III.

AKČNÍ PLÁN

KE STRATEGII PRO OBLAST KYBERNETICKÉ BEZPEČNOSTI V ČESKÉ REPUBLICE NA OBDOBÍ 2012 - 2015

Obsah

ÚVOD

Vláda České republiky schválila svým usnesením ze dne 20. července 2011 č. 564 Strategii pro oblast kybernetické bezpečnosti České republiky na období 2011 – 2015 a Akční plán opatření ke Strategii pro oblast kybernetické bezpečnosti České republiky na období 2011 - 2015. Následně vláda usnesením ze dne 19. října 2011 č. 781 uložila Národnímu bezpečnostnímu úřadu tuto Strategii a Akční plán aktualizovat. V průběhu procesu aktualizace uvedených dokumentů, při zachování základní podmínky splnitelnosti stanovených úkolů a reálnosti termínů, dospěl Národní bezpečnostní úřad k závěru, že je třeba dokument zásadním způsobem přepracovat.

S přihlédnutím k výsledkům připomínkového řízení tak vznikly úplně nové dokumenty pro období 2012 – 2015, které navazují na původní a úkoly na roky 2012 – 2015 vytyčují zcela nově.

Cílem nové Strategie pro oblast kybernetické bezpečnosti České republiky na období 2012 – 2015 (dále jen „Strategie“) je formulovat oblasti, priority a cíle kybernetické bezpečnosti, které je nutné zavést do praxe v období let 2012 - 2015. Strategie stanovuje tyto hlavní prioritní oblasti v budování kybernetické bezpečnosti v České republice, kterými jsou:

I. Vytvoření legislativního rámce k posílení kybernetické bezpečnosti České republiky, podpora a ochrana lidských práv a svobod.
II. Podpora mezinárodní spolupráce v oblasti kybernetické bezpečnosti.
III. Národní spolupráce v oblasti kybernetické bezpečnosti (veřejné, soukromé a akademické).
IV. Koordinace a řízení rizik kybernetické bezpečnosti České republiky.
V. Zvyšování povědomí a znalostí o kybernetické bezpečnosti.

Každá prioritní oblast Strategie obsahuje cíle a v rámci jednotlivých cílů jsou uvedena opatření, jejichž realizací budou naplňovány jednotlivé cíle. Každá prioritní oblast se také zaměřuje na řešení detekce, reakce a prevence kybernetických hrozeb České republiky.

Ze Strategie vychází Akční plán opatření ke Strategii pro oblast kybernetické bezpečnosti České republiky na období 2012 – 2015, který je rozčleněn do pěti oblastí. V každé oblasti jsou rozpracovány úkoly k naplňování jednotlivých strategických cílů Strategie do projektů a úkolů orgánů veřejné správy, které jsou věcně v jejich gesci.

Tento Akční plán bude aktualizován průběžně vyhodnocován na základě výsledků zprávy o stavu kybernetické bezpečnosti.

OBLAST I: VYTVOŘENÍ LEGISLATIVNÍHO RÁMCE K POSÍLENÍ KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY A PODPORA OCHRANY LIDSKÝCH PRÁV A SVOBOD

Poř. č.	Název cíle	Název úkolu	Realizace a výstupy	Kompetence	Termín
1.	Zákon o kybernetické bezpečnosti	Příprava zákona o kybernetické bezpečnosti.	Zákon o kybernetické bezpečnosti, prováděcí předpisy, novelizace jiných právních předpisů.	NBÚ, MV, ČTÚ, MO, BIS, MPO	Srpen 2013

OBLAST II: PODPORA MEZINÁRODNÍ SPOLUPRÁCE V OBLASTI KYBERNETICKÉ BEZPEČNOSTI

Poř. č.	Název cíle	Název úkolu	Realizace a výstupy	Kompetence	Termín
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.	NBÚ, zpravodajské služby, ostatní orgány veřejné správy	Od 2012 průběžně
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.	NBÚ	Od července 2012 průběžně
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.	NBÚ, MZV, ostatní orgány veřejné správy	Od 2012 průběžně
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.	NBÚ	Od 2012 průběžně

OBLAST III: NÁRODNÍ SPOLUPRÁCE V OBLASTI KYBERNETICKÉ BEZPEČNOSTI (STÁTNÍ, SOUKROMÉ A AKADEMICKÉ)

Poř. č.	Název cíle	Název úkolu	Realizace a výstupy	Kompetence	Termín
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	NBÚ	Od července 2012
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.	NBÚ	Od 2013 průběžně

OBLAST IV: KOORDINACE A ŘÍZENÍ RIZIK KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY

Poř. č.	Název cíle	Název úkolu	Realizace a výstupy	Kompetence	Termín
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.	NBÚ	Od července 2012 průběžně
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.	NBÚ	Od července 2012 průběžně
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.	NBÚ, ostatní orgány veřejné správy do úrovně kraje	Od července 2012 průběžně
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	Nastavení a zlepšování spolupráce a výměna zkušeností. Uzavírání smluv.	NBÚ	Od července 2012 průběžně

		problematikou kybernetické bezpečnosti			
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.	NBÚ	Od dubna 2013
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.	NBÚ, ostatní orgány veřejné správy do úrovně kraje	Od ledna 2013 průběžně
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.	NBÚ, MV, ostatní orgány veřejné správy do úrovně kraje	Od srpna 2012 průběžně

OBLAST V: ZVYŠOVÁNÍ ZNALOSTÍ A POVĚDOMÍ V OBLASTI KYBERNETICKÉ BEZPEČNOSTI

Poř. č.	Název cíle	Název úkolu	Realizace a výstupy	Kompetence	Termín
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.	NBÚ	Od července 2012 průběžně
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.	NBÚ, MŠMT, vysoké školy, poskytovatelé	Od července 2013
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.	NBÚ, MŠMT, vysoké školy	Od července 2013