Vytvoření Národního centra kybernetické bezpečnosti (NCKB) a jeho činnost

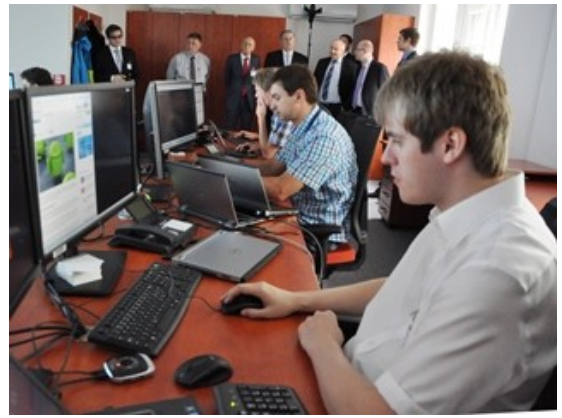
Ing. Dušan Navrátil

Usnesení vlády č. 781 ze dne 19. října 2011

- **NBÚ ustaven gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast**
- **Zřízena Rada pro kybernetickou bezpečnost**
- **Ř/NBÚ má předložit návrh věcného záměru zákona o kybernetické bezpečnosti vládě do 31. března 2012**
- **Ř/NBÚ má vybudovat do 31. prosince 2015 plně funkční Národní centrum kybernetické bezpečnosti a jako jeho součást vládní koordinační místo pro okamžitou reakci na počítačové incidenty (vládní CERT - Computer Emergency Response Team)**

NCKB

NCKB bylo slavnostně otevřeno 1.května 2014



NCKB

Součásti:

- **Vládni CERT (GOVCERT.CZ)**
- **Odbor kybernetických bezpečnostních politik**
- **Odbor regulace**
- **Odbor kontroly**

CERT/CSIRT

- **Trošku historie - první pracoviště CERT/CSIRT- Cordination Center (CERT/CC) vzniklo v roce 1988 na Carnegie Mellon University.**

- **Vytvoření světové sítě CERT/CSIRT pracovišť zodpovědných za reakci na kybernetické incidenty pro určitý okruh subjektů.**

- **Celosvětová spolupráce pracovišť CERT/CSIRT na bázi důvěry a dobrovolnosti provádí výměnu informací bez jakýchkoliv právních regulí.**

- **Každý CERT/CSIRT zveřejňuje základní informace o pracovišti, možnostech jeho kontaktování, jeho poslání, odpovědnosti, financování, constituency, organizační zakotvení, nabízených službách atd.**

CERT/CSIRT

Členění dle řešení podle řešení incidentů:

- **interní**
- **koordinační**
- **národní/vládní**
- **regionální**
- **sektorové**
- **produktové**

CERT/CSIRT

Členění dle typu působnosti:

- **Veřejný sektor**
- **Soukromý sektor**
- **Vojenský sektor**
- **Akademický sektor**

CERT/CSIRT

Členství v mezinárodních organizacích

FIRST (Forum for incident Responce and Security Teams)

Možnost stát se členem po atestaci a možnost vyloučení pro nedodržení zásad.

Zásady – operační nezávislost, reciprocita, důvěrnost a transparentnost.

Výhody členství:

- **Přístup k aktuálním dokumentům o osvědčených postupech při řešení incidentů**
- **Možnost účastnit se technických kolokvií pro bezpečnostní experty a školení.**
- **Možnost výročních konferencí FIRST k problematice řešení incidentů**

Další mezinárodní organizace – TF-CSIRT, CSIRT network a další

CERT/CSIRT

Základním těchto pracovišť úkolem je řešení incidentů (incident handling):

detekce události/hlášení o události

↓

založení události

↓

triage

↓

řešení(analýza) incidentu

↓

uzavření a klasifikace incidentu

↓

post analýza a závěrečný report

↓

doporučení/lesson learned

GOVSERT.CZ

- **Činnosti:**
- **Reaktivní – prvotní koordinace, zpracování a řešení kybernetických incidentů a vedení komunikačních kanálů s ostatními subjekty.**
- **Analýza síťového provozu – provozování síťových sond, IDS/IPS systémy a honeypoty, analýza dat získaných tímto způsobem a systémových logů**
- **Forézní analýza počítačů a mobilních zařízení.**
- **Analýza artefaktů vzniklých v souvislosti s bezpečnostními incidenty**
- **Analýza malware a reverzní inženýrství**
- **Získávání indikátorů kompromitace pro zamezení šíření malwaru**
- **Penetrační testování**
- **Problematika kybernetické bezpečnosti průmyslově orientovaných technologií a řídících systému (SCADA systémy.**
- **Spolupráce na cvičeních**

GOVSERT.CZ

Sdílení informací:

- **Informace o zranitelnostech**

- **Informace o možných hrozbách**

- **Vývoj bezpečnostní situace**

- **Strojově zpracovávaná data**
  - **Microsoft (BotNet Feee), Shadowserver, reputační služby, atd**
  - **detekce špatné konfigurace služeb**
  - **detekce zranitelností**

GOVCERT.CZ

Spolupráce

- Česká republika
  - tuzemské CSIRT týmy
  - Policie ČR
  - Zpravodajské služby

- Evropa
  - CSIRT NETWORK
  - TF-CSIRT
  - NATO a CCDCOE

- Svět
  - FIRST

GOVCERT.CZ

Činnost při kybernetickém útoku na nemocnici v Benešově:

- Zpráva v médiích
- Snaha kontaktovat nemocnici
- Rozhodnutí o pomoci a vyslání responce týmu
- Vydání upozornění na hrozbu Emotet-Trickbot-Ryuk
- Naplánováno penetrační testování

GOVCERT.CZ

Činnost responce týmu:

- **Analýza stavu**
- **Určení časového i věcného rozsahu kompromitace systému**
- **Návrh možných postupu při procesu obnovy dat**
- **Výpomoc při odstraňování a analýze škodlivého kódu**
- **Doporučení pro zabezpečení systému a sítě**

Odbor kybernetických bezpečnostních politik

- Vytváření dlouhodobých strategií, plánů a projektů
- Monitorování a evaluace nových hrozeb na strategické úrovni
- Právní a policy podpora GOVCERTU a úřadu
- Tvorba národních pozic ve vztahu k NATO, EU, OBSE
- Analytika založená na otevřených zdrojích a informací od GOVCERT partnerů
- Příprava varování
- Příprava konferencí
- Příprava technických a table top cvičení
- Vzdělávání
- Věda a výzkum

Odbor kybernetických bezpečnostních politik

Cvičení:

Technické cvičení

- **Modré týmy versus červený tým**
- **Cílové skupiny – subjekty podléhající zákonu z veřejné i neveřejné sféry**
- **Ve spolupráci s MU (projekt bezpečnostního výzkumu)**
- **Přibližně 80 osob zainteresovaných osob**

Strategické table top cvičení

- **Cílem provičit rozhodovací procesy na strategické úrovni**
- **Cílová skupina – zástupci subjektů veřejné i soukromé sféry**
- **Cvičící reagují na připravený scénář**

Odbor kybernetických bezpečnostních politik

Mezinárodní cvičení

NATO

- **Locked Shields**
- **Cyber Coalition**
- **CMX**

EU

- **Cyber Europe**
- **EU Pace**

Odbor regulace

- Zmapování informačních systémů veřejné správy
- Zmapování důležitých informačních systémů kritické infrastruktury soukromé sféry
- Zmapování informačních systémů v odvětvích definovaných NIS I.
- Stanovování kritérií pro určení informačních systémů spadajících pod zákon
- Tvorba a změna vyhlášek pro KII,VIS,PZS
- Určování KII,PZS
- Identifikace VIS
- Podpora a konzultační činnost subjektům, které jsou a mohou být určeny
- Posuzování nabídek cloud computingu
- Příprava implementace NIS II.
- Příprava zákona o dodavatelských řetězcích

Odbor kontroly

- **Provádí kontrolu na dodržování požadavků ZKB u regulovaných subjektů**
- **Na kontroly si zve odborníky z jiných odborů především z CERTu**
- **Dává podněty k zahájení správního řízení k udělení pokuty**

Odbor kontroly

Základní zjištěné nedostatky

Technické nedostatky:

- **Nedostatečná segmentace sítě**
- **Nikdo se nestará o zranitelnosti**
- **Nedochází k aktualizaci systémů**
- **Vystavování služeb do internetu bez dostatečného důvodu**
- **Ignorace „best practises“**
- **Neexistující sběr logů (centrální, často i lokální)**
- **Nevyhodnocování logů**
- **Neexistující nebo nedostatečný síťový monitoring**
- **Nedochází k analýze provozu**

Odbor kontroly

Základní zjištěné nedostatky

Manažérské:

- **Podfinancování kybernetické bezpečnosti**
- **Pravidlo minimálního nutného přístupu**
- **Provoz šéfuje bezpečnosti**
- **Management nejde příkladem (vyjimky)**
- **Nízké bezpečnostní povědomí uživatelů – neexistence školení**
- **Závislost na dodavatelích a outsourcing**
- **Nejsou havarijní plány**
- **Neexistence centrální správy**

Odbor vzdělávání

Uživatelé bez proškolení jsou bezpečnostní hrozbou

Příklady činnosti:

Vytvoření kontaktního místa pro koordinaci vzdělávacích pracovišť

- **Vedení evidence vzdělávacích aktivit kurzů školení atd.**
- **Koordinace se zahraničními vzdělávacími pracovišti**

E – lerning pro zaměstnance veřejné správy

- **Základy kybernetické bezpečnosti – určeny pro všechny pracovníky**
- **Kurz kybernetické bezpečnosti kteří plní role dle ZKB**

Rozcestníky s se vzdělávacími materiály pro:

- **Děti**
- **Rodiče**
- **Senioři**
- **učitelé**

Dotazy?

Diskuze.