Vznik národních strategií kybernetické bezpečnosti v České republice a převedení kompetence za kybernetickou bezpečnost státu na NBÚ

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

2017

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

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 změnpro 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 zaváděnía 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.