MANAGEMENT KYBERNETICKÉ BEZPEČNOSTI

TÉMA Č. 2
KONCEPCE KYBERNETICKÉ OBRANY V ČR (V REZORTU MO)

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.
- ✓Definice - Kybernetická bezpečnost.
- ✓Kybernetická bezpečnost v ČR.
- ✓Strategie pro oblast KB ČR na období 2011 – 2015.
- ✓Akční plán opatření ke Strategii pro oblast KB ČR na období 2011 – 2015.
- ✓Co je CERT?
- ✓Co je CSIRT?
- ✓Koncepce kybernetické obrany rezortu MO.
- ✓Závěr.

Literatura

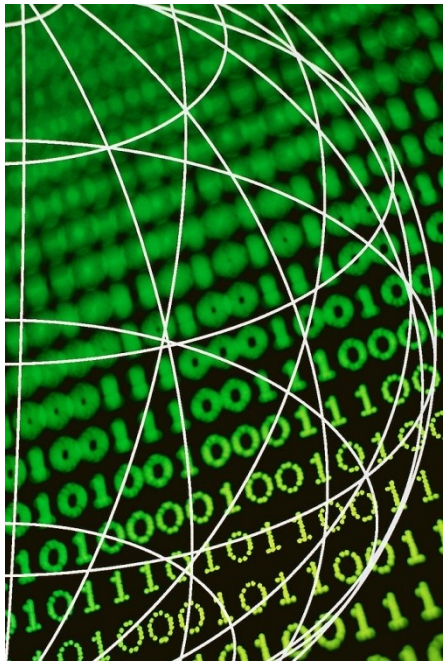
Zákony:
412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

Usnesení vlády:
677/2007, Akční plán plnění opatření Národní strategie bezpečnosti České republiky
564/2011, o Strategii pro oblast kybernetické bezpečnosti České republiky na období 2011 – 2015
781/2011, o ustavení Národního bezpečnostního úřadu gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast

ČSN ISO/IEC 27000 Datum vydání : 1.5.2010
Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník.

Základní pojmy

- aktivum
- útok
- bezpečnost informací
- bezpečnostní událost
- bezpečnostní incident
- riziko
- systém řízení bezpečnosti informací
- zranitelnost



Definice - Kybernetická bezpečnost

Cyber Security (Kybernetická bezpečnost)

Kybernetická bezpečnost (Cyber Security) je odvětví výpočetní techniky známé jako informační bezpečnost, uplatňované jak u počítačů tak i sítí. Cílem informační bezpečnosti je ochrana Informací a majetku před krádeží, korupcí, nebo přírodní katastrofou, přičemž informace a majetek musí zůstat přístupné a produktivní jeho předpokládaným uživatelům.

Definice - Kybernetická bezpečnost

Termínem Bezpečnost informačních systémů se rozumí kolektivní postupy a mechanismy, jejichž citlivé a cenné informace a služby jsou chráněny před zveřejněním, poškozením nebo kolapsem neoprávněnou činností nebo činností nedůvěryhodné osoby a neplánované události. Strategie a metody informační bezpečnosti se často liší od většiny jiných výpočetních technologií, protože jejich výhradním cílem je zabránit nežádoucímu chování počítačů.

Kybernetická bezpečnost v ČR

Právo vnímá kybernetickou bezpečnost jako **ochranu národního kyberprostoru před bezpečnostními hrozbami**. Jednotlivé bezpečnostní incidenty samozřejmě mohou dosáhnout takové intenzity, že se negativně projeví v národním měřítku, tj. dojde například k výpadku páteřní sítě. Většina běžně se vyskytujících incidentů však nedosahuje takové závažnosti, aby bylo nutno se jimi na úrovni národní kybernetické bezpečnosti zabývat – s takovými jevy se pak právo vypořádává za užití standardních ochranných institutů trestního, správního a civilního práva. Typickým příkladem může být únik osobních údajů nebo průnik do firemního informačního systému.

Kybernetická bezpečnost v ČR

Vláda České republiky dne **15. března 2010** schválila usnesení **č. 205** o řešení problematiky kybernetické bezpečnosti .

Dne **20. července 2011** Vláda České republika přijala usnesení **č. 564** jímž mimo jiné schválila Strategii pro oblast kybernetické bezpečnosti České republiky na období 2011 - 2015.

Dne **19. října 2011** Vláda České republiky přijala usnesení **č. 781** jímž ustavila Národní bezpečnostní úřad gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast.

Strategie pro oblast kybernetické bezpečnosti České republiky na období 2011 - 2015

- navazuje na Bezpečnostní strategii České republiky.
- je základním dokumentem při tvorbě politik, právních norem, směrnic, metodických pokynů, pravidel, zásad, příruček, provozních režimů, plánů, doporučení, apod.
- definuje zájmy a záměry ČR v oblasti kybernetické bezpečnosti pro budování důvěryhodné informační společnosti na právních základech, která dbá na zabezpečení kybernetického přenosu a zpracování informací ve všech oblastech lidské činnosti a umožňuje informace svobodně a bezpečně sdílet a využívat.

Akční plán opatření ke Strategii pro oblast kybernetické bezpečnosti ČR na období 2011 – 2015

Akční plán je rozčleněn do sedmi oblastí. V každé jsou rozpracovány úkoly k naplňování jednotlivých strategických cílů Strategie do projektů a úkolů orgánů veřejné správy, které jsou věcně v jejich gesci.

Tento akční plán bude aktualizován vždy v závěru roku na základě výsledků závěrečné zprávy pro oblast kybernetické bezpečnosti České republiky.

Akční plán opatření ke Strategii pro oblast kybernetické bezpečnosti ČR na období 2011 – 2015

Strategie stanovuje tyto hlavní prioritní oblasti :

I. Koordinace a řízení rizik kybernetické bezpečnosti ČR.

II. Podpora mezinárodní spolupráce v oblasti kybernetické bezpečnosti ČR.

III. Národní spolupráce v oblasti kybernetické bezpečnosti (veřejné, soukromé a akademické).

IV. Vytvoření legislativního rámce k posílení kybernetické bezpečnosti ČR, podpora a ochrana lidských práv a svobod.

V. Zvyšování povědomí a znalostí o kybernetické bezpečnosti ČR.

VI. Posilování kybernetické bezpečnosti v ICT veřejné správy a komunikační infrastruktury ČR.

VII. Posilování odolnosti proti narušení ICT systémů a proti kybernetickým útokům.

CO JE CERT?

CERT (Computer Emergency Response Team)

je pracoviště vybavené odpovídajícími technologickými, analytickými a personálními prostředky.

CERT poskytuje z pohledu kybernetické bezpečnosti následující služby:

Reaktivní služby:

- výstrahy a varování před kybernetickými hrozbami prostřednictvím systému včasného varování,
- řešení bezpečnostních incidentů,
- podpora reakcí na bezpečnostní incidenty,
- koordinace reakcí na bezpečnostní incidenty.

CO JE CERT?

Aktivní služby:

- shromažďování a šíření informací týkajících se kybernetické bezpečnosti,
- monitorování výskytu bezpečnostních hrozeb,
- sledování vývoje bezpečnostní situace,
- metodická pomoc při zajišťování kybernetické bezpečnosti.

Vládní CERT České republiky kromě výše uvedených služeb plní funkci posledního záchytného bodu (tzv. last resort) pro řešení konkrétních bezpečnostních problémů, souvisejících s napadením počítačových sítí institucí veřejné správy a subjektů provozujících prvky kritické infrastruktury.

CO JE CSIRT?

CSIRT.CZ (CSIRT = Computer Security Incident Response Team) je bezpečnostní tým pro koordinaci řešení bezpečnostních incidentů v počítačových sítích provozovaných v České republice.

Cílem CSIRT.CZ je pomáhat provozovatelům internetových sítí v České republice zřizovat jejich vlastní bezpečnostní týmy a bezpečnostní infrastrukturu, řešit bezpečnostní incidenty a tím zlepšovat bezpečnost jejich sítí i globálního Internetu.

CSIRT.CZ také pomáhá předávat hlášení o bezpečnostních incidentech správcům těch sítí nebo domén, z nichž incidenty pocházejí, ale které na stížnosti nereagují.

Koncepce kybernetické obrany rezortu MO

Kybernetická obrana není řešením technických provozních problémů komunikační a informační infrastruktury rezortu Ministerstva obrany (MO), ale souhrn bezpečnostních opatření, která brání inteligentním protivníkům dosahovat pomocí kybernetických útoků cílů, jež nejsou v souladu se zájmy ČR.

Cílem koncepce je navrhnout opatření, která povedou ke zvýšení (posílení) schopnosti rezortu MO chránit vlastní systémy, které jsou součástí kritické infrastruktury rezortu MO, před kybernetickými útoky. Koncepce stanoví v souladu s požadavky NATO základní principy, postupy a doporučení k institucionalizaci kybernetické obrany v rezortu MO, jejímu provádění a vyhodnocování a zásady spolupráce s orgány kybernetické obrany v ČR, členských státech NATO a EU.

Koncepce bude podle potřeby aktualizována v dvouletých cyklech.

ZÁVĚR

- Kybernetická bezpečnost .
- Kybernetická bezpečnost v ČR.
- Strategie pro oblast KB ČR na období 2011 – 2015.
- Akční plán opatření ke Strategii pro oblast KB ČR na období 2011 – 2015.
- CERT.
- CSIRT.
- NBÚ.
- Koncepce kybernetické obrany v rezortu MO.
- Právní úprava národní kybernetické 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

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