III.

STRATEGIE PRO OBLAST KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY NA OBDOBÍ 2011 - 2015

Strategie pro oblast kybernetické bezpečnosti České republiky na období 2011-2015 navazuje na Bezpečnostní strategii České republiky a reflektuje výzvy moderní informační společnosti. Strategie je institucionálním rámcem, který dotváří bezpečnostní systém České republiky. Tento rámec je počátkem aktivní politiky kybernetické obrany státu, kterou je nutné neustále vyhodnocovat a dotvářet. Povědomí každého jednotlivce, provozovatele, správce, univerzity, podniku nebo firmy o bezpečnostních výzvách ICT, je základním předpokladem k zajištění spolehlivosti a bezpečnosti kyberprostoru. Česká republika vnímá problematiku kybernetické bezpečnosti jako důležitou součást každodenního využívání ICT a bude nadále realizovat opatření k jejímu zajištění.

Obsah

Úvod

Strategie pro oblast kybernetické bezpečnosti České republiky (dále ČR) na období 2011 – 2015 je připravována v souladu se směřováním Bezpečnostní strategie ČR. Definuje zájmy a záměry ČR v oblasti kybernetické bezpečnosti pro budování důvěryhodné informační společnosti na právních základech, která dbá na zabezpečení kybernetického přenosu a zpracování informací ve všech oblastech lidské činnosti a umožňuje informace svobodně a bezpečně sdílet a využívat.

Základními cíli politiky kybernetické bezpečnosti jsou ochrana před hrozbami, kterými jsou informační a komunikační systémy vystaveny, a snížení potenciálních škod v případě útoků na tyto informační a komunikační systémy (Information and Communication Technologies) dále ICT.

Tato Strategie je základním dokumentem při tvorbě politik, právních norem, směrnic, metodických pokynů, pravidel, zásad, příruček, provozních režimů, plánů, doporučení, apod.

Zavádění důvěryhodných informačních a komunikačních systémů, jejich bezpečný provoz a správa, je povinností ČR a odpovědností všech úrovní veřejné správy, soukromého sektoru a široké veřejnosti s cílem udržení bezpečného, odolného a důvěryhodného prostředí, které využívá příležitostí digitálního věku. Strategie se zaměřuje především na nerušenou dostupnost služeb, integritu dat a důvěrnost kybernetického prostoru ČR a je koordinována s ostatními souvisejícími strategiemi a koncepty.

I. Východiska

ICT významně ovlivňuje fungování vyspělé společnosti a ekonomiky

1. Bezpečné a spolehlivé fungování ICT je nezbytné pro fungování státních i veřejných struktur a je jedním ze základních předpokladů prosperity a trvalého ekonomického růstu. Neustále roste podíl lidských činností a produkce přímo či nepřímo závislé na fungování ICT. ČR má ambice patřit v tomto směru mezi vyspělé země. Online služby a sítě musí být nejen bezpečné a odolné, ale také spolehlivé. Celá společnost musí zvyšovat svoje aktivity zaměřené na oblast bezpečnosti a spolehlivosti ICT.

ICT a společnosti na nich závislé jsou zranitelné

2. Nepřetržitý a rychlý pokrok v oblasti ICT přináší stále nové příležitosti pro společnost, ale spolu s tím i nové bezpečnostní výzvy. Kombinace rostoucí závislosti na ICT, s možnou technickou chybou či selháním lidského faktoru nebo úmyslným poškozením ICT, komplikuje minimalizaci následků v případě prolomení slabin celého systému ICT. Nástup nových technologií generuje nové příležitosti pro rozvoj společnosti, ale také nová zadání pro zajištění bezpečnost ICT a tím i celé společnosti.

3. Rostoucí závislost na informačních a komunikačních technologiích zvyšuje zranitelnost státu a jeho občanů vůči kybernetickým útokům. Tyto útoky mohou představovat nový způsob vedení války nebo mohou mít kriminální, ekonomickou či teroristickou motivaci a mohou být použity k destabilizaci společnosti. Úniky strategicky důležitých informací, zásahy do ICT státních institucí či strategických podniků a společností, které zajišťují základní funkce státu, mohou ohrozit strategické zájmy ČR. Příklady ukazují, jak rychlý a různorodý je vývoj v oblasti kybernetické bezpečnosti. Útoky proti ICT strukturám jsou stále sofistikovanější a komplexnější. Tyto útoky jsou již vedeny různými metodami a proti různým cílům. Mění se také povaha a motivy útočníků. Stále častěji se terčem dobře organizovaných útoků stávají prvky kritické infrastruktury (dále jen KI), které jsou životně důležité pro fungování státu. S prorůstáním ICT do řady důležitých oblastí běžného života se kritickou infrastrukturou stává sama ICT.

II. Základní principy

4. Problematiku kybernetické bezpečnosti nelze vnímat jako izolovaný problém ČR nebo izolovaný problém jedné nebo několika částí naší společnosti. Je to problém nejen mezinárodní, meziresortní, problém veřejné i privátní sféry, ale problém celé společnosti. Proto si zajištění kybernetické bezpečnosti zaslouží vysokou prioritu.

Propojení a posílení spolupráce všech sektorů společnosti

5. Je žádoucí propojení všech iniciativ, ať už státních (civilních, policejních i vojenských), komerčních a akademických, které již ve svých sektorech vykonaly mnoho užitečné práce v oblasti kybernetické bezpečnosti. Toto spojené úsilí vedlo k posílení kybernetické bezpečnosti tak, aby nedocházelo k tříštění sil a mnohdy zbytečnému dublování. ICT infrastruktura, výrobky a služby jsou z velké části zajišťovány soukromým sektorem. Vzájemná důvěra a sdílení informací jsou základním předpokladem pro úspěšnou spolupráci mezi veřejným a soukromým sektorem.

Individuální zodpovědnost

6. Je zájmem státu stanovit pravidla pro bezpečnost ICT a musí být cílem, aby každý občan, podnik, organizace či instituce, přijali odpovědnost za bezpečnost systémů, které vlastní a provozují. Všichni provozovatelé a správci (ale také občané, společnosti, instituce) musejí přijímat vhodná opatření pro zajištění bezpečnosti a spolehlivosti vlastních ICT systémů a sítí.

Odpovědnost podnikatelského sektoru

7. Je v zájmu státu a podnikatelského sektoru definovat minimální standardy kybernetické bezpečnosti a vyžadovat jejich zavedení do praxe a jejich důsledné dodržování.

Resortní spolupráce

8. Gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou v této oblasti je podle Usnesení vlády č. 205 ze dne 15. března 2010 Ministerstvo vnitra ČR. Důležitou roli ve spolupráci mezi resorty zaujímá Meziresortní koordinační rada pro kybernetickou bezpečnost (dále MKRPKB), která bude i nadále iniciovat součinnost státních institucí. V souladu se statutem bude MKRPKB zřizovat pracovní skupiny složené z věcně příslušných odborníků, a tyto pracovní skupiny

budou společně diskutovat problematiku kybernetické bezpečnosti, týkající se nejen veřejného sektoru, ale také např. z oblastí bankovního sektoru, dodávek energií atd.

Mezinárodní spolupráce

9. ČR se zapojí do mezinárodní spolupráce v oblasti kybernetické a informační bezpečnosti. Bude se podílet v rámci Evropské unie (dále EU) a Severoatlantické aliance (dále NATO) na tvorbě norem a mezinárodních politik, doporučení a předpisů, eventuálně na činnosti společných institucí, a současně adekvátně aplikovat tyto standardy a mechanismy do vnitrostátní legislativy členských států souvisejících s kybernetickou bezpečností. Při naplňování těchto požadavků bude ČR dodržovat principy demokratické společnosti a zohledňovat oprávněné zájmy občanů, podnikatelské sféry a veřejné správy ve vztahu k občanům.

Přiměřenost přijatých opatření

10. Pro zajištění kybernetické bezpečnosti ČR přijme vláda (na základě analýzy rizik i relevantních mezinárodních doporučení) vyplývající nezbytná opatření. Tato opatření budou respektovat ochranu soukromí, základní práva, svobodný přístup k informacím a další demokratické principy. Bude dbát na přiměřenost přijatých opatření vzhledem k nutnosti zajistit bezpečnost na jedné straně a respektování základních práv a svobod na straně druhé.

III. Strategické cíle a opatření

Vytvoření legislativního rámce

11. Legislativní úprava vymezí činnosti příslušného orgánu při koordinaci postupu veřejné moci v oblasti kybernetické bezpečnosti, povinnosti pro subjekty vytvářející či využívající ICT služby, a také vymezí formy (způsoby) a rámce (rozsahy) spolupráce se soukromým sektorem a s veřejností.

12. ČR vytvoří odpovídající legislativní rámec pro zajištění kybernetické bezpečnosti, který nebude omezovat Ústavou zaručená práva na svobodu projevu, přístup k informacím pro všechny skupiny obyvatel, ochranu soukromí a důvěrnost informací v souladu s mezinárodními závazky ČR (zejména vůči EU a NATO).

13. ČR bude pravidelně vyhodnocovat mezinárodní legislativu, smlouvy, trendy a doporučení v oblasti kybernetické a informační bezpečnosti, elektronického obchodu a elektronických transakcí a z vyhodnocení bude vyvozovat závěry a aplikovat odpovídající doporučení do českého prostředí. ČR se bude aktivně účastnit přípravy legislativy, norem a další spolupráce týkající se kybernetické bezpečnosti v rámci EU a dalších mezinárodních organizací.

14. ČR bude zdokonalovat legislativní a procedurální kroky tak, aby oblast kybernetické bezpečnosti zahrnovala prevenci, detekci, reakci a opatření, vedoucí nejen k odhalování, ale také k potírání kybernetické kriminality.

Posilování kybernetické bezpečnosti v ICT veřejné správy a KI

15. Zavádění bezpečnostních norem v informačních systémech veřejné správy a prvcích KI je jedním z předpokladů pro posílení kybernetické bezpečnosti informačních systémů. Efektivní kybernetická bezpečnost vyžaduje povinnou implementaci a důsledné dodržování těchto bezpečnostních norem s důslednou a periodickou kontrolou jejich dodržování ve všech orgánech veřejné správy a subjektech zahrnutých do KI státu. Celá řada prvků KI není v majetku státu, proto je nutná důsledná analýza rizik z toho plynoucích i ve vztahu k ICT a zákonné stanovení závazných pravidel pro tyto systémy, zejména KI.

16. Budou průběžně zpracovávány metodické materiály pro definování požadované základní úrovně kybernetické bezpečnosti (směrnice a doporučené postupy). ČR bude podporovat a prosazovat konvergenci používaných bezpečnostních procedur založených na doporučených postupech ve státním i soukromém sektoru. Zlepšování úrovně informační bezpečnosti ve státních institucích je realizováno mimo jiné zaváděním systému řízení informační bezpečnosti – ISMS.

17. ČR vytvoří nové metodiky a definuje způsoby nakládání a ochrany neutajovaných důvěrných informací (jejichž ochrana není předmětem zákona o utajovaných informacích), s nimiž je nakládáno v informačních systémech provozovaných a používaných orgány veřejné správy, a především těch informačních

systémů, které jsou nezbytné k zajištění chodu KI státu. ČR také definuje jednotné metodiky pro kategorizaci informací a kategorizaci informačních a komunikačních systémů.

Vybudování vládního pracoviště CERT

18. V souvislosti s hrozbou narušení ICT patří k prioritám vlády zajištění bezpečnosti a spolehlivosti informačních a komunikačních systémů zapojených do KI pomocí vládního koordinačního místa pro okamžitou reakci na počítačové incidenty Computer Emergency Response Team (dále CERT). Toto pracoviště bude součástí národního a mezinárodního systému včasného varování o kybernetických hrozbách. ČR bude upřednostňovat a prosazovat budování systémů schopných nejen minimalizovat dopady kybernetického útoku, ale také uvést systém rychle zpět do funkčního stavu.

19. Vládní pracoviště CERT bude optimalizovat možnosti identifikace, koordinace a nápravných opatření při potenciálních kybernetických útocích. Toto centrum bude ve spolupráci s ostatními relevantními složkami státu koordinovat a navrhovat preventivní opatření pro odvrácení případného útoku na informační a komunikační systémy státu a na systémy KI státu. Pracoviště bude dále provádět identifikaci, zaznamenávání a vyhodnocování bezpečnostních incidentů. Vládní pracoviště CERT bude spolupracovat s pracovištěm národním a ostatními pracovišti podobného zaměření z veřejné, komerční i akademické sféry a bude jim poskytovat metodickou podporu při řešení bezpečnostních incidentů.

20. ČR vytvoří národní systém včasného varování před kybernetickými hrozbami, reakce a výměny informací ke snížení rizik plynoucích z hrozeb pro prvky informačních a komunikačních systémů a zapojí jej do mezinárodního systému včasného varování před kybernetickými hrozbami. Trvale bude zkvalitňována vzájemná komunikace bezpečnostních složek zajišťujících obranu proti útokům na informační a komunikační systémy KI.

21. ČR prosadí zavedení a pravidelnou aktualizaci plánů pro řešení provozních a bezpečnostních incidentů v oblasti kybernetické bezpečnosti a následnou obnovu ve všech informačních systémech veřejné správy a KI.

22. ČR zavede monitorování a testování účinnosti procesů zvládání bezpečnostních rizik a navržených protiopatření jako součást systému řízení bezpečnostních rizik. Pravidelně se budou tyto schopnosti prověřovat cvičením kybernetické obrany na národní i mezinárodní úrovni.

Mezinárodní spolupráce

23. Koordinovaná mezinárodní spolupráce je základním předpokladem globálního rozměru a srovnatelné úrovně bezpečnosti v kybernetickém prostoru.

24. ČR se aktivně podílí a bude podílet na rozvoji opatření proti kybernetickým hrozbám a spolupráce v rámci mezinárodních organizací, zejména

EU, NATO a dalších. ČR se také zapojuje a bude zapojovat do intenzivní mezinárodní výměny informací a zkušeností, zastoupením v relevantních mezinárodních institucích.

25. ČR podporuje a bude podporovat posílení mezinárodní soudní a policejní spolupráce s cílem dopadení pachatelů kybernetických útoků.

26. ČR by se měla připojit k účinným a perspektivním iniciativám prosazujícím tvorbu mezinárodních právních norem upravujících problematiku kybernetické a informační bezpečnosti.

Spolupráce státu, soukromé a akademické sféry

27. Dynamika rozvoje ICT vyžaduje neustálou spolupráci mezi veřejnou, komerční a akademickou sférou. Bez této spolupráce nelze zajistit posilování kybernetické bezpečnosti ČR, nelze minimalizovat škody způsobené narušením této bezpečnosti a stejně tak nelze zajistit rychlou obnovu funkčnosti ICT systémů. Důležitým prvkem této spolupráce je oficiální platforma pro sdílení informací a zkušeností z oblasti kybernetické bezpečnosti.

28. ČR podpoří spolupráci na projektech pro výměnu informací a nejlepší praxe pro oblast kybernetické bezpečnosti mezi veřejnou správou a soukromou a akademickou sférou v národním i mezinárodním měřítku.

29. ČR podporuje výzkum a vývoj zaměřený na perspektivní a aktuální problémy kybernetické bezpečnosti (zejména zintenzívnění spolupráce státu, soukromé sféry a akademického prostředí).

30. ČR využívá výsledků mezinárodní spolupráce jako zpřístupňování informací o problémech, řešeních, trendech, legislativě, standardech a mezinárodních iniciativách v oblasti informační bezpečnosti.

Zvyšování povědomí o kybernetické bezpečnosti

31. Informace o bezpečnostních výzvách ICT jsou veřejně publikovány, přesto je nutné zvyšovat povědomí o bezpečnosti kyberprostoru na straně koncových uživatelů, správců systémů, vývojových pracovníků, zadavatelů veřejných zakázek, úředníků, auditorů a vedoucích pracovníků. Nedostatečná informovanost o zabezpečení ICT systémů představuje vážná rizika pro KI i v případě, kdy nejsou součástí samotné KI. Nedostatek školeného a informovaného personálu, absence průběžného vzdělávání a systému certifikace pracovníků zvyšují zranitelnost a zvětšují způsobené škody.

32. ČR bude zvyšovat povědomí občanů o kybernetické a informační bezpečnosti šířením relevantních informací ve spolupráci se sdělovacími prostředky. Bude zvyšovat povědomí o důležitosti bezpečnostní certifikace výrobků a služeb

v oblasti ICT. Vybuduje platformu pro zajištění efektivní komunikace v oblasti kybernetické bezpečnosti.

33. ČR zahrne kybernetickou bezpečnost do vzdělávacích programů zaměstnanců veřejné správy a bude prosazovat toto vzdělávání i v soukromé sféře. Cílem je dosažení cílové úrovně znalostí pro jednotlivé role v oblasti kybernetické i informační bezpečnosti.

34. ČR bude metodicky spolupracovat se soukromým sektorem při zavádění školicích programů, zaměřených na kybernetickou a informační bezpečnost.

35. ČR bude průběžně analyzovat kvalifikační potřeby uživatelů ICT v ČR v oblasti kybernetické a informační bezpečnosti, možnosti školního a mimoškolního vzdělávání a zavede problematiku kybernetické a informační bezpečnosti do metodiky všech úrovní vzdělávání.