
NBU

národní centrum kybernetické bezpečnosti

Role NBÚ v oblasti kybernetické bezpečnosti

Jaroslav Šmíd

náměstek ředitele NBÚ

j.smid@nbu.cz

Obsah

- Něco z historie
- Vliv Internetu na národní hospodářství
- Legislativní rámec
- Hlavní činnosti NCKB
  - NCKB současnost
  - NCKB budoucnost
- Co je Vládní CERT
  - Kompetence Vládního CERTu
- Dotazy

Něco z historie

- 13.2.1992 první počítač v ČR připojen k Internetu
- Počet uživatelů Internetu
- Rychlost připojení
- Služby Internetu
- Využití Internetu
- Státní správa na Internetu

Vliv Internetu na národní hospodářství 1

- jádro internetové ekonomiky tvoří 2,7 až 3,2 % HDP
- na dalších odvětvích se podílí 8,2 až 9,5 % přidané hodnoty
- IT odborníci představují 2,5 % všech pracovníků
- internet představuje 6,3% podíl na celkové zaměstnanosti
- 34,9 % zaměstnanců používá v práci aktivně internet (alespoň jednou týdně)

Vliv Internetu na národní hospodářství 2

- 97 % firem má přístup k internetu
- 92 % využívá internet k jednání s orgány veřejné správy
- 40 % firem nakupuje na internetu
- 25 % firem přes internet prodává
- internet přináší do ekonomiky 350 miliard korun ročně

Svobodný a otevřený Internet

- Svobodný a otevřený svět dnes závisí na svobodném a otevřeném Internetu
  - Zásady Internetu by tomu měly odpovídat
  - Svoboda projevu
  - Ochrana soukromí
  - Svobodný přístup
- za takový Internet je však třeba stále bojovat

Pravidla chování na Internetu

- Kybernetický svět potřebuje závazná pravidla a standardy jako ostatní oblasti lidské činnosti
- Tříletá snaha iniciovaná Velkou Británií - Cyber space conference 2011
- Snahy Ruska a Číny v OSN a ITU
- Aktivity Evropské Unie

Využití Internetu

- Komunikační médium (e-mail, sociální sítě, Skype,..)
- Zpřístupnění informací (zpravodajství, umělecká díla,…)
- Elektronické obchodování, vzdělávání,…
- Komunikace s institucemi
- …

Zneužití Internetu

- Kyber - kriminalita
  - organizovaný zločin
  - útoky zevnitř
- špionáž (průmyslová, vojenská,…)
  - státní organizace
  - specializované hackerské skupiny
- sabotáž
  - vládní aktivity
  - haktivismus
  - terorismus (SCADA)
  - nájemní útočníci

Nejčastější trestné činy na Internetu

- 1740x podvod
- 206x poškození a zneužití záznamu na nosičích informací
- 173x porušení autorských práv
- 114x ostatní trestná činnost
- 113x úvěrový podvod

Historie aktivit NBÚ v kybernetické bezpečnosti

- **Usnesení vlády č. 781** ze dne 19. října 2011 – NBÚ ustaven gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast
- 11.2011 – 3.2012 **příprava Věcného záměru zákona**, novely Strategie pro oblast KB a Akčního plánu opatření ke Strategii
- **UV č. 382 ze dne** 30.5.2012 - ukládá řediteli Národního bezpečnostního úřadu, kromě jiného, zpracovat na základě věcného záměru zákona a předložit vládě do 31. července 2013 návrh zákona o kybernetické bezpečnosti.
- 30.6.2013 – návrh **ZKB** a vyhlášky odeslány **vládě**
- 9.2013 – začíná **práce** mezirezortní komise **na vyhláškách**
- 2.1.2014 – **schválení ZKB vládou** a odeslání do parlamentu
- 14.2.2014 **první čtení** – projednávání ve výborech

Základní principy budování kybernetické bezpečnosti v ČR

- Propojení a posílení spolupráce všech sektorů společnosti
  - Koordinace aktivit státu, akademické sféry a komerce
  - Důvěra a sdílení informací
- Individuální zodpovědnost
  - Odolnost systému vůči vnějším i vnitřním útokům
- Resortní spolupráce - gesce NBÚ, zřízení RKB a poradní komise ŘNBÚ
- Mezinárodní spolupráce – bilaterální, EU (ENISA,CERT EU), NATO, CCDCoE,…
- Přiměřenost přijatých opatření
- Analýza rizik

Hlavní zásady a pilíře nového ZKB

- 2 zásady ZKB:
  - minimalizace zásahů do práv soukromoprávních subjektů
  - individuální odpovědnost za bezpečnost vlastní sítě
- 3 pilíře ZKB:
  - bezpečnostní opatření (standardizace)
  - hlášení kybernetických bezpečnostních incidentů
  - (proti)opatření

Systém zajištění kybernetické bezpečnosti I.

- bezpečnostní opatření:
  - organizační
  - technická
- oznamování kontaktních údajů
- hlášení kybernetických bezpečnostních incidentů,
- (proti)opatření a
- činnost dohledových pracovišť

Systém zajištění kybernetické bezpečnosti II.

- **Kybernetickou bezpečnostní událostí** je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb a sítí elektronických komunikací.

- **Kybernetickým bezpečnostním incidentem** je kybernetická bezpečnostní událost, která představuje narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb a sítí elektronických komunikací.

- **ZKB** stanovuje povinnost detekce a hlášení kybernetických bezpečnostních incidentů.

Systém zajištění kybernetické bezpečnosti III.

- **Opatřeními** se rozumí úkony vydané Úřadem, jichž je třeba
  - k ochraně informačních systémů nebo služeb a sítí elektronických komunikací před hrozbou v oblasti kybernetické bezpečnosti
  - k předcházení kybernetickým bezpečnostním incidentům, nebo
  - k řešení již nastalého kybernetického bezpečnostního incidentu
- **Druhy opatření:**
  - varování,
  - reaktivní opatření
  - ochranné opatření

Systém zajištění kybernetické bezpečnosti IV.

- Vrcholová dohledová pracoviště:
  - **Vládní CERT** (GOVCERT.CZ),
    - provozuje Úřad v rámci NCKB
  - **Národní CERT** (CSIRT.CZ)
    - osoba soukromého práva – právnická osoba

Co je NCKB?

- Organizační složka NBÚ
- Součást státního systému chránícího kybernetický prostor
- Má 2 části:
  - Vládní CERT
  - Oddělení teoretické podpory, vzdělávání a výzkumu
- Hlavní úlohou centra je koordinace spolupráce na národní i mezinárodní úrovni při předcházení kybernetickým útokům i při návrhu a přijímání opatření při řešení incidentů i proti probíhajícím útokům.

Hlavní činnosti NCKB

- Plnit roli vrcholového pracoviště KB na úrovni státu
- Provozovat Vládní CERT České republiky
- Spolupráce s ostatními národními pracovišti CERT / CSIRT
- Spolupráce s mezinárodními pracovišti CERT / CSIRT
- Zastupování ČR v mezinárodních organizacích
- Příprava bezpečnostních standardů pro jednotlivé kategorie organizací v ČR
- Osvěta a podpora vzdělávání v oblasti kybernetické bezpečnosti
- Výzkum a vývoj v oblasti kybernetické bezpečnosti

Národní bezpečnostní úřad

NCKB – současnost I.

- Ukončena rekonstrukce sídla NCKB v Brně
- Instalace technologií
- Nábor lidí – specializace (forenzní analýzy, honey-nety, SCADA, výzkum, reverzní inženýrství – analýzy malware,…)
- Řešení nahlášených kybernetických incidentů (phishing, DDoS, …)
- Příprava nové národní strategie a akčního plánu
- Metodická podpora
- Pomoc při řešení incidentů
- „Botnet feeds“

NCKB – současnost II.

- Výzkum vývoj – Kybernetický polygon, CCC CoE
- Příprava projektu na bezpečné používání mobilních zařízení
- Veřejný informační servis (www.govcert.cz)
- Spolupráce NATO, Europol, OBSE, OSN, CCDCoE
- Připravujeme národní cvičení a zapojení do cvičení CMX 2014, Cyber Europe 2014, LS14 a Cyber Coalition 2014, CECSP 2014

NCKB – budoucnost

- Do budoucna i neveřejný informační servis
- ECG (TERENA, TF CSIRT, FIRST)
- Vybudování důvěry hodného komunikačního prostředí pro sdílení citlivých a utajovaných informací na národní a mezinárodní úrovni
- Vytvoření systému vzdělávání v oblasti kybernetické bezpečnosti pro základní a střední školy, zapojení do výuky vysokých škol
- Připravujeme účast na transatlantickém kybernetickém cvičení

Kompetence Vládního CERTu

- **Správci IS veřejné správy**
- **Správci systémů kritické informační infrastruktury**

Jejich základní povinnosti:

- oznámit NBÚ kontaktní údaje pro *okamžité* předávání informací o kybernetických bezpečnostních událostech;
- chránit své informační systémy bezpečnostními opatřeními, jejichž náležitosti stanoví NBÚ vyhláškou;
- hlásit výskyt bezpečnostních incidentů NBÚ a provádět protiopatření, která jim NBÚ stanoví.

Další dohledová pracoviště: (mezinárodně uznaná - TI)

(http://www.trusted-introducer.org/directory/country_LICSA.html)

- **CESNET-CERTS (A - 1/08) - CESNET**
- **CZ.NIC–CSIRT (A - 8/10) –CZ.NIC**
- **CSIRT-MU (A - 2/11) - MU**
- **CSIRT.CZ (A- 10/11) – CZ.NIC**
- **ACTIVE 24–CSIRT (L - 2/12) – ACTIVE 24**
- **SEZNAM.CZ–CSIRT (L - 10/13) - SEZNAM**
- **GovCERT.CZ (L - 11/13) - NBÚ**

Ostatní:

- **CIRC-MO**

Integrace kybernetické bezpečnosti státu

- Kybernetická dimenze musí být standardní součástí posouzení rizik
- Ochrana kyberprostoru musí integrovat a koordinovat již existující schopnosti:
  - Provozovatel národního CSIRTu
  - Policie
  - Zpravodajské služby
  - MO a AČR
  - Komerční sektor
  - Akademická sféra
- Nutnost efektivní koordinace a možnost jednotného zadávání úkolů

Dotazy?