Kybernetická bezpečnost

Václav Stupka

Význam ICT

- Rostoucí podíl činností závislých na fungování ICT
- Nezbytnost bezpečného a spolehlivého fungování ICT pro fungování veřejné i soukromé sféry
- Práce s informacemi prostřednictvím ICT je základem takzvané informační společnosti

Závislost na ICT

- Bezpečné a spolehlivé fungování ICT je jedním ze základních předpokladů prosperity a trvalého ekonomického růstu
- Rozvoj ICT představuje bezpečnostní výzvu pro celou informační společnost
- Rostoucí závislost společnosti na ICT zvyšuje zranitelnost státu a jeho občanů vůči kybernetickým útokům

Náchylnost ICT

- Globální dostupnost
- Rychlost
- Anonymita
- Dostupnost
- Asymetrie mezi „útočníky“ a „obránci“

Kybernetická bezpečnost

- Cíl každého vyspělého státu je zajistit kybernetickou bezpečnost – tedy pracovat na ofenzivní i defenzivní kybernetické politice.
- Je tedy třeba analyzovat hrozby, zkoumat nové technologie a všemi prostředky aktivně snižovat rizika.
- Nejedná se však o izolovaný problém jednoho státu, je to problém meziresortní i mezinárodní, problém veřejné i privátní sféry.

Kybernetická bezpečnost ve světě

- Nedostatečná pozornost, organizovanost
- V poslední době patrná globální snaha o zjištění kybernetické bezpečnosti jednotlivých států
- Nutnost vnitrostátní i mezinárodní kooperace
- Sdílení best practises a informací o hrozbách
- Důležitá informovanost uživatelů
- Vznik mezinárodních organizací sdružujících CERT/CSIRT týmy

Kybernetická bezpečnost v ČR

- Národní strategie informační bezpečnosti ČR (2007)
- Koncepce přenosu klasifikovaných informací komunikační infrastrukturou veřejné správy ČR
- Bezpečnostní politika přenosu klasifikovaných informací komunikační infrastrukturou veřejné správy ČR
- Novela zákona č. 101/2000 Sb., o ochraně osobních údajů
- Návrh úrovní zabezpečení informačních systémů nezbytných pro chod kritické infrastruktury ČR
- Zákon č. 412/2005 Sb. O ochraně utajovaných informací a bezpečnostní způsobilosti
- Bezpečnostní strategie ČR
- Koncepce boje proti trestné činnosti v oblasti ICT

Základní cíle

- Ochrana před hrozbami, kterými jsou informační a komunikační systémy vystaveny (prevence)
- Snížení potenciálních škod v případě útoků na tyto informační a komunikační systémy
- Nastavení mechanismů reakcí na kybernetické incidenty (represe)
- Přiměřenost přijímaných opatření (soukromí, základní práva, svobodný přístup k informacím, demokratické standardy)

Strategie pro oblast kybernetické bezpečnosti ČR 2011-2015

- Spolupráce všech složek společnosti (předpokladem efektivity, nutná důvěra a sdílení informací)
- Individuálni zodpovědnost (odpovědnost za vlasntní ICT prostředky, osvěta)
- Odpovědnost podnikatelského sektoru (minimální standardy)
- Resortní spolupráce (Usnesení vlády č. 205 - MVČR, Usnesení vlády č. 380 – MKRKPB, Memorandum – CSIRT, CERT)
- Mezinárodní spolupráce (mezinárodní politiky EU a NATO)

Legislativní rámec

- Koordinace postupu v oblasti kybernetické bezpečnosti
- Cílem je vytvořit legislativní rámec respektující Ústavu a mezinárodní závazky
- Účelem rámce je dosažení stavu, kdy budou existovat legislativní a procedurální nástroje pro prevenci, detekci, reakci a opatření, vedoucí k předcházení, odhalování a potírání kybernetické kriminality

Zákon o kybernetické bezpečnosti

- Po přechodu gesce pod NBÚ
- Cíl – vytvořit vládní CERT, dohled nad kritickou infrastrukturou
- Definování standardů, osvěta, dohled, reakce, prevence
- Kooperace s ostatními CERTY (i mezinárodní)

Věcná působnost zákona o KB

- Kritická a ostatní část kyberprostoru
- Kritická: Kritická informační infrastruktura vs. Kritická komunikační infrastruktura
- Ostatní: komunikační infrastruktura, ISVS

- Kybernetická bezpečnostní událost

Osobní působnost zákona o KB

- ISP
- Správci kritické komunikační infrastruktury
- Správci IS kritické informační infrastruktury
- Správci ISVS

Národní centrum kybernetické bezpečnosti

- Součást organizační struktury NBÚ
- Národní dohledové pracoviště a organizační útvary
- Zvlášť: ústřední dohledové pracoviště

Stav kybernetického nebezpečí

- Pro případ rozsáhlé bezpečnostní události, která by mohla ohrozit fungování služeb informační společnosti v ČR, nebo v mezinárodním měřítku.
- Vyhlašuje ředitel NBÚ
- Nejvýše 7 dnů
- Krizový štáb
- Nouzový stav
- Povinnost ISP k protiopatření

Shrnutí

- Nebezpečí kybernetických útoků
- Důležitost obrany
- Specifika kybernetické bezpečnosti
- Mezinárodní situace
- Situace v ČR

Děkuji za pozornost.