Vyhodnocení Strategie pro oblast kybernetické bezpečnosti v České republice na období 2012 – 2015

Předkládaný materiál je vyhodnocením Strategie pro oblast kybernetické bezpečnosti v České republice na období 2012 – 2015 (dále jen Strategie), kterou nahradí od 1. ledna 2015 „Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020“.

Strategie měla zlepšit úroveň kybernetické bezpečnosti pro vládní instituce, kritickou infrastrukturu i pro komerční sféru, potažmo i pro obyvatele České republiky. Samotný dokument je členěn do tří částí. První část popisuje východiska, která určují nutnost řešení problému. Druhá část přináší analýzu problému a základní principy kybernetické bezpečnosti. Ve třetí části jsou stanoveny cíle a popsány aktivity důležité pro zvyšování kybernetické bezpečnosti – aktivity prováděné a implementované vládou České republiky a aktivity prováděné ve spolupráci s partnery.

Zde předkládané vyhodnocení Strategie je zaměřeno na evaluaci především třetí části, tj. vyhodnocení hlavních cílů a aktivit – zdali a do jaké míry byly cíle dosaženy a aktivity realizovány. Ve strategii totiž můžeme identifikovat hlavní prioritní oblasti v budování kybernetické bezpečnosti v České republice mezi lety 2012 – 2015, které jsou následně rozpracovány do úkolů v Akčním plánu. A právě tyto úkoly odvozené z hlavních cílů, u nichž byl stanoven jak způsob realizace, tak i výstupy jsou předmětem zde předkládaného vyhodnocení.

Závěrem je tedy třeba podtrhnout, že dva hlavní strategické cíle, o něž se Strategie opírala (vytvoření legislativního rámce v kybernetické bezpečnosti a vybudování Národního centra kybernetické bezpečnosti a vládního pracoviště CERT), byly úspěšně splněny a zbytek úkolů, respektive hlavních cílů Strategie byl rovněž uskutečněn, či je průběžně naplňován. Realizaci Strategie je tak na základě zde překládaného vyhodnocení možno považovat za úspěšnou a lze konstatovat, že v České republice byla od roku 2012 znatelně navýšena úroveň kybernetické bezpečnosti.

Vyhodnocení Strategie

I. Vytvoření legislativního rámce k posílení kybernetické bezpečnosti České republiky, podpora a ochrana lidských práv a svobod

Poř. č.	Název cíle	Název úkolu	Realizace a výstupy
1.	Zákon o kybernetické bezpečnosti	Příprava zákona o kybernetické bezpečnosti.	Zákon o kybernetické bezpečnosti, prováděcí předpisy, novelizace jiných právních předpisů.
Vyhodnocení: Splněno			
Národní bezpečnostní úřad (dále již jen NBÚ) dne 28. června 2013 předložil vládě České republiky návrh zákona o kybernetické bezpečnosti a o změně souvisejících zákonů, který byl následně schválen vládou i Parlamentem ČR a Prezident republiky jej podepsal dne 13. srpna 2014. Zákon o kybernetické bezpečnosti nabude platnosti dnem vyhlášení ve Sbírce zákonů, účinný bude od 1. ledna 2015.			

II. Podpora mezinárodní spolupráce v oblasti kybernetické bezpečnosti

Poř. č.	Název cíle	Název úkolu	Realizace a výstupy
2.	Zapojení do mezinárodních cvičení v oblasti kybernetické bezpečnosti	Aktivně se zapojit do mezinárodních cvičení s prvky národní kybernetické obrany.	Zlepšování spolupráce a výměna zkušeností zejména při cvičeních EU a NATO.
Vyhodnocení: Průběžně plněno			
NBÚ, potažmo jeho specializované pracoviště NCKB se zúčastnilo již mnoha cvičení v oblasti kybernetické bezpečnosti, a to ať již samostatně, tak i ve spolupráci s např. vojenským CIRC, MO, MZV, Policií ČR, BIS, CZ.NIC, aj. Česká republika participovala v letech 2012 – 2015 např. na těchto cvičeních: Cyber Coalition, CMX, Locked Shield, Cyber Europe, cvičení CECSP.			

Poř. č.	Název cíle	Název úkolu	Realizace a výstupy
3.	Realizace efektivní spolupráce a koordinace na národní i mezinárodní úrovni	Provozovat portál GovCERT jako jednotný informační prostředek pro zajištění efektivní komunikace v oblasti kybernetické bezpečnosti na národní i mezinárodní úrovni.	Zřízení pracovních skupin pro oblast kybernetické bezpečnosti České republiky v rámci RKB. Zveřejnění výstupů na portálu GovCERTu jako platformy pro zajištění spolupráce s odbornou veřejností.
Vyhodnocení: Průběžně plněno			
Efektivní spolupráce a koordinace na národní i mezinárodní úrovni je prováděna kontinuálně. Portál GovCERT.CZ je provozován NBÚ a slouží jako informační platforma ohledně kybernetické bezpečnosti v ČR, zveřejňují se zde veškeré výstupy Národního centra kybernetické bezpečnosti (NCKB), potažmo vládního CERTu (GovCERT.CZ), (aktuality, publikace, informace o hrozbách a zranitelnostech, legislativa, atd.). Portál slouží i jako platforma pro zajištění spolupráce s odbornou veřejností.		

Poř. č.	Název cíle	Název úkolu	Realizace a výstupy
4.	Realizace aktivní mezinárodní spolupráce	Aktivně se účastnit přípravy legislativy a norem a další spolupráce týkající se kybernetické bezpečnosti v rámci Evropské unie i mimo ní.	Zapojení expertů v oblasti legislativy, ICT a bezpečnosti jednotlivých resortů v oblasti kybernetické bezpečnosti do přípravy legislativy a norem v rámci EU a NATO.
Vyhodnocení: Průběžně plněno			
ČR se aktivně účastní přípravy legislativy, norem a participuje na dalších aktivitách týkajících se kybernetické bezpečnosti v rámci Evropské unie i mimo ní (viz např. Zpráva o stavu kybernetické bezpečnosti České republiky – dostupné na www.govcert.cz). V rámci legislativy a norem se především jedná aktivní zapojení do diskuze ohledně návrhu směrnice Evropského parlamentu a Rady EU o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v EU („Směrnice NIS“) či přijetí opatření za účelem budování důvěry v oblasti kybernetické bezpečnosti (Confidence Building Measures) na půdě OBSE.			

Poř. č.	Název cíle	Název úkolu	Realizace a výstupy
5.	Realizace aktivní mezinárodní spolupráce	Zapojit se do vytváření národních a mezinárodních pozorovacích a varovných sítí, se schopností odhalit a zabránit kybernetickým útokům v době vzniku.	Zajištění uvedených činností prostřednictvím uzavírání mezinárodních smluv.
Vyhodnocení: Splněno			
NBÚ/NCKB připravilo zapojení České republiky do NATO Cooperative Cyber Defence Centre of Excellence v Tallinnu. Dne 4. prosince 2013 vláda schválila usnesení č. 926/2013 Sb., o zapojení České republiky do NATO Cooperative Cyber Defence Centre of Excellence. Díky tomu se NBÚ/NCKB brzy zapojí mimo jiné i do platformy MISP (Malware Information Sharing Platform), která umožňuje důvěryhodným stranám sdílet technické charakteristiky malwaru. V roce 2013 byla rovněž podepsána smlouva mezi NBÚ/NCKB a společností Microsoft upravující spolupráci v problematice botnetů, respektive předávání informací ze strany Microsoftu o napadených počítačích malwarem, které jsou součástí botnetů. Česká republika se tak aktivně zapojuje do vytváření národních a mezinárodních pozorovacích a varovných sítí, se schopností odhalit a zabránit kybernetickým útokům.			

III. Národní spolupráce v oblasti kybernetické bezpečnosti (veřejné, soukromé a akademické)

Poř. č.	Název cíle	Název úkolu	Realizace a výstupy
6.	Zvýšení informovanosti	Prostřednictvím portálu GovCERTu a dalších prostředků prezentovat nejlepší znalosti a praxi v oblasti kybernetické bezpečnosti.	Zveřejňování získaných zkušeností při eliminaci kybernetických hrozeb na portálu GovCERTu i jinými prostředky
Vyhodnocení: Splněno			
NBÚ pravidelně zveřejňuje na svém portálu GovCERT.CZ nejnovější informace o kybernetických bezpečnostních hrozbách a rizicích a tím zvyšuje povědomí a informovanost o kybernetické bezpečnosti a možnostech ochrany. Na portálu jsou rovněž pravidelně v měsíčních intervalech zveřejňovány i bulletiny NCKB, respektive zprávy o bezpečnostních incidentech za daný měsíc.			

Poř. č.	Název cíle	Název úkolu	Realizace a výstupy
7.	Využívání stávajících zkušeností při budování kybernetické bezpečnosti	Podporovat zavádění a efektivní správu systémů řízení kybernetické bezpečnosti.	Příprava metodik, standardů a doporučení vycházejících ze zásad zavádění systému ISMS a norem řady BS ISO/IEC 270XX.
Vyhodnocení: Splněno			
NBÚ vypracoval návrh vyhlášky o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti) k provedení zákona o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Návrh vyhlášky, který byl vypracován ve spolupráci s Ministerstvy vnitra a obrany, Českým telekomunikačním úřadem, Bezpečnostní informační službou a Úřadem pro zahraniční styky a informace a byl konzultován se zástupci odborné veřejnosti, naplňuje a rozvádí především první pilíř zákona o kybernetické bezpečnosti, tj. obsah a rozsah bezpečnostních opatření pro kritickou informační infrastrukturu a významné informační systémy.			

IV. Koordinace a řízení rizik kybernetické bezpečnosti České republiky

Poř. č.	Název cíle	Název úkolu	Realizace a výstupy
8.	Organizační začlenění systému včasného varování a reakce na kybernetické útoky	Budovat vládní pracoviště pro koordinaci, řízení, monitoring a analýzu aktuálního stavu informačních a komunikačních systémů České republiky.	Budování vládního pracoviště CERT s kompetencemi koordinovat činnost při stanovení prevence detekce a reakce na kybernetické útoky v České republice.
Vyhodnocení: Splněno			
Česká republika otevřela 13. května 2014 NCKB v Brně, které nyní slouží jako pracoviště zajišťující koordinaci spolupráce na národní i mezinárodní úrovni v oblasti kybernetické bezpečnosti a provádí kvalitní a efektivní systém detekce, analýzy, řešení a předpovídání kybernetických útoků. Součástí tohoto centra je i GovCERT.CZ, jehož úloha spočívá v monitorování kybernetického prostoru a odhalování a řešení kybernetických útoků, jejich prevence, apod.			

Poř. č.	Název cíle	Název úkolu	Realizace a výstupy
9.	Realizace systému včasného varování a reakce na kybernetické útoky	Vládní pracoviště CERT vytvoří jednotný systém včasného varování, reakce a výměny informací ke snížení rizik plynoucích z hrozeb informačních a komunikačních systémů.	Zveřejňovat varování o bezpečnostních hrozbách a incidentech na portálu GovCERTu nebo i jiným vhodným způsobem s doporučením na zvládání rizik.
Vyhodnocení: Splněno			
NBÚ pravidelně zveřejňuje na svém portálu (www.GovCER0054.cz) nejnovější informace a varování ohledně kybernetických bezpečnostních incidentů, hrozbách a rizicích spolu s doporučeními na jejich zvládání.			

Poř. č.	Název cíle	Název úkolu	Realizace a výstupy
10.	Sběr informací a analýza kybernetických hrozeb a rizik v České republice	Provádět sběr informací o hrozbách a rizicích a analyzování současné situace v České republice i ve světě	Zřízení evidence bezpečnostních událostí a jejich pravidelné vyhodnocování a aktualizace.
Vyhodnocení: Průběžně plněno			
GovCERT.CZ provozuje systém „Request Tracker (RT)“, který slouží pro hlášení a evidenci požadavků, respektive kybernetických bezpečnostních událostí/incidentů. Kybernetické bezpečnostní incidenty se pak vyhodnocují a zveřejňují jednak měsíčně v rámci tzv. „Bulletinů“ a jednak jednou ročně v rámci Zprávy o stavu kybernetické bezpečnosti v ČR (viz www.GovCERT.cz). Sběr informací o kybernetických bezpečnostních hrozbách, rizicích a zranitelnostech provádí GovCERT.CZ pomocí systému Taranis. Tento nástroj slouží pro monitoring velkého množství internetových zdrojů, z nichž jsou stahovány a hodnoceny informace v pravidelných intervalech a výsledkem je tvorba analýz, bezpečnostních doporučení, či e-mailů rychlého varování.			

Poř. č.	Název cíle	Název úkolu	Realizace a výstupy
11.	Nastavení spolupráce při zabezpečení kybernetické bezpečnosti se soukromým sektorem a akademickou obcí	Nastavit a dále podporovat spolupráci NCKB s orgány veřejné moci, soukromými subjekty a akademickými subjekty zabývajícími se problematikou kybernetické bezpečnosti	Nastavení a zlepšování spolupráce a výměna zkušeností. Uzavírání smluv.
Vyhodnocení: průběžně plněno			
NBÚ s vybranými vysokými školami podepsalo rámcové smlouvy o spolupráci, které umožňují realizaci společných projektů v rámci kybernetické bezpečnosti.			

Poř. č.	Název cíle	Název úkolu	Realizace a výstupy
12.	Vyhodnocování účinnosti navržených opatření	Posuzování účinnosti navržených a prováděných opatření	Zpracování zprávy o stavu kybernetické bezpečnosti 1x ročně a předložení této zprávy vládě cestou Rady pro kybernetickou bezpečnost (RKB). Jednání RKB. Společná setkání odborníků.
Vyhodnocení: Splněno			
Pravidelně (1x ročně) vychází zpráva o stavu kybernetické bezpečnosti (viz www.govcert.cz), která se předkládá vládě cestou RKB. Zároveň probíhají několikrát ročně i jednání RKB a NBÚ i další aktéři kybernetické bezpečnosti ČR pravidelně spolupracují s odborníky z akademické či soukromé sféry.			

Poř. č.	Název cíle	Název úkolu	Realizace a výstupy
13.	Zlepšení spolupráce při zabezpečení kybernetické bezpečnosti	Vytvořit pro informační a komunikační systémy státu potřebné postupy pro rychlý přechod z běžného do krizového stavu.	Na úrovni RKB zadat zpracování krizových plánů jednotlivých systémů, realizace pravidelných vzdělávacích programů personálu, nácviky postupů při obnově služeb informačních systémů.
Vyhodnocení: Průběžně plněno			
Postupy nezbytné pro ochranu informačních a komunikačních systémů spadajících pod kritickou informační infrastrukturu a významné informační systémy jsou definovány ve vyhlášce ke kybernetické bezpečnosti, tzv. standardizační vyhlášce. K procvičení těchto0020postupů a tudíž pozvednutí úrovně znalostí a připravenosti na krizový stav slouží institut kybernetických cvičení.			

Poř. č.	Název cíle	Název úkolu	Realizace a výstupy
14.	Zpracování analýzy rizik informačních a komunikačních systémů veřejné správy s návrhem na zvládání rizik.	Vytvoření přehledu informačních a komunikačních systémů České republiky. Provedení analýzy rizik poskytovaných služeb dodavatelů, kteří nejsou v majetku veřejné správy. Návrh opatření ke zvládání rizik.	Návrh komplexních opatření na zvládání uvedených rizik.
Vyhodnocení: Částečně splněno			
Analýze rizik (dále jen AR) informačních systémů předcházel proces mapování IS u subjektů identifikovaných jako držitelé KII nebo VIS. Komplexní analýza na úrovni státu je možná až po zevrubném zmapování aktiv jednotlivých subjektů. Vzhledem k časové a finanční náročnosti komplexní analýzy rizik vykonané jedním subjektem, je preferovanou variantou zpracování AR v jednotlivých subjektech nad jejich aktivy. Tento proces byl nastartován mapováním a pokračuje určováním KII a VIS v průběhu let 2014-2015. Po určení IS a jejich statusu, kde AR je jedním z klíčových parametrů bezpečnosti ICT bude stav vyhodnocen a rozhodnuto, jakým způsobem přistoupit ke komplexní AR na úrovni státu v oblasti kybernetické bezpečnosti. Požadavek na AR na úrovni státu nadále trvá.			

V. Zvyšování povědomí a znalostí o kybernetické bezpečnosti

Poř. č.	Název cíle	Název úkolu	Realizace a výstupy
15.	Zvyšovat povědomí o kybernetické bezpečnosti, rizicích a možnostech obrany občanů, subjektů komerční a nekomerční sféry a orgánů veřejné správy	Podporovat povědomí o kybernetické bezpečnosti mezi firmami, veřejnou správou a dalšími organizacemi.	Zveřejňování zkušeností a praxe v oblasti kybernetické bezpečnosti na portálu GovCERTu a jinými vhodnými prostředky.
Vyhodnocení: Splněno			
NBÚ pravidelně zveřejňuje na svém portálu (www.GovCERT.cz) nejnovější informace o kybernetických bezpečnostních hrozbách a rizicích a tím zvyšuje povědomí o kybernetické bezpečnosti a možnostech ochrany občanů, subjektů komerční a nekomerční sféry a orgánů veřejné správy.			

Poř. č.	Název cíle	Název úkolu	Realizace a výstupy
16.	Zavést školicí a vzdělávací programy	Definovat cílovou úroveň znalostí pro jednotlivé role v oblasti kybernetické bezpečnosti podle role, kterou zde uživatelé plní.	Zpracování metodického pokynu a způsobu plnění.
Vyhodnocení: Splněno			
Byl proveden průzkum úrovně kybernetické vzdělanosti žáků základních a středních škol a také mapování systému vzdělávání na těchto školách. NBÚ s vybranými vysokými školami podepsalo rámcové smlouvy o spolupráci, které umožňují realizaci společných projektů v rámci zvyšování osvěty a vzdělávání ohledně kybernetické bezpečnosti.			

Poř. č.	Název cíle	Název úkolu	Realizace a výstupy
17.	Podpořit celkový program národního povědomí o kybernetické bezpečnosti	Kybernetickou bezpečnost začlenit do odborného vzdělávání.	Zpracování metodického pokynu a způsobu plnění, edukace v oblasti kybernetické bezpečnosti.
Vyhodnocení: Průběžně plněno			
NBÚ znatelně přispívá k edukaci české společnosti v oblasti kybernetické bezpečnosti. Mezi lety 2012 - 2014 se zástupci NBÚ, potažmo NCKB zúčastnili např. konferencí eGovernment, AFCEA, ICT unie, AEC Security, New Media Inspiration, CyberCon Brno, Job Challenge, pracovní skupiny CSIRT.CZ, klubového večera ISACA, aj. a v květnu 2014 NBÚ/NCKB dokonce uspořádalo vlastní odbornou konferenci s názvem „Kybernetická bezpečnost - výsledky a výzvy“. Mimo to NBÚ/NCKB poskytuje rozhovory a vystupuje v rámci nejrůznějších médií (TV, rozhlas, noviny, odborné časopisy), a to jak na témata aktuálních hrozeb, útoků či rizik, tak na témata týkající se obecně problematiky kybernetické bezpečnosti. NBÚ/NCKB také spolupracuje s Národním centrem bezpečnějšího internetu (NCBI), a to zejména v rámci každoroční akce „Evropský měsíc kybernetické bezpečnosti“, který je napříč Evropskou unií koordinován Evropskou agenturou pro síťovou a informační bezpečnost (ENISA) a v České republice konkrétně NCBI. Jedním ze způsobů edukace pracovníků státní správy a společnosti obecně je i e-learning. NBÚ/NCKB připravuje elektronické kurzy ke zvýšení povědomí v oblasti kybernetické bezpečnosti. NBÚ/NCKB uzavřelo partnerské smlouvy s univerzitami a vysokými školami v ČR k zajištění těsnější spolupráce na vzdělávání a výzkum v oblasti KB.			