AKČNÍ PLÁN

KE STRATEGII PRO OBLAST KYBERNETICKÉ BEZPEČNOSTI V ČR NA OBDOBÍ 2011 - 2015

OBSAH

ÚVOD

Vláda České republiky uložila svým usnesením č. 205 ze dne 15. března 2010 zpracovat Strategii pro oblast kybernetické bezpečnosti (dále Strategie). Cílem Strategie je formulovat strategické oblasti, priority a cíle kybernetické bezpečnosti, které je nutné zavést do praxe v období let 2011 - 2015. Strategie stanovuje tyto hlavní prioritní oblasti v budování kybernetické bezpečnosti v České republice, kterými jsou:

I. Koordinace a řízení rizik kybernetické bezpečnosti ČR.
II. Podpora mezinárodní spolupráce v oblasti kybernetické bezpečnosti ČR.
III. Národní spolupráce v oblasti kybernetické bezpečnosti (veřejné, soukromé a akademické).
IV. Vytvoření legislativního rámce k posílení kybernetické bezpečnosti ČR, podpora a ochrana lidských práv a svobod.
V. Zvyšování povědomí a znalostí o kybernetické bezpečnosti ČR.
VI. Posilování kybernetické bezpečnosti v ICT veřejné správy a komunikační infrastruktury ČR.
VII. Posilování odolnosti proti narušení ICT systémů a proti kybernetickým útokům.

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.

Akční plán je rozčleněn do sedmi oblastí. V každé 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 vždy v závěru roku na základě výsledků závěrečné zprávy pro oblast kybernetické bezpečnosti České republiky.

OBLAST I: KOORDINACE A ŘÍZENÍ RIZIK KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY

Poř. Č.	Název cíle	Název úkolu	Realizace a výstupy	Kompetence	Termín
1.	Alokace finančních zdrojů ke snížení dopadu kybernetickýc h hrozeb v ČR	Provedení analýz zaměřených na zajištění finančních zdrojů potřebných k plnění všech úkolů ve všech oblastech akčního plánu	Garantování odpovídajícího finančního rámce pro plnění úkolů k zajištění kybernetické bezpečnosti ČR v jednotlivých rozpočtových kapitolách rezortů.	MV, MF, MO	Prosinec 2011
2.	Organizační začlenění systému včasného varování a reakce na kybernetické útoky	Vybudovat vládní pracoviště pro koordinaci, řízení, monitoring a analýzu aktuálního stavu informačních a komunikačních systémů ČR.	Vybudování vládního pracoviště CERT s kompetencem i koordinovat činnost při stanovení prevence detekce a reakce na kybernetické útoky v ČR.	MV , MO	Leden 2012
3.	Realizace systému včasného varování a reakce na kybernetické útoky	Prostřednictvím CERT vytvořit 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 CERT s doporučením na eliminaci rizik.	MV, MO	Leden 2012

4.	Nepřetržité monitorování a analýza kybernetických hrozeb ČR	Provádět systémové a pravidelné monitorování hrozeb a analyzování současné situace v ČR i ve světě.	Zřízení národního registru bezpečnostních incidentů a jeho pravidelné vyhodnocování a aktualizace.	MV, orgány veřejné správy	Od ledna 2012 průběžně
5.	Alokace zdrojů ke snížení dopadu kybernetických útoků ČR	Alokovat finanční zdroje na reálné stanovení cílů a plánování procesů při výstavbě a provozu kybernetické obrany ČR v návaznosti na EU a NATO.	Garantování finančního rámce na výstavbu kybernetické obrany ČR. Získání finančních zdrojů z ESF a realizace projektů kybernetické obrany.	MF, MMR, MV, MO, orgány veřejné správy	Od 2012
6.	Alokace lidských zdrojů k eliminaci kybernetických hrozeb ČR a edukace subjektů OČTŘ v potírání kyberkriminality.	Zajistit podmínky pro další rozvoj (včetně materiálního a personálního posilování) struktur, přímo zapojených do potírání kybernetické kriminality.	Získání lidských a finančních zdrojů, tvorba koncepce dalšího vzdělávání	MV, MSPr , Policie ČR, BIS, MO	Od ledna 2012
7.	Stanovení cílů, kompetencí, rolí, odpovědnosti při výstavbě kybernetické obrany jako součásti kybernetické bezpečnosti ČR	Alokovat lidské zdroje na stanovení reálných cílů při výstavbě a provozu kybernetické obrany ČR v návaznosti na EU a NATO.	Alokace prostředků na financování lidských zdrojů z ESF a realizace výstavby projektů kybernetické obrany.	MF, MMR, MV, MO, orgány veřejné správy	Od srpna 2011

8.	Monitorování účinnosti navržených protiopatření	Alokace finančních zdrojů na stanovení reálných cílů a plánování procesů při výstavbě a provozu kybernetické bezpečnosti ČR v návaznosti na EU a NATO.	Alokace finančních zdrojů na experty a realizace cílů výstavby kybernetické bezpečnosti.	MF, MMR, MV, MO orgány veřejné správy	Od srpna 2012
9.	Zlepšení spolupráce při zabezpečení kybernetické bezpečnosti	Zavést monitorování účinnosti procesů zvládání bezpečnostních rizik a navržených protiopatření jako součást národního systému řízení bezpečnostních rizik včetně vyhodnocování účinnosti nasazovaných opatření.	Bude řešeno v rámci vládního pracoviště CERT s koordinační úlohou ve vztahu ke kritické infrastruktuře ČR.	MV, MO, orgány veřené správy, podnikatelský sektor	Leden 2012
10.	Ochrana kritické informační infrastruktury státu	Rozšiřovat a podporovat spolupráci policejních orgánů se zpravodajskými službami a nevládními neziskovými subjekty, zabývajícími se problematikou boje proti kybernetické kriminalitě	Zlepšování spolupráce a výměna zkušeností	MV, Policie ČR, zpravodajské služby, MO, nevládní organizace	Leden 2012

11.	Zlepšení spolupráce při zabezpečení kybernetické bezpečnosti	Vytvořit pro informační a komunikační systémy kritické infrastruktury státu potřebné postupy pro rychlý přechod z běžného do krizového stavu.	Zpracování krizových plánů jednotlivých systémů KI, realizace pravidelných vzdělávacích programů personálu, nácviky postupů při obnově služeb informačních systémů.	MV, MO, orgány veřejné správy	Od června 2012
12.	Zlepšení spolupráce při zabezpečení kybernetické bezpečnosti	Zlepšit součinnost mezi subjekty zodpovědnými za informační a komunikační systémy kritické infrastruktury státu a věcně příslušnými bezpečnostními složkami státu.	Zpracovat zásady a stanovit úroveň bezpečnosti systémů KI sjednocením a definováním práv a odpovědnosti. Optimalizace existujících právních a technických norem.	MV, Policie ČR, MO, MZV, orgány veřejné správy	Červen 2012

OBLAST II: PODPORA MEZINÁRODNÍ SPOLUPRÁCE V OBLASTI KYBERNETICKÉ BEZPEČNOSTI

Poř Č.	Název cíle	Název úkolu	Realizace a výstupy	Kompetence	Termín
13.	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.	MV, MO, zpravodajské služby, orgány veřejné správy	průběžně
14.	Realizace efektivní spolupráce a koordinace na národní i mezinárodní úrovni	Podporovat portál CERT jako jednotný informační prostředek pro zajištění efektivní komunikace v oblasti kybernetické bezpečnosti na národní i mezinárodní úrovni.	Zřízení pracovních skupin pro oblast kybernetické bezpečnosti ČR v rámci MKRPKB. Zveřejnění výstupů na portálu CERT jako platformy pro zajištění spolupráce s odbornou veřejností v oblasti kybernetické bezpečnosti.	MV,BIS, MO	2012
15.	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 (v rámci OECD, ISO, CERT, ENISA, ASEM, NATO a jiných mezinárodních organizací).	Zapojení expertů v oblasti legislativy, ICT a bezpečnosti jednotlivých resortů v oblasti kybernetické bezpečnosti do přípravy legislativy a norem v rámci EU, NATO.	MV, MZV, MO, orgány veřejné správy	Od 2011

16.	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 vládního pracoviště CERT ve spolupráci s dalšími pracovišti typu CSIRT.	MV, MO, MZV, podnikatelský sektor	2012

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

Poř. Č.	Název cíle	Název úkolu	Realizace a výstupy	Kompetence	Termín
17.	Výměna zkušeností	Prostřednictvím portálu CERT a dalších prostředků prezentovat nejlepší znalosti a praxi v oblasti kybernetické bezpečnosti.	Zveřejňování nejlepších znalostí a praxe při eliminaci kybernetických hrozeb (praktické dokumenty) na portálu CERT a jiných prostředcích	MV, Policie ČR, MO, BIS	Červen 2011
18.	Využívání nejlepší praxe při budování kybernetické bezpečnosti	Podporovat zavádění a efektivní správu systémů řízení kybernetické bezpečnosti.	Zavádění systému ISMS a norem řady BS ISO/IEC 270XX.	MV, UNMZ, orgány veřejné správy	Průběžně od 2013

OBLAST IV: VYTVOŘENÍ LEGISLATIVNÍHO RÁMCE K POSÍLENÍ KYBERNETICKÉ BEZPEČNOSTI ČR A PODPORA OCHRANY LIDSKÝCH PRÁV A SVOBOD

Poř. Č.	Název cíle	Název úkolu	Realizace a výstupy	Kompetence	Termín
19.	Vytvoření legislativního rámce na zvýšení kybernetické bezpečnosti ČR	Příprava věcného záměru zákona o kybernetické bezpečnosti ČR a příslušných prováděcích předpisů	Definovat pojmy v právním systému ČR, které jsou nutné pro zvýšení kybernetické bezpečnosti ČR, vymáhání práv a povinností v kyberprostoru ČR. Definovat práva a povinnosti uživatelů a poskytovatelů služeb kyberprostoru ČR v souladu s nařízeními a předpisy EU.	MV, MSPr, Policie ČR, ČTÚ, NBÚ, MO, BIS, MPO	Prosinec 2011
20.	Vytvoření legislativního rámce na zvýšení kybernetické bezpečnosti ČR	Analýza současného právního prostředí v oblasti kybernetické bezpečnosti ČR	Zpracování analýzy platného práva se zaměřením na bezpečnost a potírání kriminality v kyberprostoru při respektování a dodržování lidských práv a svobod	MV, Policie ČR, MSpr, ČTÚ, NBÚ, MO, MPO	Prosinec 2011
21.	Vytvoření zákona na zvýšení kybernetické bezpečnosti ČR	Příprava zákona na zvýšení kybernetické bezpečnosti.	Návrh novelizace právních norem ke zvýšení vymahatelnosti práva ČR týkající se kyberkriminality.	MV, Policie ČR, MSPr , ČTÚ, NBÚ, MO, MPO	Prosinec 2013

OBLAST V: ZVYŠOVÁNÍ ZNALOSTÍ A POVĚDOMÍ V OBLASTI KYBERNETICKÉ BEZPEČNOSTI ČR

Poř. Č.	Název cíle	Název úkolu	Realizace a výstupy	Kompetence	Termín
22.	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 CERT.	MV, MSPr, Policie ČR, BIS, MO	Od ledna 2012 průběžně
23.	Zvyšovat povědomí o kybernetické bezpečnosti, bezpečnostních rizicích a možnostech obrany u občanů, subjektů komerční a nekomerční sféry a orgánů veřejné správy.	Podporovat zvyšování povědomí jednotlivců školeními na téma kybernetické bezpečnosti.	Realizovat vzdělávací programy na téma kybernetické bezpečnosti podle role, kterou uživatelé, experti a řídící pracovníci plní, včetně orgánů činných v trestním řízení.	MV, MSpr, Policie ČR, BIS, MO	Od června 2012 průběžně
24.	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.	MV, MŠMT, MSpr	Leden 2012
25.	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.	MŠMT, MV, MSpr, MO, MPO	Od září 2012

OBLAST VI: POSILOVÁNÍ KYBERNETICKÉ BEZPEČNOSTI V ICT VEŘEJNÉ SPRÁVY A KOMUNIKAČNÍ INFRASTRUKTURY ČESKÉ REPUBLIKY

Poř. Č.	Název cíle	Název úkolu	Realizace a výstupy	Kompetence	Termín
26.	Zpracování analýzy rizik informačních a komunikačních systémů veřejné správy s návrhem na eliminaci rizik.	Vytvoření přehledu informačních a komunikačních systémů ČR. Provedení analýzy rizik poskytovaných služeb dodavatelů, kteří nejsou v majetku veřejné správy. Návrh opatření k eliminaci rizik.	Návrh komplexních opatření na eliminaci uvedených rizik.	MV, orgány veřejné správy	Od srpna 2011 průběžně
27.	Definování ochrany neutajovaných informací veřejné správy	Podpora k vytváření podzákonných norem k systematické kategorizaci informací neutajovaného charakteru a kategorizaci ICT ve veřejné správě, které zpracovávají neutajované informace neveřejného charakteru.	Vypracování předpisů a směrnic k ochraně důvěrných neutajovaných informací neveřejného charakteru a způsobu nakládání v informačních a komunikačních systémech veřejné správy.	MV, orgány veřejné správy	Od ledna 2012 průběžně
28.	Zavádění bezpečnostních norem a mezinárodních norem v oblasti ICT do veřejné správy	Podporovat zavádění a efektivní správu systémů řízení kybernetické bezpečnosti.	Zavádění systému ISMS a norem řady BS ISO/IEC 270XX atd.	MV, orgány veřejné správy	Od ledna 2012 průběžně

OBLAST VII: POSILOVÁNÍ ODOLNOSTI PROTI NARUŠENÍ ICT SYSTÉMŮ A PROTI KYBERNETICKÝM ÚTOKŮM ČR

Poř. Č.	Název cíle	Název úkolu	Realizace a výstupy	Kompetence	Termín
29.	Monitorování účinnosti navržených protiopatření	Zavést monitorování účinnosti procesů zvládání bezpečnostních rizik a navržených protiopatření.	Bude řešeno v rámci vládního pracoviště CERT.	MV, BIS, MO, MPO	Od ledna 2012
30.	Zajištění kybernetické bezpečnosti orgánů veřejné správy	Zajistit dohled kybernetické bezpečnosti v rámci komunikační a informační infrastruktury veřejné správy.	Zřízení vládního pracoviště CERT.	MV, BIS, MO	Od ledna 2012
31.	Ochrana kritické informační a komunikační infrastruktury státu	Vyžadovat zavádění nástrojů kybernetické bezpečnosti pro ochranu informačních a komunikačních systémů kritické infrastruktury státu.	Zavedení bezpečnostní správy vybraných systémů a sítí, provozní bezpečnostní dokumentace, kontroly zabezpečení jejich vzájemného koordinovaného řízení a výměna informací při zjištění bezpečnostních incidentů.	MV, orgány veřejné správy	Od ledna 2012
32.	Zavedení sy stému řízení bezpečnosti informací ve veřejné správě	Stanovit minimální rozsah úkolů k zajištění bezpečnosti infor mací ve veřejné správě v souladu s příslušnými normami ČSN ISO/IEC řady 27000 apod.	Návrh novelizace právních norem a zpracován í metodik a směrnic stanovujících povinnosti veřejné správě k zavedení ISMS včetně kontrolních mechanismů a sankcí.	MV, MPO, orgány veřejné správy	Od 2012

33.	Spolupráce při zabezpečení kybernetické obrany	Zlepšit součinnost mezi subjekty zodpovědnými za informační a komunikační systémy kritické infrastruktury státu a věcně příslušnými bezpečnostními složkami státu.	Zpracovat zásady a stanovit úroveň bezpečnosti systémů KI sjednocením a definováním práv a odpovědnosti. Optimalizace existujících právních a technických norem.	MV, Policie ČR, MO, BIS, MZV, orgány veřejné správy	Od ledna 2012 průběžně
34.	Zavedení plánu obnovy systému ICT ve veřejné správě	Zvýšit bezpečnost ICT a dat ve veřejné správě možností spolehlivé a rychlé obnovy funkčnosti systému, služeb a dat.	Zpracování metodik a směrnic nařizujících aplikaci plánů obnovy ICT ve veřejné správě, včetně ověření reálné funkčnosti.	orgány veřejné správy	Od června 2012
35.	Cvičení na národní a mezinárodní úrovni k testování účinnosti procesů zvládání bezpečnostních rizik	Provádění cvičení na národní a mezinárodní úrovni k nácviku testování účinnosti procesů zvládání bezpečnostních hrozeb a zavedení protiopatření prvků veřejné informační a komunikační infrastruktury.	Zpracování plánů a metodik k provádění cvičení na národní a mezinárodní úrovni k nácviku testování účinnosti procesů zvládání bezpečnostních rizik a zavedení protiopatření vybraných prvků veřejné informační a komunikační infrastruktury.	orgány veřejné správy	Leden 2012