Vznik Národního centra kybernetické bezpečnosti v rámci NBÚ, jeho přeměna v NÚKIB, vývoj strategií kybernetické bezpečností.

Ing. Dušan Navrátil

Vývoj problematiky informační a kybernetické bezpečnosti

2000	Aktualizovaná koncepce koncepce boje proti organizovanému zločinu
2001	Koncepce boje proti trestné činnosti v oblasti informačních technologií
2004	Státní informační a komunikační politika e-Česko 2006
2007	Akční plán realizace opatření Národní strategie informační bezpečnosti České republiky
2010	Zřízení mezirezortní koordinační rady pro oblast kybernetické bezpečnosti
2010	Podpis Memoranda o CSIRT se sdružením CZ.NIC
2011	Strategie pro oblast kybernetické bezpečnosti České republiky na období 2011-2015
2011	Přechod gesce na kybernetickou na NBÚ
2011	Zřízení Rady pro kybernetickou bezpečnost

Proč došlo ke změně garanta ? A proč regulace zákonem? Stav v roce 2011.

. Kybernetická bezpečnost státu byla řešena prostřednictvím soukromých/ akademických, subjektů, bez právní regulace

. Nedostatek koordinace a nedostatečné sdílení informací

. Kybernetická ochrana byla roztříštěná a neefektivní

. Nebyly bezpečnostní standarty kybernetické bezpečnosti (s vyjímkou ICT obsahujících utajované informace)

Odpovědnost NBÚ v oblasti kybernetické bezpečnosti

- **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 zákona o kybernetické bezpečnosti vládě**
- **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)**

Pozn. Materiální zajištění bylo 60 milionu Kč na rok 2012, budova v Brně, zřízení nových funkčních míst) 8 v roce 2012,10 v roce 2013, 10 v roce 2014 a 5 v roce 2015

NBÚ garant kybernetické bezpečnosti

2011
- **NBÚ ustanoven jako národní autorita a gestor KB vznik Národního centra kybernetické bezpečnosti**

2012
- **Národní strategie kybernetické bezpečnosti I.**

2014
- **Národní centrum kybernetické bezpečnosti**

2015
- **Zákon o kybernetické bezpečnosti a příslušné vyhlášky**
- **Národní strategie kybernetické bezpečnosti II.**

2016
- **Směrnice NIS I**

2017
- **Novela zákona o kybernetické bezpečnosti**
- **Vznik NÚKIB**

NBÚ

nckb

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

NCKB

Součásti:

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

NCKB

- **NCKB slavnostně otevřeno 1.května 2014**

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.**

Pozn. CERT - Computer Emergency Response Team

CSIRT - Computer Security Incident Response Team

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 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**

NUKIB

- **Rozhodnutí vlády z prosince 2016 o vzniku samostatného úřadu NUKIB delimitací z NBÚ**
- **V prosinci 2016 v Poslanecké sněmovně Parlamentem ČR byla po prvním čtení novela ZKB (implementace směrnice EU - NIS I.)**
- **Pozměňovací poslanecký návrh předložený ve druhém čtení ve výboru pro bezpečnost definoval nový úřad – NUKIB**
- **Součástí pozměňovacího návrhu byla i novela Zákona o utajovaných informacích 412/2005 Sb.**
- **Novely schváleny v červnu 2017 Senátem Parlamentu ČR a podepsány prezidentem**
- **Platnost novely od 1. srpna 2017 – vznik NUKIB**
- **Leden – červenec 2017 - příprava delimitace NCKB, certifikace IS obsahujících utajované informace, Tempest, krypto a Galileo z NBU**
- **Leden – červenec 2017 – vytvoření nové obslužné sekcee – ekonomika, správa, vnitřní IT a právní věci ještě v rámci NBU a poté delimitováno**
- **Červen 2017 - novela zákona o státním rozpočtu – vlastní rozpočtová kapitola**
- **1. srpna 2017 vznik NUKIB**
- **Říjen 2017 – parlamentní volby**

Národní strategie kybernetické bezpečnosti na období 2012 - 2015

Základní principy:

. propojení a posílení spolupráce všech sektorů společnosti

. individuální zodpovědnost

. resortní spolupráce

. mezinárodní spolupráce

. přiměřenost přijatých opatření

úkoly:

. Vytvoření legislativního rámce

. Vybudování Národního centra kybernetické bezpečnosti a vládního pracoviště CERT

Národní strategie kybernetické bezpečnosti na období 2012 - 2015

Cíle:

. ochrana kritických informačních infrastruktur

. posilování kybernetické bezpečnosti informačních a komunikačních systémů veřejné správy

. zefektivnění potírání kriminality v kybernetickém prostoru

. koordinace aktivit k zajištění kybernetické bezpečnosti v Evropě

. používání spolehlivých a důvěryhodných informačních technologií

. zvyšování povědomí o kybernetické bezpečnosti

. odezva na kybernetické útoky

Akční plán ke Strategii 2012-2015

- **Vytvoření legislativního rámce k posílení kybernetické bezpečnosti ČR, podpora a ochrana lidských práv a svobod.**
- **Podpora mezinárodní spolupráce v v oblasti kybernetické bezpečnosti.**
- **Národní spolupráce v oblasti kybernetické bezpečnosti(veřejné, soukromé a akademické).**
- **Koordinace a řízení rizik ČR.**
- **Zvyšování povědomí a znalostí o kybernetické bezpečnosti.**

Národní strategie kybernetické bezpečnosti na období 2015 - 2020

Principy:

- **Ochrana základních lidských práv a principů demokratického právního státu.**
- **Komplexní přístup ke kybernetické bezpečnosti na principu subsidiarity a spolupráce.**
- **Budování důvěry a spolupráce mezi veřejným sektorem a občanskou společností.**
- **Rozvoj kapacit k zajišťování kybernetické bezpečnosti.**

Národní strategie kybernetické bezpečnosti na období 2015 - 2020

Výzvy:

- **ČR jako možný testovací objekt.**
- **Nedostatečná důvěra ve stát.**
- **Vzrůstající počet uživatelů internetu, informačních a komunikačních technologií a nárůstající kritičnost jejich selhání.**
- **Se vzrůstajícím počtem uživatelů mobilních platforem stoupá i množství mobilního malwere.**
- **Možnosti zneužití zadních vrátek hardwere pro exfiltraci informací.**
- **Koncept „internet věcí“.**
- **Bezpečnostní rizika spjatá s elektronizací veřejné správy (eGoverment)**
- **Nedostatečné zabezpečení malých podniků**
- **Big data, skladování dat v nových prostředích.**

Národní strategie kybernetické bezpečnosti na období 2015 - 2020

Výzvy:

- **Ochrana průmyslových řídících systémů a informačních systémů ve zdravotnictví.**
- **Inteligentní energetické sítě.**
- **Vzrůstající závislost obraných složek státu na informačních a komunikačních technologiích.**
- **Malware je stále sofistikovanější.**
- **Botnety a a DDoS/DoS útoky.**
- **Nárust informační kriminality.**
- **Hrozby rizika spjaté s užíváním sítí na internetu.**
- **Nízká digitální gramotnost koncových uživatelů.**
- **Nedostatek odborníků na kybernetickou bezpečnost a nutnost revize stávajících studijních programů ve školství.**

Národní strategie kybernetické bezpečnosti na období 2015 - 2020

Hlavní cíle:

- **Zajišťování efektivity a posilování všech struktur, procesů a spolupráce při zajišťování kybernetické bezpečnosti.**
- **Aktivní mezinárodní spolupráce.**
- **Ochrana národní KII a VIS**
- **Spolupráce se soukromým sektorem.**
- **Výzkum a vývoj.**
- **Podpora vzdělávání, osvěta a rozvoj informační společnosti.**
- **Podpora rozvoje schopností Policie ČR vyšetřovat a postihovat informační kriminalitu.**
- **Právní úprava pro kybernetickou bezpečnost (vytváření právního rámce). Účast na tvorbě a implementaci evropských a mezinárodních pravidel.**

Akční plán ke Strategii 2015-2020

Celkem 45 cílů a 141 úkoly

Některé vybrané úkoly:

- **Provádět technická i netechnická národní cvičení kybernetické bezpečnosti.**
- **Aktivně spolupracovat s EU, Evropskou komisí a jejími agenturami k zajištění větší koherence.**
- **Spolupracovat a aktivně se podílet na práci ENISA v oblasti síťové a informační bezpečnosti.**
- **Pravidelně se účastnit a aktivně se podílet na vytváření scénářů mezinárodních cvičení v oblasti kybernetické bezpečnosti.**
- **Podílet se na vytváření efektivního modelu spolupráce a budování důvěry mezi pracovišti CERT a CSIRT na mezinárodní úrovni , mezinárodními organizacemi a akademickými centry**

Akční plán ke Strategii 2015-2020

- **Podílet se vytváření mezinárodního koncenzu v rámci oficiálních i neoficiálních kanálů ohledně právních norem a chování v kyberprostoru, zajištění otevřenosti internetu lidských práv a dohod.**
- **Zajišťovat a Metodicky řídit nasazování detekčních systémů pro monitorování provozu sítí v rámci státní správy.**
- **Podporovat projekt Fénix a zapojení významných sítí veřejné správy za účelem funkcionalit a služeb během masívních kybernetických útoků.**
- **Vytvořit a vládě předložit Národní strategii cloud computingu. - MV**
- **Vypracovat a vládě předložit projekt státního cloudu včetně datových uložišť a další potřebné podklady (finační, bezpečnostní,organizační a technické nároky). – MV**
- **Zmapovat současný stav a případně vypracovat návrh legislativních změn s ohledem na vytvoření státního cloudu včetně datových úložišť. - MV**

Akční plán ke Strategii 2015-2020

- **V rámci Vojenského zpravodajství vytvořit Národní centrum kybernetických sil, které bude schopné provádět široké spektrum operací v kyberprostoru a aktivity nutné pro zajištění kybernetické obrany ČR. - VZ**
- **Připravit návrh nutných legislativních změn pro potřeby plné funkčnosti NCKS. – VZ**
- **Navyšovat povědomí a gramotnost v otázkách kybernetické bezpečnosti jak u žáků a studentů základních a středních škol, tak u široké veřejnosti, respektive koncových uživatelů.**
- **Posílit personálně jednotlivá policejní pracoviště informační kriminality. - MV**

Národní strategie kybernetické bezpečnosti na období 2021 - 2025

Sebevědomě v kyberprostoru

- **Společný přístup ke kybernetické bezpečnosti.**
- **Bezpečná infrastruktura.**
- **Účinná strategická komunikace.**
- **Sebevědomá reakce.**
- **Budoucí výzvy**

Silná a spolehlivá spojenectví

- **Efektivní mezinárodní spolupráce**
- **Prohlubování a tvorba aktivních spoluprací.**
- **Mezinárodní právní rámec.**
- **Schopnosti a expertíza.**

Národní strategie kybernetické bezpečnosti na období 2021 - 2025

Odolná společnost

- **Zabezpečení digitální společnosti a veřejné správy.**
- **Vzdělávání a osvěta.**
- **Rozšíření expertní základy.**

Akční plán ke Strategii 2021-2025

Některé vybrané úkoly:

- **Sbližovat přístup ke kybernetické bezpečnosti a ochraně utajovaných informací v informačních a komunikačních systémech.**
- **Vytvořit návrh posuzování rizikového profilu na národní úrovni a uplatňování omezování vysoké rizikových dodavatelů do systému regulovaných ZKB a pro bezpečné zavádění a realizaci telekomunikačních sítí nastupující generace.**
- **Vhodně propojovat činnost vedoucí k navyšování kybernetické bezpečnosti s aktivitami navyšujícími rovněž odolnost ČR proti hybridním hrozbám.**
- **Vytvořit, implementovat a v relevantních případech aktivovat efektivní národní rámec plnohodnotné atribuce závažných kybernetických útoků.**
- **Konsolidovat přístupy k odstrašení kybernetických útoků s cílem následně koncepčně využít pro co nejefektivnější původců útoku.**

Akční plán ke Strategii 2021-2025

- **Vypracovat koncepci rozvoje schopností rychlé reakce určené k řešení rozsáhlých bezpečnostních incidentů.**
- **Připravit návrh aktualizace standardů šifrování pro orgány a osoby povinné dle ZKB zohledňující nástup kvantovaných počítačů a tím související hrozbu prolomení současných metod šifrování.**
- **Vytvořit návrh jednotné sítě státní správy a souvisejících navazujících , relevantních projektů, s cílem navýšit kybernetickou bezpečnost státních institucí s pomocí plošně aktivovaných standartů zabezpečení.**
- **Naplňovat „Koncepci rozvoje Národního úřadu pro kybernetickou a informační bezpečnost“ a rozvíjet kapacity NÚKIB v oblasti nových hrozeb.**

Příklady nových hrozeb

- **Umělá inteligence.**
- **Kvantové počítače a s tím související post-kvatovou kryptografii a kvantovou komunikační infrastrukturu.**
- **Bio-technologie.**
- **Bio-hacking.**
- **Bezpečnostní systémy založené na umělé inteligenci a strojovém učení.**
- **Drony a další robotická, autonomní zařízení.**
- **Rozšířená realita.**
- **Smart(„chytré“) technologie a jejich bezpečnostní protokoly.**
- **Používání bezpečných senzorových sítí.**
- **Nové metody kybernetického válčení.**
- **Problematika digitálních měn, apod.**

Dotazy?

Diskuze.