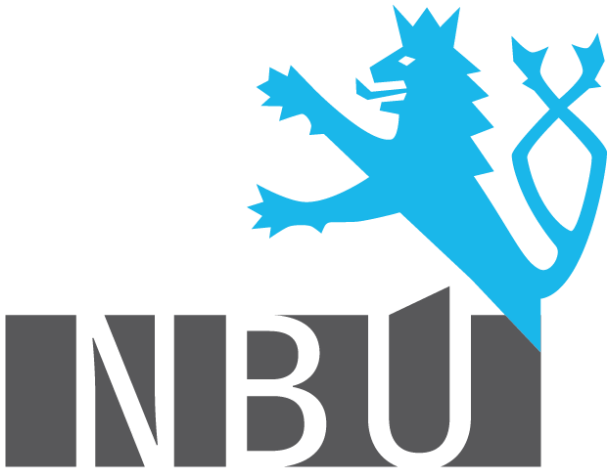

Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020

Úvodní slovo

Stále více a více lidských činností a aktivit se přesouvá z fyzického prostředí do kyberprostoru. V průběhu posledních desetiletí změnily informační a komunikační technologie téměř každý aspekt našeho života, když značnou měrou ulehčily komunikaci či sdílení a přístup k informacím a službám. Na druhou stranu však tento fenomén činí společnost zranitelnější a kybernetická bezpečnost se tak stává jednou z nejvýznamnějších výzev dnešní doby, na kterou musí stát reagovat.

V České republice působí Národní bezpečnostní úřad již od roku 2011 jako gestor a národní autorita pro oblast kybernetické bezpečnosti. Za tuto dobu se nám podařilo dosáhnout mimo jiné i dvou důležitých milníků, které jsme si stanovili v předešlé Strategii pro oblast kybernetické bezpečnosti České republiky na období 2012 – 2015. Prvním z nich bylo přijetí Zákona o kybernetické bezpečnosti a druhým se stalo květnové otevření Národního centra kybernetické bezpečnosti, jehož součástí je i plně funkční vládní CERT pro zvládání kybernetických bezpečnostních incidentů. Co se týče ostatních cílů stanovených předchozí strategií, ty lze také považovat za splněné, či průběžně naplňované. Česká republika se již pravidelně účastní mnoha mezinárodních cvičení kybernetické bezpečnosti, úspěšně započala mapování kritické informační infrastruktury a významných informačních systémů a spolupráce se subjekty jak na národní, tak na mezinárodní úrovni je již nyní na velmi dobré úrovni. Lze tedy konstatovat, že předešlá strategie byla zdárně zrealizována a v České republice byla od roku 2012 znatelně navýšena úroveň kybernetické bezpečnosti. S blížícím se ukončením platnosti strategie a splněním všech zásadních cílů a úkolů začal Národní bezpečnostní úřad pracovat na vytvoření zcela nové „Národní strategie kybernetické bezpečnosti na období let 2015 až 2020“, která představuje pro Českou republiku zásadní předěl ve vnímání kybernetické bezpečnosti. Oproti minulé strategii se tak kvalitativně přesouváme od budování základních kapacit nezbytných pro zajištění

elementární míry kybernetické bezpečnosti směrem k jejímu dalšímu hlubšímu a pokročilému zajišťování.

Zveřejněním této nové národní strategie jsou stanoveny vize a priority České republiky v oblasti zajišťování kybernetické bezpečnosti v zemi. Česká republika bude v nadcházejících letech čelit mnoha kybernetickým bezpečnostním hrozbám a rizikům a naše sítě a systémy musí být za všech okolností vždy stabilní a bezpečné. Strategie proto určuje jak tohoto stavu dosáhnout, a jakým způsobem a nástroji se bude Česká republika snažit redukovat rizika a zmírňovat hrozby plynoucí z kyberprostoru, aniž by jakkoliv omezovala výhody jeho využívání.

Kybernetické bezpečnosti však nelze dosáhnout bez hluboké důvěry a spolupráce mezi veřejným sektorem a zbytkem společnosti. Národní bezpečnostní úřad se stal národní koordinační autoritou kybernetické bezpečnosti, avšak žádný veřejný či soukromý subjekt, ani jednotlivec se v České republice nesmí zříci své zodpovědnosti a úlohy při zajišťování kybernetické bezpečnosti. Pouze společně můžeme vytvořit opravdu otevřený a bezpečný kyberprostor, ve kterém budeme všichni prosperovat.

Ing. Dušan Navrátil

OBSAH

Oblast kybernetické bezpečnosti nabývá neustále na svém významu a již nyní platí za jeden z určujících aspektů bezpečnostního prostředí České republiky. Kybernetická bezpečnost představuje souhrn organizačních, politických, právních, technických a vzdělávacích opatření a nástrojů směřujících k zajištění zabezpečeného, chráněného a odolného kyberprostoru v České republice, a to jak pro subjekty veřejného a soukromého sektoru, tak pro širokou českou veřejnost. Kybernetická bezpečnost pomáhá identifikovat, hodnotit a řešit hrozby v kyberprostoru, snižovat kybernetická rizika a eliminovat dopady kybernetických útoků, informační kriminality, kyberterorismu a kybernetické špionáže ve smyslu posilování důvěrnosti, integrity a dostupnosti dat, systémů a dalších prvků informační a komunikační infrastruktury. Hlavním smyslem kybernetické bezpečnosti je pak ochrana prostředí k realizaci informačních práv člověka.

Úvod

Zajištění kybernetické bezpečnosti státu je jednou z klíčových výzev současné doby. Závislost veřejného a soukromého sektoru na informačních a komunikačních technologiích se stává stále zřetelnější. Sdílení a ochrana informací je v dnešní době zásadní pro ochranu zájmů státu a jeho obyvatel v oblasti bezpečnosti, ekonomiky a hospodářství. Zatímco široká veřejnost se nejvíce obává finančních ztrát či ztráty svých dat a zneužití osobních údajů, realita celé problematiky kybernetické bezpečnosti je mnohem rozsáhlejší. Významnými riziky jsou kybernetická špionáž (ať průmyslová, vojenská, politická či jiná), za kterou stále častěji stojí přímo vlády, potažmo bezpečnostní struktury konkrétního státu, působení organizovaného zločinu v kyberprostoru, hacktivismus, záměrné šíření dezinformací za účelem dosažení politických a vojenských cílů, či v budoucnu i kyberterorismus. Riziko v současnosti představují nejen velmi frekventované kybernetické útoky prováděné za účelem např. ekonomického prospěchu, ale i případy narušení bezpečnosti a integrity sítí způsobené nezáměrně, např. selháním lidského faktoru, živelnou pohromou apod.

Stát musí být schopen zajistit účinnou reakci na všechny současné i budoucí výzvy v prostředí neustále se měnících kybernetických hrozeb, které mohou z dynamicky se vyvíjejícího kyberprostoru přicházet, a garantovat tak zabezpečený a důvěryhodný kyberprostor.

S ohledem na svůj otevřený a veřejně přístupný charakter, který se vyznačuje absencí geografických hranic, vyžaduje internet ke svému zabezpečení a ochraně nejen iniciativu samotného státu, ale také součinnost všech občanů. Stát soustavně buduje a navyšuje národní kapacity v této oblasti, avšak bez kooperace se soukromým sektorem a akademickou sférou, dále bez intenzivní mezinárodní spolupráce a zejména bez zapojení samotných obyvatel, není zajištěna potřebná efektivita těchto aktivit.

Tato Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020 (dále jen „Strategie“) představuje základní koncepční dokument vlády České republiky pro příslušnou oblast a je v souladu s bezpečnostními zájmy a východisky definovanými v Bezpečnostní strategii České republiky. Slouží jako výchozí dokument pro tvorbu navazujících právních předpisů, politik či standardů, směrnic a jiných doporučení v rámci ochrany a zabezpečení kyberprostoru.

Strategie plně respektuje logický rámec Metodiky přípravy veřejných strategií spolu s dalšími doporučeními. Z hlediska struktury a členění textu je nejprve představena vize České republiky pro oblast kybernetické bezpečnosti, přesahující časový rámec této Strategie (2015 – 2020), a následně jsou definovány základní principy, které stát následuje při zajišťování kybernetické bezpečnosti v České republice. Na tuto první obecnější část navazuje kapitola o konkrétních výzvách na poli kybernetické bezpečnosti jak pro Českou republiku, tak i pro mezinárodní prostředí, v jehož rámci se Česká republika nachází. Závěrem jsou představeny hlavní strategické cíle, které těmto výzvám čelí a ze kterých vychází konkrétní Akční plán kybernetické bezpečnosti České republiky na období let 2015 až 2020 (dále jen „Akční plán“).

Vize

- Česká republika zajistí v rámci kyberprostoru podmínky pro hladce fungující informační společnost.
- Česká republika zaměří své úsilí na nepřetržité rozšiřování expertní základny v oblasti kybernetické bezpečnosti a schopností čelit nejnovějším kybernetickým hrozbám. Zároveň bude podporovat a rozvíjet také schopnosti bezpečnostních složek státu tak, aby byly schopny předcházet a včas detekovat aktuální hrozby.
- Česká republika, jakožto moderní středoevropská země a aktivní člen Evropské unie, Severoatlantické aliance, Organizace spojených národů a dalších mezinárodních organizací, bude v nejbližších letech aspirovat na přední postavení v oblasti kybernetické bezpečnosti, a to jak v rámci svého regionu, tak i celé Evropy.
- Česká republika bude při předcházení i řešení kybernetických útoků aktivně pomáhat svým mezinárodním partnerům, plnit závazky vyplývající z členství v mezinárodních organizacích, kolektivní obrany Severoatlantické aliance a podporovat bezpečnost v dalších státech světa.
- Česká republika bude intenzivně podporovat spolupráci a dialog zemí středoevropského regionu v oblasti kybernetické bezpečnosti a obrany skrze mezinárodní organizace, jejichž je členem.
- Česká republika bude efektivně zajišťovat nejen prvky kritické informační infrastruktury (dále jen „KII“), ale celkově bezpečnost sítí a kyberprostoru, v jehož rámci vyvíjejí aktivity její obyvatelé, a který je zásadní pro jejich ekonomické a sociální zájmy.
- Česká republika se v rámci zabezpečování své KII výrazně zaměří na zabezpečení industriálních systémů, které jsou v KII obsaženy, a do několika let bude patřit mezi přední státy se silnou expertízou a znalostmi v této oblasti.

- Česká republika, respektive GovCERT.CZ [1)], bude usilovat o budování důvěry a efektivního modelu spolupráce s národním CERT [2)], a zároveň působit jako zastřešující subjekt pro další české týmy typu CERT/CSIRT, jejichž vznik a vývoj bude zejména v rámci subjektů KII plně podporovat.

- Česká republika bude spolupracovat se subjekty ze soukromé a akademické sféry na výzkumu a vývoji zabezpečení informačních a komunikačních technologií.

- Česká republika se bude snažit dosáhnout co nejvyššího zabezpečení kyberprostoru. Zároveň bude podporovat výrobu, výzkum, vývoj a implementaci špičkových technologií a přispívat tak k zvýšení technologické úrovně v České republice s cílem zvýšit konkurenceschopnost a vytvořit optimální prostředí pro realizaci tuzemských i zahraničních investic, pro něž je funkční informační infrastruktura zásadním faktorem.

- Česká republika bude podporovat rozvoj kultury informační společnosti pomocí osvěty svých občanů i subjektů soukromého sektoru. Těm zajistí svobodný přístup ke službám informační společnosti, respektive k informacím pro zodpovědné chování a používání informačních technologií. Své občany bude chránit před škodlivými dopady, jež mohou kybernetické útoky způsobovat, a které by mohly mít negativní vliv na kvalitu jejich života či důvěru ve stát.

[1)] GovCERT.CZ představuje vládní koordinační místo pro okamžitou reakci na kybernetické bezpečnostní incidenty (vládní CERT – Computer Emergency Response Team), které je organizační složkou Národního bezpečnostního úřadu, respektive jeho specializovaného pracoviště Národního centra kybernetické bezpečnosti.

[2)] Národní CERT představuje národní koordinační místo pro okamžitou reakci na kybernetické bezpečnostní incidenty (národní CSIRT – Computer Security Incident Response Team) provozované na základě memoranda s Národním bezpečnostním úřadem.

Principy

Ochrana základních lidských práv a svobod a principů demokratického právního státu

Česká republika dodržuje při zajišťování kybernetické bezpečnosti základní lidská práva, demokratické principy a hodnoty. Respektuje charakter otevřeného a neutrálního prostředí internetu, dbá na dodržování svobody projevu, ochrany osobních dat a soukromí. Při zajišťování kybernetické bezpečnosti proto usiluje o maximální otevřenost přístupu k informacím a minimalizaci zásahů do práv občanů a soukromých subjektů. Jedním ze základních principů činnosti Národního bezpečnostního úřadu (dále jen „NBÚ“) v oblasti kybernetické bezpečnosti je ochrana základních informačních práv.

Komplexní přístup ke kybernetické bezpečnosti založený na principu subsidiarity a spolupráce

Celá Strategie dodržuje princip nedělitelnosti bezpečnosti, kde kybernetickou bezpečnost České republiky nelze oddělovat od kybernetické bezpečnosti globální, respektive v euroatlantické oblasti. Česká republika na ni tedy nahlíží komplexně, jako na úzce propojený fenomén.

Hlavním gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast je NBÚ, který koordinuje úsilí v této oblasti a poskytuje metodické vedení ostatním zainteresovaným subjektům. NBÚ je zodpovědný za rozhodnutí o předkládaných návrzích a návodech na přijetí opatření při předcházení i řešení kybernetických bezpečnostních incidentů a probíhajících kybernetických útoků.

S ohledem na komplexitu problematiky kybernetické bezpečnosti a obrany a s cílem usnadnit spolupráci mezi dotčenými subjekty, podpořit synergii jejich úsilí a zabránit nežádoucím duplikacím bude Česká republika aplikovat princip subsidiarity a zároveň koordinovat aktivity na národní úrovni[3)].

Budování důvěry a spolupráce mezi veřejným a soukromým sektorem a občanskou společností

Za zajišťování kybernetické bezpečnosti nemůže být odpovědný pouze stát a orgány veřejné správy, ale je nutná i aktivní spolupráce občanů České republiky, soukromých právnických a podnikajících fyzických osob.

Kyberprostor a především část KII jsou z velké části vlastněny a provozovány soukromým sektorem. Bezpečnostní politika v této oblasti je proto založena na inkluzivní spolupráci veřejného sektoru se soukromými subjekty, občanskou společností, i akademickou obcí. Zásadní je zde důvěryhodné prostředí, ve kterém je možno účinně spolupracovat. Důvěra mezi státem, soukromými subjekty a obecně občanskou společností je totiž nezbytná k efektivnímu zajišťování kybernetické bezpečnosti.

Vzhledem k tomu, že se stále více stírají rozdíly mezi vnitřními a vnějšími hrozbami a riziky, respektive vnitřní a vnější bezpečností, bude Česká republika rozvíjet koordinaci úsilí a posilovat důvěru mezi zainteresovanými subjekty na národní i mezinárodní úrovni.

[3)] Princip subsidiarity je ošetřen také zákonem o kybernetické bezpečnosti, který jednak stanovuje povinnosti správce či provozovatele při zabezpečení svého systému či sítě a jednak rozděluje kyberprostor do oblastí spadajících buď pod GovCERT.CZ nebo národního CERT.

Rozvoj kapacit k zajišťování kybernetické bezpečnosti

Vzhledem ke značné závislosti společnosti na informačních a komunikačních technologiích a neustálým změnám povahy současných kybernetických hrozeb a rizik závisí kybernetická bezpečnost České republiky nejen na neustálém budování robustnější, odolnější informační infrastruktury, ale i na společnosti jako celku.

Proto Česká republika podporuje a navyšuje investice do výzkumu a vývoje v oblasti kybernetické bezpečnosti (a to i do vývoje a výroby vlastních národních technologií v oblasti kybernetické bezpečnosti), stejně jako do vzdělávání a osvěty koncových uživatelů, tedy obyvatel České republiky.

Česká republika v rámci zajišťování kybernetické bezpečnosti buduje a kontinuálně navyšuje možnosti a schopnosti národní expertízy a rovněž posiluje stávající struktury a procesy spolupráce v oblasti potírání informační kriminality. Jednou z priorit je i posílení kooperace mezi orgány činnými v trestním řízení a dalšími složkami zajištujícími kybernetickou bezpečnost v České republice.

Výzvy

1. **Česká republika jako možný testovací objekt**

   Česká republika, jakožto země využívající ke svému zabezpečení moderní technologie používané i dalšími státy, může sloužit útočníkům jako testovací objekt před samotným útokem na naše spojence či jiné státy s větším strategickým významem, užívající stejné technologie a zabezpečovací mechanismy a procesy jako Česká republika.

2. **Nedostatečná důvěra veřejnosti ve stát**

   V poslední době obecně utrpěla důvěra veřejnosti ve státy jako entity zajišťující kybernetickou bezpečnost a jejich bezpečnostní aparáty. Bez důvěry a dobrovolné spolupráce českých občanů a soukromého sektoru se subjekty zajišťujícími kybernetickou bezpečnost je však celý koncept kybernetické bezpečnosti bez významu.

3. **Vzrůstající počet uživatelů internetu, informačních a komunikačních technologií a narůstající kritičnost jejich selhání**

   Se zvýšeným počtem uživatelů internetu (okolo 67% českých domácností) [4)] a informačních a komunikačních technologií se váže i vzrůstající závislost veřejné i soukromé sféry (97% firem využívá internet)[5)] na těchto technologiích, narůstá kritičnost jejich selhání, a to především u těch spadajících pod KII a významné informační systémy (dále jen „VIS“).

---

4) Podle údajů ČSÚ za rok 2013 (viz www.czso.cz).

5) Podle údajů nezávislé studie EEIP „ Česká internetová ekonomika“ 2013 (viz www.studiespir.cz)

4. **Se vzrůstajícím počtem uživatelů mobilních platforem stoupá i množství mobilního malware**

   Malá část společnosti využívá alespoň základní ochranné prvky (např. antivirové programy) ve svých chytrých telefonech a tabletech. Tohoto využívají útočníci, což dokládá každoročně se zvyšující množství malware i uskutečněných útoků na tato zařízení.

5. **Možnosti zneužití zadních vrátek hardware pro exfiltraci informací**

   Se zvyšujícím se počtem uživatelů a dodavatelů technologií roste riziko zabudování zadních vrátek do hardware. Ta mohou být následně zneužita například pro sledování a získávání strategicky důležitých či osobních a citlivých dat.

6. **Koncept „internetu věcí“**

   Zatímco počet zařízení připojených k internetu neustále narůstá, velké části společnosti chybí povědomí o nezbytné digitální hygieně, tedy jak se v online prostředí pohybovat a jak zabezpečit používaná zařízení. Významu zde nabývá koncept „internetu věcí“, který tuto výzvu ještě umocňuje. Zatímco s klasickými zařízeními jako PC či notebooky jsou antivirové programy, firewall apod. automaticky spojovány, s ostatními chytrými zařízeními jako TV, lednice apod. to neplatí a jejich uživatelé mnohdy ani netuší, jak jejich provoz zabezpečit.

7. **Bezpečnostní rizika spjatá s přechodem z protokolu IPv4 na IPv6**

   Nutný přechod z protokolu IPv4 na nový IPv6 s sebou nese i nová kybernetická bezpečnostní rizika. Tato rizika musí být minimalizována tak, aby bylo dosaženo úspěšné implementace a zabezpečení tohoto protokolu jak na úrovni veřejné správy, tak u soukromých subjektů.

8. **Bezpečnostní rizika spjatá s elektronizací veřejné správy (eGovernment)**

   Pokračující digitalizace veřejné správy v České republice slouží k zlepšení fungování veřejné správy a jejího vztahu k veřejnosti. Avšak služby a aplikace poskytované

občanům a soukromým podnikům prostřednictvím eGovernment s sebou nesou značná kybernetická bezpečnostní rizika.

9. **Nedostatečné zabezpečení malých a středních podniků**

Vzrůstá potřeba provádět u malých a středních podniků osvětu, seznamovat je s nejlepší praxí, metodami na ochranu své informační infrastruktury, bezpečným nakládáním s informacemi a pomáhat je tak chránit před kybernetickými útoky. Ze své podstaty si jednak neuvědomují svůj význam a potřebu řešit vlastní kybernetickou bezpečnost a jednak ani nedisponují potřebnými prostředky a know-how pro svou ochranu. Jejich systémy a data přitom mohou být stejně kritická jako u velkých podniků, případně mohou pracovat s kritickými daty nebo systémy v rámci zajišťování služeb pro jiné subjekty.

10. **Big data, skladování dat v nových prostředích**

Ochrana a zabezpečení dat je pro Českou republiku velmi důležité, a to především těch, které jsou záležitostí veřejného zájmu (data relevantní k KII a VIS). Ve veřejné i soukromé sféře narůstá množství dat, se kterými se pracuje a která je zapotřebí nadále skladovat. Začaly se proto využívat nové formy ukládání dat, např. cloudová úložiště. Zvýšené používání těchto online služeb a cloudů však vede mnohdy k netransparentnímu řešení zabezpečení, jehož důvěryhodnost je minimálně sporná.

11. **Ochrana průmyslových řídicích systémů a informačních systémů ve zdravotnictví**

Ze sféry přímého ekonomického prospěchu útočníků se útoky přesouvají například do oblasti kybernetické průmyslové špionáže, kybernetického vandalismu a vyhledávání zranitelností prvků kritické infrastruktury a významných informačních systémů. Útočníci se stále více zaměřují na takové prvky informační infrastruktury, jakými jsou např. energetické systémy, produktovody a informační systémy ve zdravotnictví. Tyto systémy, jejichž selhání může mít fatální následky, se však vyznačují vysokou heterogenností technického řešení, s čímž přímo souvisí i technická náročnost jakýchkoliv ex post analýz.

12. **Inteligentní energetické sítě**

Inteligentní rozvodné sítě představují potenciálně další krok v modernizaci distribučního systému energetické sítě České republiky. Tyto technologie mohou zlepšit spolehlivost, bezpečnost a účinnost energetických sítí. Na druhou stranu však digitalizace těchto do té doby pasivních systémů znamená riziko jejich narušení útočníkem či možné narušení soukromí uživatelů energetických sítí.

13. **Vzrůstající závislost obranných složek státu na informačních a komunikačních technologiích**

Informační a komunikační technologie ve stále větší míře pronikají do systémů, sítí i samotné techniky (např. vozidla ozbrojených sil, vojenská letecká technika) obranných složek státu. Zranitelnosti těchto technologií a hrozby jejich narušení nebo zničení včetně působení kybernetických útoků výrazně zvyšují rizika negativního dopadu na plnění základních schopností obranných složek při obraně státu a při plnění závazků vyplývajících zejména z členství v Severoatlantické alianci a Evropské Unii. Obranné složky státu musí mít schopnost efektivně reagovat na hrozby plynoucí z kyberprostoru a aktivně participovat na jejich zneškodnění.

14. **Malware je stále sofistikovanější**

S vyšší sofistikovaností škodlivého softwaru i samotných útočníků jsou silně omezeny možnosti dohledání zdroje útoku, tj. možnosti reverzního inženýrství a forenzní analýzy. Tyto analytické postupy budou předmětem vzdělávání odborníků na kybernetickou bezpečnost.

15. **Botnety a DDoS/DoS útoky**

Botnety, pomocí nichž se provádějí velmi časté DDoS/DoS útoky, nabývají na robustnosti, odolnosti a míře svého utajení. Z těchto důvodu je nezbytné zvýšit povědomí o možnostech obrany proti DDoS/DoS útokům.

16. **Nárůst informační kriminality**

Vzhledem k otevřenému, anonymnímu charakteru internetu narůstají i možnosti obchodování s citlivými informacemi, snadná dostupnost, či dokonce volné nakupování kriminálních služeb. V souvislosti s pokračujícím pronikáním informačních technologií do běžného života a fungování společnosti dochází také k rychlému přesunu řady kriminálních aktivit do virtuálního prostředí, které pachatelům slibuje rychlý účinek při výrazně sníženém riziku postihu. K tomu přispívá zejména anonymita a prostorová neuchopitelnost internetu. To vše umožňuje jak vysoce cílené, tak masové a plošné útoky.

17. **Hrozby a rizika spjaté s užíváním sociálních sítí na internetu**

Se vzrůstajícím počtem uživatelů sociálních sítí na internetu roste i nebezpečí odcizení soukromých dat či dokonce digitální identity jednotlivců a entit.

18. **Nízká digitální gramotnost koncových uživatelů**

Velké části koncových uživatelů nejen v rámci veřejné správy, ale i z řad veřejnosti chybí základní povědomí o běžných metodách počítačových útoků (zejména phishing, falešné e-shopy apod.), jejichž obětí se ročně stávají tisíce občanů České republiky.

19. **Nedostatek odborníků na kybernetickou bezpečnost a nutnost revize stávajících studijních programů ve školství**

Český model vzdělávání a výchovy v oblasti kybernetické bezpečnosti neodpovídá v současné podobě aktuálním požadavkům a trendům. Z tohoto důvodu pak nedostatečně vzdělává a vychovává na základním a středním stupni žáky a také v nedostatečné míře nabízí vysokoškolské programy, které by vytvářely odborníky na kybernetickou bezpečnost. Poptávka po těchto odbornících je přitom vysoká.

Hlavní cíle

A. Zajištění efektivity a posilování všech struktur, procesů a spolupráce při zajišťování kybernetické bezpečnosti

- Vytvořit efektivní model spolupráce na národní úrovni mezi jednotlivými subjekty kybernetické bezpečnosti – pracoviště typu CERT a CSIRT, subjekty KII apod., a posilovat jejich stávající struktury a procesy.
- Vytvořit národní, koordinovaný postup pro zvládání incidentů, který nastaví formát spolupráce, bude obsahovat komunikační matici, protokol postupu a definovat jednotlivé role aktérů.
- Vytvořit metodologii pro hodnocení rizik v České republice na úrovni státu.
- Udržovat jednotný postoj České republiky směrem do zahraničí, který bude koordinován s ostatními resorty zainteresovanými v oblasti kybernetické bezpečnosti[6)].
- Zohledňovat odpovídajícím způsobem neustále se vyvíjející problematiku kybernetických hrozeb v rámci tvorby a aktualizací významných bezpečnostně-strategických materiálů České republiky (Bezpečnostní strategie České republiky a další).

B. Aktivní mezinárodní spolupráce

- V rámci svého členství v Evropské Unii, Severoatlantické alianci, Organizaci spojených národů, Organizaci pro bezpečnost a spolupráci v Evropě, Mezinárodní telekomunikační unii a dalších mezinárodních organizacích se aktivně podílet na mezinárodní diskuzi v aktivitách v rámci fór, programů, iniciativ apod.
- Ve středoevropském prostoru působit jako propagátor kybernetické bezpečnosti a dialogu mezi státy regionu.

[6)] Konkrétní řešení problematiky koordinace ostatních zainteresovaných subjektů bude ošetřena v Akčním plánu.

- Navazovat a prohlubovat bilaterální spolupráci s dalšími státy.
- Účastnit se a organizovat mezinárodní cvičení.
- Účastnit se a organizovat mezinárodní školení.
- Podílet se na vytváření efektivního modelu spolupráce a budování důvěry mezi pracovišti typu CERT a CSIRT na mezinárodní úrovni, mezinárodními organizacemi a akademickými centry.
- Podílet se na vytváření mezinárodního konsenzu v rámci oficiálních i neoficiálních kanálů ohledně právních norem a chování v kyberprostoru, zajištění otevřenosti internetu, lidských práv a svobod.

C. Ochrana národní KII a VIS

- Pokračovat v průběžné analýze a kontinuálním sledování zabezpečení systémů KII a VIS v České republice pomocí jasně definovaného protokolu.
- Podporovat vznik dalších pracovišť typu CERT a CSIRT v České republice.
- Průběžně navyšovat odolnost, integritu a důvěryhodnost systémů a sítí KII a VIS.
- Kontinuálně provádět analýzu a monitoring hrozeb a rizik v České republice.
- Efektivně sdílet informace mezi státem a subjekty KII a VIS.
- Navyšovat technologické kapacity a schopnosti Národního centra kybernetické bezpečnosti (dále jen „NCKB“), potažmo GovCERT.CZ a v rovině personální neustále vzdělávat a školit zaměstnance/experty tohoto pracoviště.
- Důkladně a důvěryhodně zabezpečit prostředí pro skladování a práci s daty subjektů KII a VIS, které zřídí a bude spravovat stát.
- Pravidelně provádět kontroly, odhalování chyb a zranitelností v informačních systémech a sítích využívaných státem, založené na principu penetračních testů v KII a VIS.
- Průběžně navyšovat technologické a organizační předpoklady k aktivnímu odvrácení (potlačení) kybernetických útoků.
- Zvyšovat národní možnosti, schopnosti a kapacity v oblasti aktivní obrany a protiopatření proti kybernetickým útokům.

- Vzdělávat specializované odborníky, kteří se zaměří na problematiku a možnosti aktivních protiopatření při zajišťování kybernetické bezpečnosti a obrany a na obecně ofenzivní pojetí kybernetické bezpečnosti.
- Zpracovat postup pro přechod mezi vyhlášeným stavem kybernetického nebezpečí dle zákona o kybernetické bezpečnosti a stavy dle ústavního zákona č. 110/1998 Sb., o bezpečnosti České republiky.

D. Spolupráce se soukromým sektorem

- Pokračovat v navazování spolupráce se soukromým sektorem a navyšovat povědomí o práci a aktivitách NBÚ v oblasti kybernetické bezpečnosti.
- Vytvořit v kooperaci se soukromými subjekty jednotné bezpečnostní normy, standardizovat spolupráci a stanovit povinnou úroveň zabezpečení pro subjekty kritické informační infrastruktury.
- Zajistit v kooperaci se soukromým sektorem kyberprostor poskytující spolehlivé prostředí pro sdílení informací, výzkum a vývoj a zajistit bezpečnou informační infrastrukturu stimulující podnikání soukromých subjektů v zájmu podpory konkurenceschopnosti všech podnikajících soukromých subjektů v České republice a chránicí jejich investice.
- Vzdělávat a provádět osvětu soukromého sektoru v oblasti kybernetické bezpečnosti. Soukromým subjektům tak poskytnout potřebné vedení, jak se správně chovat nejen při mimořádných situacích, respektive při kybernetických incidentech, ale i při každodenní činnosti.
- Navyšovat důvěru mezi soukromým sektorem a státem, mimo jiné vytvořením platformy/systému na národní úrovni pro sdílení informací o hrozbách, incidentech a aktuálním ohrožení.

E. Výzkum a vývoj / Spotřebitelská důvěra

- Podílet se na národních i evropských výzkumných projektech a aktivitách v oblasti kybernetické bezpečnosti.
- Určit NBÚ jako hlavní kontaktní centrum v oblasti výzkumu v kybernetické bezpečnosti. NBÚ bude přispívat ke koordinaci výzkumných aktivit v této oblasti s cílem zabránit zdvojování výzkumných aktivit. Výzkum v oblasti kybernetické bezpečnosti se tak zaměří na opravdu podstatné problémy a převod výzkumných výsledků do praxe.
- Spolupracovat se soukromým a akademickým sektorem na vývoji a implementaci technologií využívaných státem k zajištění jejich maximálního zabezpečení a transparentnosti. Testovat a hodnotit míru zabezpečení používaných technologií.
- Spolupracovat s akademickou a soukromou sférou na výzkumných projektech (včetně primárního i experimentálního výzkumu) a aktivitách v technologické i společenskovědní oblasti, a to především na národní, evropské i mezinárodní transatlantické úrovni.
- Stanovením výzkumu a vývoje národní prioritou aktivně stimulovat investice do této oblasti.

F. Podpora vzdělávání, osvěta a rozvoj informační společnosti

- Navyšovat povědomí a gramotnost v otázkách kybernetické bezpečnosti jak u žáků a studentů základních a středních škol, tak i u široké veřejnosti, respektive koncových uživatelů, pomocí podpory iniciativ a osvětových kampaní, pořádáním konferencí pro veřejnost apod.
- Modernizovat stávající vzdělávací programy na základní a středoškolské úrovni a podporovat na vysokoškolské úrovni nové studijní programy, které budou přímo vytvářet experty na kybernetickou bezpečnost.
- Vzdělávat a školit zaměstnance veřejné správy působící nejen v oblasti kybernetické bezpečnosti a informační kriminality.

G. Podpora rozvoje schopností Policie České republiky vyšetřovat a postihovat informační kriminalitu

- Posílit personálně jednotlivá policejní pracoviště informační kriminality.
- Modernizovat technologické vybavení odborných policejních pracovišť.
- Zakotvit vazby přímé a rychlé spolupráce se zainteresovanými národními subjekty a ostatními bezpečnostními složkami pro oblast informační kriminality.
- Podpořit spolupráci se zahraničními subjekty v oblasti výměny informací k informační kriminalitě a v oblasti vzdělávání.
- Odborně vzdělávat a školit policejní specialisty.
- Vybudovat multidisciplinární akademické prostředí pro podporu rozvoje schopností Policie České republiky postihovat informační kriminalitu.

H. Právní úprava pro kybernetickou bezpečnost (vytváření právního rámce). Účast na tvorbě a implementaci evropských a mezinárodních pravidel

- Na základě systematického přístupu, tj. vzhledem k existujícím právním předpisům, vytvářet v oblasti kybernetické bezpečnosti srozumitelné, efektivní a proporcionální právní předpisy.
- Aktivně se účastnit tvorby a implementace evropských a mezinárodních pravidel.
- Provádět jak kontinuální analýzu efektivity účinné právní úpravy a jejího souladu s aktuálními poznatky z dotčených technických a společenskovědních oborů, tak i průběžné provádění změn a doplňování tak, aby právní úprava odpovídala aktuálním požadavkům bezpečné informační společnosti.
- Podporovat vzdělávání v problematice kybernetické bezpečnosti v rámci justičních orgánů (tj. státních zástupců nebo soudců).

Implementace

Na základě hlavních cílů Strategie je v koordinaci s ostatními zainteresovanými subjekty vypracován podrobný **Akční plán**, který definuje konkrétní kroky, stanoví u nich zodpovědnost, termíny jejich plnění a kontrolu[7)].

NBÚ a jeho specializované pracoviště NCKB bude průběžně sledovat, diskutovat a hodnotit plnění jednotlivých cílů ve spolupráci s ostatními zainteresovanými subjekty. V rámci každoroční **Zprávy o stavu kybernetické bezpečnosti v České republice** zajistí zpracování **hlášení o stavu naplňování Akčního plánu** ve formě přílohy. Zpráva bude vládu i širokou veřejnost informovat o efektivitě přijímaných opatření a plnění úkolů definovaných Strategií.

7) Předpokládané schválení Akčního plánu Vládou České republiky je 2. čtvrtletí roku 2015.

Seznam použitých zkratek

CERT – Computer Emergency Response Team

CSIRT – Computer Security Incident Response Team

DDoS/DoS – Distributed Denial of Service / Denial of Service

IPv4 – Internet Protocol version 4

IPv6 – Internet Protocol version 6

KII – Kritická informační infrastruktura

NBÚ – Národní bezpečnostní úřad

NCKB – Národní centrum kybernetické bezpečnosti

Slovník použitých pojmů [8)]

Botnet

Sítě infikovaných počítačů zneužitelných k páchání kriminálních aktivit, které díky přístupu k výpočetnímu výkonu mnoha tisíců strojů současně mohou provádět nezákonnou činnost ve velkém měřítku – zejména útoky DDoS a distribuci spamu.

Cloud / Cloudové úložiště

Model skladování digitálních dat v online prostředí.

DDoS / DoS útoky

Technika útoku na internetové služby nebo stránky, při níž dochází k přehlcení požadavky a k pádu nebo nefunkčnosti a nedostupnosti systému pro ostatní uživatele a to útokem z mnoha vektorů.

Forenzní analýza

Vyšetřovací postup nad digitálními daty používaný k získávání důkazů o aktivitách uživatelů (útočníků) v oblasti informačních a komunikačních technologií.

Hacktivismus

Použití hackerských dovedností a technik k dosažení sociálních a politických cílů.

Malware

Souhrnné označení pro škodlivý software, mezi který patří počítačové viry, trojské koně, červi či špionážní software.

Reverzní inženýrství

Zpětné analyzování škodlivého software, jehož cílem je odkrýt jeho strukturu a princip fungování.

Penetrační testování

Zkoumání funkcí počítačového systému a sítí s cílem najít slabá místa informační bezpečnosti tak, aby bylo možno tato slabá místa odstranit.

[8)] Obsáhlejší výkladový slovník termínů kybernetické bezpečnosti je k nalezení na www.govcert.cz.