STRATEGIE PRO OBLAST KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY NA OBDOBÍ 2012 - 2015

Obsah

Úvod

Strategie pro oblast kybernetické bezpečnosti České republiky na období 2012 - 2015 (dále jen „Strategie“) je jedním z kroků vlády České republiky v reakci na celosvětový nárůst kybernetických hrozeb. Strategie vychází z úsilí vládních i nevládních institucí ke zvyšování kybernetické bezpečnosti. Přichází s iniciativami, které zlepší kybernetickou bezpečnost pro vládní instituce, kritickou infrastrukturu i pro komerční sféru, potažmo i pro občany.

Strategie definuje zájmy a záměry České republiky v oblasti kybernetické bezpečnosti pro budování důvěryhodné informační společnosti a je v souladu s Bezpečnostní strategií České republiky.

Tato Strategie je základním dokumentem pro tvorbu právních předpisů, bezpečnostních politik informačních a komunikačních systémů, standardů, směrnic, metodických pokynů, pravidel, provozních režimů, plánů obnovy, doporučení a dalších nástrojů užívaných k zajištění kybernetické bezpečnosti.

Strategie je členěna 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.

I. Východiska

V posledních letech jsou útoky na kritickou informační infrastrukturu stále častější, komplexnější a sofistikovanější, pachatelé jsou mnohem profesionálnější. Možnosti včasné reakce na takové útoky a zjišťování pachatelů jsou velmi omezené a náročné. Trend vývoje informačních systémů pro průmyslové využití připojených do kybernetického prostoru, vedený ekonomickými důvody, má za následek nové zranitelnosti těchto systémů. Zkušenosti s virem Stuxnet ukazují, že důležité průmyslové infrastruktury nejsou před kybernetickými útoky imunní. Kybernetická bezpečnost zůstane i v budoucnu klíčovou pro zachování funkčnosti státu.

Informační a komunikační technologie významně ovlivňují fungování vyspělé společnosti a ekonomiky

Bezpečné a spolehlivé fungování Informačních a komunikačních technologií (dále jen „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. Česká republika má ambice patřit v tomto směru mezi vyspělé země. Sítě a online služby 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

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, například s možnou technickou chybou, selháním lidského faktoru nebo úmyslným poškozením, komplikuje minimalizaci následků v případě prolomení slabin celého systému. Nástup nových technologií generuje nové příležitosti pro rozvoj společnosti, ale také přináší nové zranitelnosti a tím i nová zadání pro zajištění bezpečnost ICT i celé společnosti.

Rostoucí závislost na ICT zvyšuje zranitelnost státu a jeho občanů vůči kybernetickým útokům. Tyto útoky 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 zájmy České republiky. Příklady ukazují, jak rychlý a různorodý je vývoj v oblasti kybernetické bezpečnosti. Útoky proti ICT strukturám jsou stále sofistikovanější a komplexnější. Tyto útoky jsou 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, které jsou životně důležité pro fungování státu.

Vzhledem k tomu, že digitální společnost je globalizovaná a kybernetické útoky překračují státní, kulturní a legislativní hranice, často není zřejmé, jakou

jurisdikci lze na takové činy aplikovat. I v oblasti legislativy je proto třeba úzká mezinárodní spolupráce.

II. Základní principy strategie kybernetické bezpečnosti

Investování do kybernetické bezpečnosti znamená investice do naší budoucnosti, našeho ekonomického růstu. Úroveň kybernetické bezpečnosti je souhrnem všech opatření, jak národních tak mezinárodních, přijatých k ochraně dostupnosti informací komunikačních technologií a integrity, autenticity a důvěrnosti dat v kybernetickém prostoru. Kybernetická bezpečnost musí být založena na komplexním přístupu, což vyžaduje intenzivní sdílení informací a koordinaci aktivit. Při budování kybernetické bezpečnosti je třeba prosazovat spolupráci mezi civilními a ozbrojenými složkami, veřejným a privátním sektorem a mezi národními a mezinárodními institucemi. Pouze takovým způsobem lze zajistit spolehlivý provoz informačních a komunikačních infrastruktur v kritických sektorech, rychlé a efektivní reakce na kybernetické útoky a odpovídající legislativní ochranu v digitálním světě. Problematiku kybernetické bezpečnosti nelze vnímat jako izolovaný problém České republiky nebo izolovaný problém jedné nebo několika částí naší společnosti. Je to problém nejen mezinárodní, meziresortní, veřejné nebo privátní sféry, ale problém celé společnosti. Proto si zajištění kybernetické bezpečnosti zaslouží vysokou prioritu.

Propojení a posílení spolupráce všech sektorů společnosti

Je žádoucí koordinovat všechny iniciativy, ať už státních (civilních, policejních i vojenských), komerčních a akademických subjektů, jak těch které již ve svých sektorech vykonaly mnoho užitečné práce v oblasti kybernetické bezpečnosti, tak těch které zatím v této oblasti nebyly příliš aktivní. Pouze spojené úsilí povede k posílení kybernetické bezpečnosti a nebude docházet ke tříštění sil a mnohdy zbytečnému dublování činností a zvyšování nákladů. ICT infrastruktura, výrobky a služby jsou z velké části zajišťovány soukromým sektorem. Vzájemná důvěra a sdílení informací jsou základním předpokladem pro úspěšnou vzájemnou spolupráci mezi veřejným a soukromým sektorem.

Individuální zodpovědnost

Je zájmem státu, aby stanovil pravidla pro bezpečnost ICT tak, aby všichni uživatelé kybernetického prostoru (státní instituce, subjekty kritické infrastruktury, veřejné instituce, komerční podniky i občané) a poskytovatelé služeb přijali ve svých informačních a komunikačních systémech přiměřená opatření k tomu, aby systém byl odolný proti vnějším i vnitřním útokům a aby nebyl potenciálním rizikem pro ostatní systémy.

Resortní spolupráce

Gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou v této oblasti je podle usnesení vlády České republiky ze dne 19. října 2011 č. 781 Národní bezpečnostní úřad (dále jen „NBÚ). Důležitou roli ve spolupráci mezi resorty zaujímá Rada pro kybernetickou bezpečnost (dále jen „Rada“), která bude, kromě jiného, iniciovat součinnost státních institucí. V souladu se statutem bude Rada zřizovat pracovní skupiny složené z věcně příslušných odborníků. Tyto pracovní skupiny budou připravovat materiály pro Radu týkající se specifických problematik kybernetické bezpečnosti.

Mezinárodní spolupráce

Vzhledem k tomu, že mnoho opatření může být efektivní, pouze když je jejich aplikace přijata nebo koordinována na mezinárodní úrovni, bude se Česká republika aktivně podílet a podporovat úsilí Evropské unie (dále jen „EU“) a Severoatlantické aliance (dále jen „NATO“) na tvorbě mezinárodních politik, standardů a předpisů, eventuálně na činnosti společných institucí a pracovních orgánů, a současně adekvátně aplikovat tyto politiky, standardy a předpisy do vnitrostátní legislativy související s kybernetickou bezpečností.

Přiměřenost přijatých opatření

Při zajištění kybernetické bezpečnosti nelze dosáhnout absolutní bezpečnosti. V České republice budou přijímána taková opatření, která budou založená na realistickém ohodnocení rizik a budou adekvátní těmto rizikům. Tato opatření budou respektovat ochranu soukromí a základní práva, jako je svobodný přístup k informacím, svoboda vyjadřování a další. Bude zajištěna 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

Strategie přijímá opatření proti současným hrozbám a vychází z ní Akční plán, který definuje konkrétní úkoly a určuje jejich řešitele. Prioritně budou řešeny následující strategické oblasti:

Vytvoření legislativního rámce

NBÚ připraví specializovaný zákon o kybernetické bezpečnosti, který vymezí činnosti a odpovědnosti Národního centra kybernetické bezpečnosti (dále jen „NCKB“). Zákon definuje povinnosti pro subjekty vytvářející či využívající služby ICT v kybernetickém prostoru. Dále vymezí formy (způsoby) a rámce (rozsahy) spolupráce se soukromým sektorem, s veřejností a s mezinárodními institucemi.

Pravidelně bude vyhodnocována mezinárodní legislativa, smlouvy, trendy a doporučení v oblasti kybernetické a informační bezpečnosti, elektronického obchodu a elektronických transakcí a z vyhodnocení budou vyvozovány závěry a doporučení,

které budou zaváděny do praxe. Česká republika se bude aktivně účastnit přípravy legislativy, norem a další spolupráce týkající se kybernetické bezpečnosti v rámci EU, NATO a dalších mezinárodních organizací.

Vybudování Národního centra kybernetické bezpečnosti a vládního pracoviště CERT

K optimalizaci spolupráce mezi státními orgány a ke zlepšení koordinace ochrany a implementaci protiopatření při kybernetických bezpečnostních událostech bude v rámci NBÚ zřízeno NCKB. Součástí NCKB bude vládní pracoviště CERT (Computer Emergency Response Team). NCKB bude v oblasti kybernetické bezpečnosti úzce spolupracovat s ostatními státními orgány, akademickými pracovišti a komerčními subjekty na základě smluv o spolupráci. Rychlé a efektivní sdílení informací o slabinách a zranitelnostech prostředků ICT, formách kybernetických útoků, profilech a motivacích pachatelů umožní NCKB analyzovat bezpečnostní incidenty a připravovat doporučení k opatřením. Spolupráce s NCKB je v zájmu i privátního sektoru při ochraně vlastních informačních a komunikačních systémů proti napadení prostřednictvím kybernetických útoků. Vzhledem k tomu, že bezpečnost se nejlépe zajistí včasnou přípravou a prevencí, vybuduje NCKB systém včasného varování před kybernetickými útoky a bude poskytovat doporučení k ochraně před kybernetickými útoky.

NCKB bude prosazovat zavedení systému testování účinnosti procesů zvládání bezpečnostních rizik a navržených protiopatření jako součást systému řízení bezpečnostních rizik. Pravidelně se budou tyto schopnosti prověřovat cvičeními kybernetické obrany na národní i mezinárodní úrovni.

Ochrana kritických informačních infrastruktur

Ochrana kritických informačních infrastruktur je jednou z hlavních priorit kybernetické bezpečnosti. Tyto infrastruktury jsou ústřední součástí téměř všech kritických infrastruktur a stávají se stále důležitějšími. Jak soukromý, tak veřejný sektor musí vytvářet podmínky pro užší koordinaci a spolupráci založenou na sdílení informací. Bude pečlivě zvažováno, zda a kde budou bezpečnostní opatření vyžadována povinně a zda a kde budou přijímány dodatečné pravomoci v případě specifických hrozeb a útoků.

Posilování kybernetické bezpečnosti informačních a komunikačních systémů veřejné správy

Uživatelé informačních a komunikačních systémů potřebují při jejich používání přiměřené a konzistentní informace o relevantních rizicích a o tom, jak lze bezpečným způsobem využívat kybernetický prostor. NCKB bude takové informace

publikovat na portálu GovCERT.cz. Zde budou rovněž poskytovány informace o dostupných bezpečnostních produktech a službách.

Zavádění bezpečnostních norem a standardů v informačních systémech, jejichž bezpečný provoz je pro chod státu nezbytně důležitý, je jedním z předpokladů pro posílení kybernetické bezpečnosti těchto systémů. Efektivní kybernetická bezpečnost vyžaduje povinnou implementaci a důsledné dodržování těchto bezpečnostních norem a standardů s důslednou a periodickou kontrolou jejich dodržování v orgánech veřejné správy.

Průběžně budou zpracovávány metodické materiály pro dosažení požadované minimální úrovně kybernetické bezpečnosti (směrnice a doporučené postupy). Zlepšování úrovně informační bezpečnosti ve státních institucích bude realizováno mimo jiné zaváděním systému řízení informační bezpečnosti – ISMS (Information Security Management System).

Zefektivnění potírání kriminality v kybernetickém prostoru

NCKB bude přispívat k boji s kybernetickou kriminalitou spoluprací s orgány činnými v trestním řízení a při vývoji prostředků a opatření proti kybernetickým útokům bude využívat jejich zkušeností.

Koordinace aktivit k zajištění kybernetické bezpečnosti v Evropě

Bezpečnosti v globálním kybernetickém prostoru lze dosáhnout pouze při koordinaci opatření na národní a mezinárodní úrovni.

Na úrovni EU bude NBÚ podporovat přiměřená opatření založená na evropském Akčním plánu pro ochranu kritických informačních infrastruktur. Dále bude probíhat spolupráce s European Network and Information Security Agency (ENISA) v oblasti cvičení, školení a sdílení informací. Náměty pro budoucí aktivity lze spatřovat v „EU Internal Security Strategy“ a v „Digital Agenda for Europe“ stejně jako v nové „NATO Policy on Cyber Defence“. Rovněž bude navázána spolupráce s nově vzniklou Evropskou agenturou pro provozní řízení rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva a s centrem EU pro počítačovou kriminalitu v oblastech, které bude NBÚ zastřešovat.

Používání spolehlivých a důvěryhodných informačních technologií

Pro uživatele ve veřejné správě musí být zajištěna dostupnost spolehlivých systémů ICT. Bude podporován výzkum a vývoj prostředků pro ochranu informačních a komunikačních systémů veřejné správy a prvků kritické infrastruktury. Bude usilováno, aby v oblastech kritických pro bezpečnost státu byly prioritně používány

technické a programové prostředky hodnocené podle mezinárodních bezpečnostních standardů.

Zvyšování povědomí o kybernetické bezpečnosti

Při budování kybernetické bezpečnosti nelze spoléhat jen na technické prostředky, ale nezbytnou péči je třeba věnovat koncovým uživatelům, správcům a administrátorům informačních a komunikačních systémů, vývojovým pracovníkům, zadavatelům veřejných zakázek, auditorům a vedoucím pracovníkům. Nedostatečná informovanost o zabezpečení informačních a komunikačních systémů představuje vážná rizika. Nedostatek školeného a informovaného personálu a absence dalšího průběžného vzdělávání pracovníků zvyšují zranitelnost a zvětšují způsobené škody.

Povědomí občanů o kybernetické bezpečnosti se bude zvyšovat šířením relevantních informací ve spolupráci se sdělovacími prostředky. Témata kybernetické bezpečnosti budou zahrnuta do vzdělávacích programů zaměstnanců veřejné správy a toto vzdělávání bude prosazováno i v soukromé sféře. Cílem je dosažení dostatečné úrovně znalostí pro jednotlivé zaměstnanecké role v oblasti kybernetické bezpečnosti.

Se soukromým a akademickým sektorem bude probíhat metodická spolupráce při zavádění školících programů zaměřených na kybernetickou bezpečnost. Průběžně budou analyzovány kvalifikační potřeby v oblasti kybernetické bezpečnosti, možnosti školního a mimoškolního vzdělávání a problematika kybernetické bezpečnosti se postupně zavede do náplně všech úrovní vzdělávání.

Odezva na kybernetické útoky

Vzhledem k tomu, že nelze vyloučit kybernetické útoky proti systémům veřejné správy a subjektům kritické infrastruktury, musí být stát na tyto útoky dostatečně připraven. Komplexní a koordinovaný soubor opatření, které budou v případě kybernetického útoky aplikovány, musí být vytvořen ve spolupráci se všemi kompetentními státními institucemi. Při přípravě těchto opatření bude zvažována jejich přiměřenost a nezbytnost.

Strategie pro oblast kybernetické bezpečnosti České republiky na období 2012-2015 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 ochrany státu, kterou je nutné neustále vyhodnocovat a dotvářet. Povědomí každého jednotlivce, provozovatele, správce, univerzity nebo firmy o bezpečnostních výzvách ICT, je základním předpokladem k zajištění spolehlivosti a bezpečnosti kybernetického prostoru. Česká republika vnímá problematiku kybernetické bezpečnosti jako důležitou součást každodenního využívání ICT a bude nadále realizovat opatření k jejímu zajištění.