihned hlásit na určené místo.



Hlášení bezpečnostních událostí

Bezpečnostní události by měly být co nejrychleji hlášeny příslušnými řídícími kanály.

Postupy hlášení by měly zahrnovat:

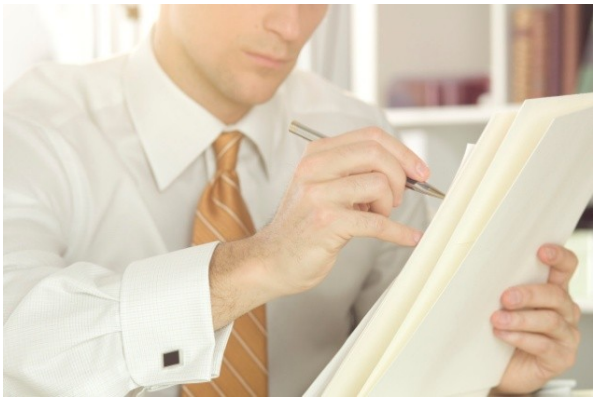
- vytvoření procesu zajišťujícího přiměřenou zpětnou vazbu;
- formuláře podporující proces hlášení bezpečnostních událostí a zároveň zajišťující, že hlášení bude splňovat všechny nezbytné kroky;
- nastavení správného chování v případě bezpečnostní události;
- odkaz na zavedená formalizovaná pravidla pro disciplinární proces se zaměstnanci, smluvními stranami nebo uživateli třetích stran, kteří způsobili narušení bezpečnosti.

Hlášení bezpečnostních událostí

Jakékoliv chybné anebo jiné neobvyklé chování systému může být příznakem pokusu o narušení nebo útoku na bezpečnost a mělo by tedy vždy být hlášeno jako bezpečnostní událost.

Příklady bezpečnostních událostí a incidentů:

- ztráta služby, zařízení nebo vybavení;
- chybné fungování nebo přetížení systému;
- lidské chyby;
- nesoulad s politikami nebo směrnicemi;
- porušení opatření fyzické bezpečnosti;
- nekontrolované změny systému;
- chybné fungování technického a programového vybavení;
- porušení přístupu.



Hlášení bezpečnostních slabin

Všichni zaměstnanci, smluvní strany a ostatní uživatelé informačního systému a služeb by měli být povinni zaznamenat a hlásit jakékoliv bezpečnostní slabiny nebo podezření na bezpečnostní slabiny v systémech nebo službách.

Postup hlášení by měl být jednoduchý, přístupný a kdykoliv dostupný.

Uživatelé by měli být informováni o tom, že nesmí za žádných okolností podezřelé slabiny prověřovat.

Testování bezpečnostních slabin může být interpretováno jako potenciální zneužití systému.

Zvládání bezpečnostních incidentů a kroky k nápravě

Cílem je zajistit odpovídající a účinný přístup ke zvládání bezpečnostních incidentů.

Pro účinné zvládání bezpečnostních útoků a slabin by měly být stanoveny odpovědnosti a zavedeny formalizované postupy umožňující okamžitou reakci.

Měl by být nastaven proces neustálého zlepšování reakce, monitorování, vyhodnocování a celkového zvládání bezpečnostních incidentů.

Pro zajištění souladu s právními požadavky by v případech, kdy je to vyžadováno, měly být shromážděny důkazy.

Odpovědnosti a postupy

Pro zajištění rychlé, účinné a systematické reakce na bezpečnostní incidenty by měly být zavedeny **odpovědnosti a postupy** pro zvládání bezpečnostních incidentů.

Kromě hlášení bezpečnostních událostí a slabin by pro detekci bezpečnostních incidentů mělo být praktikováno **monitorování systému, sledování varovných signálů a zranitelností**.

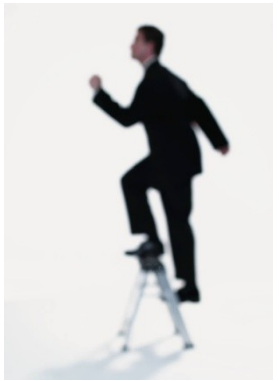
Pro správnou reakci na incidenty je třeba sladit odezvu a umožnit výměnu informací o těchto incidentech s externě spolupracujícími organizacemi podle aktuální potřeby.

Odpovědnosti a postupy

Následující doporučení:

a) postupy by měly pokrývat všechny možné typy bezpečnostních incidentů,

b) postupy by měly také zahrnovat:
   1. analýzu a identifikaci příčiny incidentu;
   2. kontrolu incidentu;
   3. plánování a implementaci opravných prostředků;
   4. komunikaci se všemi zúčastněnými;
   5. hlášení určenému subjektu.



c) soubor auditních záznamů a podobné důkazy, aby bylo možno:
   1. analyzovat vnitřní problémy;
   2. použít je jako forenzních důkazů;
   3. použít je při jednání o náhradě škody.

d) činnosti při opravách selhání systému a zotavení se z narušení bezpečnosti by měly být pečlivě a formálně kontrolovány.

Odpovědnosti a postupy

Postupy by měly zajišťovat, aby:

1) přístup do systému a k datům byl umožněn pouze na základě jednoznačné identifikace a autorizace pracovníků;
2) všechny činnosti při mimořádné události byly detailně dokumentovány;
3) činnosti při mimořádné události byly hlášeny vedení organizace a systematicky kontrolovány;
4) integrita systémů organizace a opatření byla potvrzena s minimálním prodlením.

Ponaučení z bezpečnostních incidentů

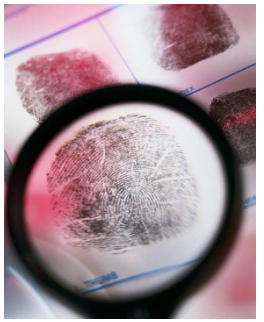
Informace získané při vyhodnocení bezpečnostních incidentů by měly být využity pro identifikaci opakujících se incidentů nebo incidentů s velkými následky.

Závěry z vyhodnocení bezpečnostních incidentů mohou také signalizovat potřebu využití dodatečných nebo důkladnějších opatření, která by omezila frekvenci, škody a náklady jejich budoucích výskytů.

Kromě toho by měly být vzaty v úvahu při revizi bezpečnostní politiky.

Shromažďování důkazů

Měly by být vytvořeny a do praxe zavedeny interní směrnice pro sběr a předkládání důkazů.



Kvalita a kompletnost postupů:

- papírové dokumenty,
- informace na počítačových médiích.

Jakákoliv forenzní zkoumání by měla být prováděna zásadně na kopiích důkazního materiálu. Vždy by měla být zajištěna integrita důkazního materiálu.

ZÁVĚR

Bezpečnostní události by měly být co nejrychleji hlášeny příslušnými řídícími kanály.

Jakékoliv chybné anebo jiné neobvyklé chování systému může být příznakem pokusu o narušení nebo útoku na bezpečnost a mělo by tedy vždy být hlášeno jako bezpečnostní událost.

Pro zajištění rychlé, účinné a systematické reakce na bezpečnostní incidenty by měly být zavedeny odpovědnosti a postupy pro zvládání bezpečnostních incidentů.

Dotazy?

pplk. Ing. Richard SLOŽIL
CIRC - MO
Email: Richard.Slozil@army.cz

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