NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

SK NBÚ CERT

NÁRODNÁ STRATÉGIA KYBERNETICKEJ BEZPEČNOSTI NA ROKY 2021 AŽ 2025

Obsah

PREDSLOV 4

1. ÚVOD 5

2. PRINCÍPY 6

3. HROZBY 9

4. STRATEGICKÉ CIELE 13

5. HLAVNÍ ZAHRANIČNOPOLITICKÍ PARTNERI 26

6. IMPLEMENTÁCIA A MERATEĽNOSŤ 27

7. FINANCOVANIE 29

8. ZÁVER 29

Predslov

Máloktorá oblasť v modernom svete sa vyvíja tak rýchlo ako výzvy, ktoré so sebou prináša riadenie kybernetickej bezpečnosti štátu. Dôkladné nastavenie procesov, postupov a cieľov sa musí dynamike tohto trendu prispôsobiť naplno.

Nová národná stratégia kybernetickej bezpečnosti vzniká v čase, keď sa môže javiť, že na mnohé opatrenia je už neskoro. Rôzni útočníci sa posúvajú míľovými krokmi každý deň. Nie je vylúčené, že aj v tejto chvíli môže byť ktokoľvek terčom kybernetického útoku bez toho, aby o tom ešte čokoľvek tušil.

Štát a jeho kritická infraštruktúra sú dlhodobo na muške štátnych aj neštátnych aktérov. Kybernetické bezpečnostné incidenty sú dnes často sofistikované a kreatívne. Presne taký by mal byť aj prístup k nim. Národná stratégia kybernetickej bezpečnosti na obdobie rokov 2021 až 2025 má jednoduchý zámer – pripraviť a dostať Slovensko na úroveň, aby bolo vždy o krok ďalej pred potenciálnou hrozbou.

Každý z nás si želá modernú, digitalizovanú krajinu, v ktorej namiesto státia v radoch vybavíme všetko z pohodlia domova či kancelárie. Komfort výdobytkov modernej doby si však vyžaduje o to väčšiu ostražitosť. Dokument pomenúva princípy, na ktorých stojí stratégia Slovenskej republiky, identifikuje hrozby pre kybernetický priestor a jednoznačné definuje ciele či smerovanie, ktorým sa krajina pri ochrane nielen virtuálneho sveta musí nevyhnutne uberať.

Víziou Národného bezpečnostného úradu je posilňovanie a vytvorenie otvoreného, slobodného a bezpečného kybernetického priestoru pre všetkých.

Predpokladom úspechu v kolektívnej bezpečnosti je predovšetkým spoločná súhra. Každý celok je len taký silný ako jeho najslabší prvok. Akákoľvek stratégia má vo svojej podstate spájať jednotlivcov do skupín, skupiny do organizácií a organizácie do systému so spoločným cieľom.

Národná stratégia kybernetickej bezpečnosti, ktorú vypracoval NBÚ, je preto určená pre každého, kto sa akýmkoľvek spôsobom podieľa na budovaní systému riadenia kybernetickej bezpečnosti Slovenskej republiky. Je a bude strešným dokumentom, z ktorého vychádza základné smerovanie krajiny v tejto oblasti.

Roman Konečný

riaditeľ Národného bezpečnostného úradu

1. Úvod

Modernizácia spoločnosti prostredníctvom informačných a komunikačných technológií, jej digitalizácia a rozvoj inovatívnych služieb sú nepopierateľným faktom, ktorý sa stal prirodzenou súčasťou našich životov. Rozvoj, ktorý prináša rozširovanie možností, však musí byť vyvažovaný zodpovednosťou za riziká, ktoré vznikajú paralelne ako negatívna daň za výhody digitálnej spoločnosti.

Kybernetická bezpečnosť je stav, v ktorom sú informačné systémy a služby odolné voči aktuálnym hrozbám a zraniteľnostiam, ale aj pripravené na detekciu a riešenie kybernetických bezpečnostných incidentov, obnovu dát a procesov a minimalizáciu následkov. Kybernetická bezpečnosť však nie je len záležitosťou konkrétnych organizácií a subjektov, ktoré prostredníctvom vhodných opatrení chránia svoje aktíva.

Informatizácia verejného sektora, automatizácia výrobných a iných procesov, ktoré boli v minulosti vykonávané manuálne, neustály rozvoj a ľahká dostupnosť technológií, jednoduchosť ich používania v širokom spektre bežných činností vytvárajú priestor, v ktorom popri nesporných výhodách vznikajú hrozby namierené proti kritickým a citlivým systémom a službám štátu. Môžu narušiť dôveru občana v štát, spôsobiť rozsiahle ekonomické a hospodárske škody až po škody na zdraví a živote občanov.

Systém riadenia informačnej a kybernetickej bezpečnosti, ktorým sa má zabezpečiť vysoká miera odolnosti systémov a služieb a tiež efektívne detekčné a reakčné schopnosti, je strategickým bezpečnostným záujmom Slovenskej republiky. Ucelený koncept riadenia informačnej a kybernetickej bezpečnosti, strategické smerovanie na základe jasných princípoch a presne definované strategické ciele sú základom pre dobre vyvinutý systém, ktorý dokáže pružne reagovať na aktuálne hrozby a zabezpečiť tak vysokú mieru kybernetickej bezpečnosti na národnej úrovni. Práve takýto koncept prináša Národná stratégia kybernetickej bezpečnosti na roky 2021 až 2025.

Historicky, Národná stratégia kybernetickej bezpečnosti na roky 2021 až 2025 (ďalej len „Národná stratégia") nie je prvým strategickým dokumentom, ktorý bol na národnej úrovni vytvorený. V roku 2007 bola vytvorená stratégia informačnej bezpečnosti spolu s akčným plánom a následne v období rokov 2015 až 2020 bola platná Koncepcia kybernetickej bezpečnosti Slovenskej republiky, ktorá bola prvým uceleným plánom, ktorý popísal princípy, zásady a ciele kybernetickej bezpečnosti. Opatrenia, ktoré zarámcovali túto koncepciu, sa zameriavali na vytvorenie inštitucionálneho rámca riadenia, prijatie vhodnej legislatívy, rozpracovanie základných mechanizmov správy kybernetického priestoru, vypracovanie systému vzdelávania, vytvorenie kultúry riadenia rizík, aktívnu medzinárodnú spoluprácu a podporu vedy a výskumu. Ku koncepcii bol vytvorený Akčný plán jej realizácie, ktorý určil konkrétne úlohy viažuce sa na jednotlivé opatrenia, gestorstvo subjektov, zodpovednosti participujúcich orgánov, ako aj časové rozmedzie plnenia úloh. V časovom horizonte, na ktorý boli Koncepcia s Akčným plánom prijaté, sa podarilo vytvoriť stabilný inštitucionálny rámec riadenia kybernetickej bezpečnosti, prijať historicky prvú komplexnú legislatívu v oblasti kybernetickej bezpečnosti a boli vytvorené špecializované entity na riešenie kybernetických bezpečnostných incidentov.

Kybernetické hrozby, ako aj kybernetická bezpečnosť sa neustále vyvíjajú. Neustále vznikajú nové ciele a vektory kybernetických útokov, ktoré sú čoraz rozsiahlejšie, častejšie a sofistikovanejšie. Niektoré štáty a neštátni aktéri sa stále viac uchyľujú k presadzovaniu svojich cieľov prostredníctvom nekalých kybernetických aktivít. Tieto môžu mať viaceré formy, vrátane útokov na kritickú infraštruktúru, kybernetickej špionáže, krádeže duševného vlastníctva, kybernetickej kriminality a kybernetických útokov ako súčasti hybridných hrozieb. Kybernetický priestor sa stále viac stáva oblasťou strategickej konfrontácie medzi štátmi, ktorá odráža dynamické geopolitické prostredie a úsilie zmenu súčasného medzinárodného poriadku. Technologické inovácie, vrátane inovácií v oblasti kybernetickej bezpečnosti sa stávajú nástrojom konfrontácie a rastúceho napätia v politickej, hospodárskej a bezpečnostnej oblasti.

Dobrou správou je, že strategické smerovanie systému kybernetickej bezpečnosti môže stavať na dobrých základoch, ktoré položila Koncepcia a rozvinul jej akčný plán aj napriek tomu, že niektoré z úloh neboli úspešne ukončené.

Nová stratégia nadväzuje na vykonané aktivity a má ambíciu moderným spôsobom reagovať na aktuálne a perspektívne bezpečnostné hrozby, zadefinovať princípy systému kybernetickej bezpečnosti a určiť strategické ciele, ktorých dosiahnutím sa zabezpečí vyššia miera bezpečnosti v kybernetickom priestore Slovenskej republiky. Národná stratégia je určená pre všetky subjekty, ktoré sa podieľajú na budovaní systému kybernetickej bezpečnosti Slovenskej republiky a je strešným dokumentom, z ktorého vychádza základné smerovanie Slovenskej republiky v tejto oblasti.

Víziou Národnej stratégie je posilňovanie a vytvorenie otvoreného, slobodného a bezpečného kybernetického priestoru pre všetkých.

2. Princípy

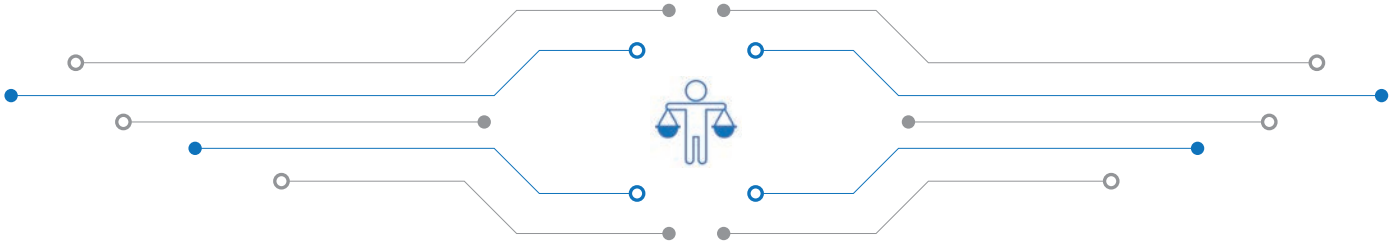
> Kybernetická bezpečnosť Slovenskej republiky je riešená komplexným systémom, ktorý zahŕňa nielen zákony, ktoré ju regulujú, ale aj praktické aktivity, ako sú riadenie rizík, detekcia a riešenie kybernetických bezpečnostných incidentov, obnova systémov, vzdelávanie, šírenie bezpečnostného povedomia a v neposlednom rade výskum a vývoj nástrojov a procesov kybernetickej bezpečnosti. Aby takýto rozsiahly systém mohol fungovať a jednotlivé zainteresované strany mohli spolupracovať na jeho udržaní a rozvoji, musia byť rešpektované základné princípy, ktoré stoja na demokratických hodnotách právneho štátu a zároveň odzrkadľujú moderný prístup k riešeniu kybernetickej bezpečnosti na národnej úrovni aj k medzinárodnej spolupráci v tejto oblasti.

2.1 Základné ľudské práva a slobody v kybernetickom priestore na prvom mieste

Kybernetický priestor je miestom, v ktorom sa s pokračujúcou digitalizáciou stretáva čoraz väčšie množstvo používateľov, ktorí tu realizujú nielen svoje potreby, ale odovzdávajú v tomto priestore aj časť svojej identity a súkromia. Prostredníctvom internetu komunikujeme s rodinou a priateľmi, nakupujeme veci bežnej spotreby, platíme účty, alebo riadime svoju inteligentnú domácnosť. Kybernetický priestor je takisto osobitnou operačnou doménou, uznanou Severoatlantickou alianciou.

Tak ako fyzický svet, ani kybernetický priestor nie je ideálnym miestom. V posledných dvoch dekádach sme svedkami zvyšujúcej sa frekvencie kybernetických útokov, väčšej sofistikovanosti útočníkov a narastajúcich strát na strane obetí. Slovenská republika sa hlási k rešpektovaniu základných ľudských práv tak, ako sú zadefinované v Charte ľudských práv a presadzuje názor, že ľudské práva sú vykonateľné ako v „offline", tak aj v „online" priestore. Tento princíp SR dlhodobo zastáva a presadzuje a hlási sa k štátom s rovnakým hodnotovým ukotvením, pričom podporuje zodpovedné správanie sa štátov a jednotný výklad medzinárodného práva v kybernetickom priestore.

Kybernetický priestor musíme začať považovať za ekvivalent fyzického sveta, spolu s aplikáciou jednoznačných pravidiel, ktoré budú rešpektovať ústavou garantované základné ľudské práva a slobody, vrátane práva na súkromie tak, aby bol nielen bezpečný, ale aj otvorený, slobodný a prístupný pre všetkých, ktorí doň vstupujú. Bezpečnosť kybernetického priestoru musí byť prepojená s jeho slobodou a základné ľudské práva a slobody v digitálnom priestore je možné garantovať iba za predpokladu zachovania digitálnej suverenity krajín Európskej únie ako celku, čo zaručuje nezávislosť a suverenitu aj v kybernetickom priestore.



2.2 Systém riadenia kybernetickej bezpečnosti založený na zákonnosti a mechanizmoch bezpečnostného systému SR

Slovenská republika je demokratický a právny štát. Systém riadenia kybernetickej bezpečnosti preto rešpektuje zásady, ktoré sú vlastné Slovenskej republike a ktoré vytvárajú prostredie, v ktorom sú rešpektované zákony, práva a slobody občanov. Systém riadenia kybernetickej bezpečnosti plne rešpektuje Ústavu Slovenskej republiky a platné a účinné zákony, pričom sa tiež opiera o Programové vyhlásenie vlády v strategických cieľoch a úlohách Národnej stratégie.

Národná stratégia kybernetickej bezpečnosti má právny základ v zákone č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov a premieta povinný obsah, ktorý je zakotvený v smernici Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii a bol transponovaný do predmetného zákona. Takisto reflektuje aj strategické smerovanie v oblasti bezpečnosti a dodržiava princípy zakotvené v Bezpečnostnej stratégii Slovenskej republiky.

2.3 Komplexný (univerzálny) prístup k problematike kybernetickej bezpečnosti

Na zaistenie bezpečnosti kybernetického priestoru neexistuje jednotný návod. Je to kontinuálny proces, ktorý musí reagovať na mnohé zložité aspekty. Pritom netreba zabúdať na technologický rozvoj spoločnosti a moderné technológie, ktoré do našich životov prenikajú oveľa rýchlejšie, ako pravidlá ich bezpečného používania.

K problematike kybernetickej bezpečnosti je potrebné stavať sa tak, aby jej riešenie bolo spoľahlivé, uchopiteľné a zrozumiteľné. Jednotlivé komponenty kybernetickej bezpečnosti nestačí iba rozvíjať, ale medzi týmito komponentami musia byť jasné vzťahy tvoriace funkčný celok. Kybernetická bezpečnosť nie je samostatne stojaca entita. Treba si uvedomiť, že zabezpečenie vysokej miery kybernetickej bezpečnosti je prostriedkom úspešného sociálno-ekonomického rozvoja spoločnosti a zvyšovania odolnosti štátu voči bezpečnostným hrozbám. Integrované previazanie kybernetickej bezpečnosti na ostatné odvetvia a uvedomenie si vzájomných vzťahov medzi bezpečnosťou a fungovaním spoločnosti je základnou zložkou opodstatnenosti a dôležitosti riešenia kybernetickej bezpečnosti na národnej úrovni.

Kybernetická a informačná bezpečnosť sa venujú ochrane informačných aktív. Informačná bezpečnosť rieši bezpečnosť aktív bez ohľadu na to, kde a akým spôsobom sú informácie spracovávané, kybernetická bezpečnosť sa venuje bezpečnosti iba určitej časti informačných aktív, konkrétne tých, ktoré sú spracúvané vo virtuálnom priestore. Údaje, označované tiež ako dáta, sa stávajú informáciami vtedy, ak nadobudnú určitý význam, zmysel, no hlavne hodnotu. V tomto kontexte teda kybernetická a informačná bezpečnosť zaručujú bezpečnosť akýchkoľvek informácií, vrátane osobných údajov. Presah kybernetickej a informačnej bezpečnosti na ochranu osobných údajov je naplnením ich cieľa – ochrana akýchkoľvek údajov a informácií.

2.4 Riadenie rizík ako nosný prvok systému riadenia národnej kybernetickej bezpečnosti

Opatrenia v oblasti zabezpečovania kybernetickej bezpečnosti musia byť vždy primerané a vyvážené voči riziku, ktoré majú znížiť resp. ošetriť. Analýza rizík je základnou činnosťou, pomocou ktorej sa zisťuje aktuálny stav aktív a hrozieb, zraniteľností, závažnosti rizík a možných dopadov. Výsledkom takejto analýzy je kvantitatívne alebo kvalitatívne hodnotenie prítomných rizík a následne je možné presne určiť opatrenia na zníženie týchto rizík.

Systém riadenia kybernetickej bezpečnosti na národnej, ale aj na sektorových úrovniach, vychádza z tzv. prístupu cez riadenie rizík, ako komplexnej a exaktnej metódy na identifikáciu rizík na rôznych úrovniach riadenia kybernetickej bezpečnosti. Identifikácia rizika na rôznych úrovniach umožní rozhodnúť o adresných a efektívnych opatreniach, ktoré nespôsobia neprimerané náklady a určí konkrétne kroky, ktoré je potrebné vykonať na dosiahnutie vysokej miery bezpečnosti kybernetického prostredia.

2.5 Podpora, spolupráca a prevencia

Kybernetickú bezpečnosť je potrebné chápať ako spoločný záujem štátu, jeho obyvateľov, komerčných i nekomerčných organizácií.. Na jednej strane je potrebné vytvárať pravidlá v podobe zákonov, nariadení, metodík a technických noriem, zároveň je však potrebné tieto pravidlá vytvárať tak, aby boli reálne vykonateľné.

Vzhľadom na charakter systému kybernetickej bezpečnosti a jeho komplexnosť, musí byť záujmom štátu podporovať jednotlivé zainteresované subjekty v zavádzaní potrebných opatrení, spolupracovať s nimi pri tvorbe pravidiel a štandardov, ako aj dostatočne tieto subjekty vzdelávať a zdieľať s nimi príklady z praxe. Podporou a spoluprácou sa štát musí snažiť budovať vzájomnú dôveru zainteresovaných subjektov. Represia a sankcie musia byť prostriedkom „ultima ratio", teda nástrojom, ktorý bude použitý len v krajnom prípade, keď všetky ostatné mechanizmy systému kybernetickej bezpečnosti zlyhajú alebo nebudú mať potrebný účinok.

2.6 Kontinuálne budovanie kapacít v oblasti kybernetickej bezpečnosti

Kybernetický priestor má ako bezpečnostné prostredie nestály a neustále sa vyvíjajúci charakter, v ktorom sa zmeny dejú oveľa dynamickejšie ako vo fyzickom svete. Systém riadenia kybernetickej bezpečnosti však musí pružne reagovať na všetky zmeny, existujúce alebo potenciálne hrozby, ako aj na bezpečnostné výzvy, akými sú moderné technológie a inovatívne služby.

Vplyvom neustále meniaceho sa prostredia je preto nutné kontinuálne budovať kapacity v oblasti kybernetickej bezpečnosti. Táto činnosť zahŕňa najmä posilňovanie odborných personálnych kapacít, vývoj vhodných technických nástrojov ako aj zavádzanie vhodných procesov na riadenie kybernetickej bezpečnosti na všetkých úrovniach.

3. Hrozby

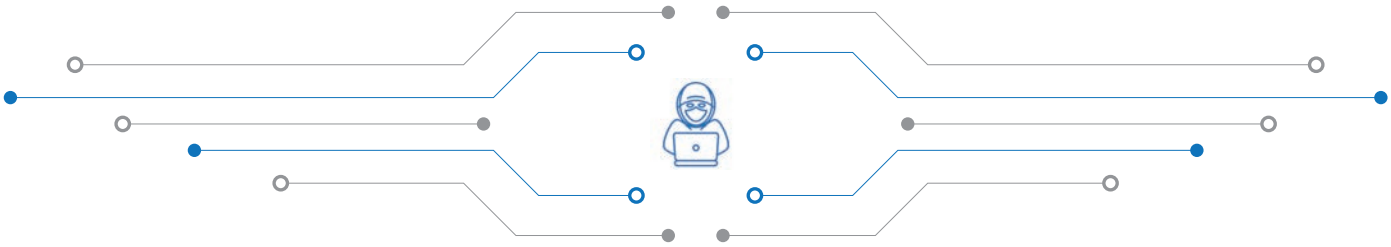
> V kybernetickom priestore sa každodenne objavuje nespočetné množstvo hrozieb, ktoré častokrát prerastú do reálneho útoku. Aj keď tieto hrozby a zraniteľnosti majú rôzny charakter a podobu a ich výpočet je takmer nerealizovateľný, možno pomenovať niekoľko konkrétnych typov hrozieb a zraniteľností, pri ktorých sa dá v strednodobom horizonte predpokladať, že pri ich neriešení môžu byť vážne narušené princípy systému kybernetickej bezpečnosti. Zo strategického hľadiska ide o výzvy, na ktoré je potrebné dostatočne reagovať.

3.1 Neustály rozvoj nových techník a spôsobov útokov

Tak, ako sa vyvíjajú bezpečnostné riešenia, rozvíjajú sa aj nové techniky a spôsoby kybernetických útokov. Možnosti útočníkov a ich nástroje sa neustále vyvíjajú a odpoveď – vhodné bezpečnostné nástroje – môže v mnohých prípadoch prísť neskoro alebo v nedostatočnej sile. Útočníci reagujú v reálnom čase na vzniknuté zraniteľnosti v produktoch a službách, takisto sa neustále zlepšujú v používaní metód sociálneho inžinierstva. Potenciálni útočníci majú navyše časovú výhodu. Príprava na útok, príprava nástrojov, prieskum prostredia, a phishingové kampane môžu hypoteticky trvať rádovo dlhší čas, než ktorý majú k dispozícii obrancovia pri reakcii na prebiehajúci útok. Takisto vzrastá trend predaja útokov a útočných nástrojov (tzv. Hacking as a Service), čo umožňuje aj menej skúseným útočníkom vykonávať sofistikované a devastačné typy útokov.

3.2 Zraniteľní používatelia

Zraniteľnosť nemusí mať len technologický charakter. Tak, ako môže byť zraniteľný počítač alebo server z dôvodu bezpečnostnej diery v softvéri alebo zlej konfigurácie, zraniteľnosť sa môže spôsobiť aj samotný používateľ – napríklad v podobe nedostatočného bezpečnostného povedomia, zanedbania povinností alebo nízkej lojality voči svojmu zamestnávateľovi. Nesprávna interakcia používateľa, nedostatočné zhodnotenie rizík či ignorovanie základných bezpečnostných zásad vedú k tomu, že útočník vie veľmi ľahko preniknúť do systémov organizácie. Môže mu k tomu stačiť jeden zamestnanec, ktorý napríklad otvorí škodlivú prílohu e-mailu alebo klikne na škodlivý odkaz. Nárast digitalizácie na úrovni organizácií prináša problém s nedostatočne rozvinutou kultúrou riadenia rizík a šírenia bezpečnostného povedomia.



3.3 Útoky zamerané na bežných používateľov s (kumulovane) veľkými finančnými stratami

Kybernetické útoky nie sú zamerané len na podnikateľské subjekty a štátne inštitúcie. Citlivo sú vnímané aj útoky na bežných používateľov, jednotlivcov. Rozširovanie škodlivého kódu, phishingové kampane, zber osobných údajov a iné podobné typy útokov pociťujú práve bežní používatelia, pričom jednotlivo môže byť strata pomerne malá, no kumulovane pri jednotlivých typoch útokov so širokým záberom obetí, môže dosiahnuť veľmi vysoké hodnoty.

3.4 Narastajúci počet technologických zraniteľností

Zraniteľnosť je v drvivej väčšine prípadov technickou vstupnou bránou útočníka k obeti po tom, ako mu táto umožní sa k nej dostať. Počet zraniteľností narastá priamo úmerne s rozvojom digitálnej spoločnosti a vývojom technológií. Vývoj väčšiny nových technológií je dynamický, počas ich návrhu sa na bezpečnosť nekladie dostatočný dôraz, keďže pred bezpečnosťou sa uprednostňuje funkcionalita a dizajn. Rovnako nastáva problém aj pri následných aktualizáciách technológií, kde na úkor novej funkcionality vznikajú nové, závažné zraniteľnosti, respektíve technológie strácajú podporu aktualizácií od výrobcu veľmi skoro po ich uvedení na trh, pričom v nich častokrát ostávajú kritické zraniteľnosti. Technické zraniteľnosti sú tiež častou súčasťou narušenia bezpečnosti dodávateľského reťazca, teda ako úmyselné zraniteľnosti zanechané v produkte výrobcom alebo implementované iným aktérom za účelom možného zneužitia tejto zraniteľnosti vo svoj prospech.

3.5 Nedostatok odborného personálu

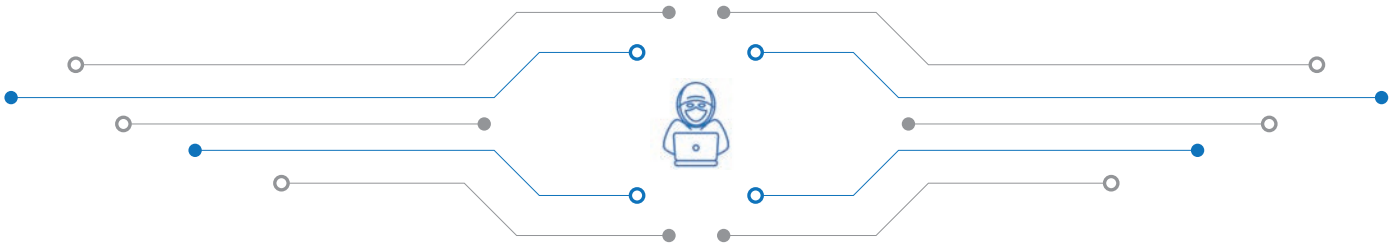
Téma bezpečnosti v organizácii sa nepovažuje za štandard, ale väčšinou len za povinnosť, ktorá musí byť splnená podľa zákona. Z tohto dôvodu jednotlivé subjekty na bezpečnosť vyčleňujú minimálny počet personálu, ktorý mnohokrát nie je dostatočne odborne spôsobilý, nemá dostatok skúseností na riadenie rizík a aplikáciu bezpečnostných opatrení, ako aj nedisponuje dostatočnou podporou vedenia a financovaním svojich aktivít. Častokrát je bezpečnosť v organizácii riešená len formálne „na papieri", pričom nie sú reálne implementované ani základné bezpečnostné opatrenia a zadefinované procesy sa nedodržiavajú alebo obchádzajú bez vyvodenia zodpovednosti.

3.6 Laxný prístup k požiadavkám vyplývajúcich z legislatívy alebo štandardov

Implementácia bezpečnostných opatrení je štandardizovaná operácia, ktorú determinuje zákon, vykonávacie predpisy alebo nelegislatívny štandard. Nedostatočne seriózny prístup k takýmto požiadavkám vedie nielen k samotnému nepochopeniu existencie bezpečnostných opatrení, ale aj k vzniku slabého miesta organizácie, ktorá je tak viac zraniteľná voči útokom zvonka, ale i zvnútra.

3.7 Nízka úroveň bezpečnostného povedomia

Povedomie o nástrahách a rizikách v kybernetickom priestore je oblasťou, ktorá zásadným spôsobom ovplyvňuje postoj používateľov, ktorí doňho vstupujú, k svojej vlastnej bezpečnosti. Absencia záujmu používateľov dbať na svoju bezpečnosť vychádza najmä z toho, že nemajú dostatočné vedomosti a skúsenosti s kybernetickou bezpečnosťou a stávajú sa tak ideálnym cieľom pre útočníkov. Práve tak používatelia často nemajú ani dostatočné vedomosti v oblasti ochrany osobných údajov, čo má za následok ich únik alebo poskytovanie bez potrebného účelu.



3.8 Zneužívanie nových technológií na vykonávanie útokov

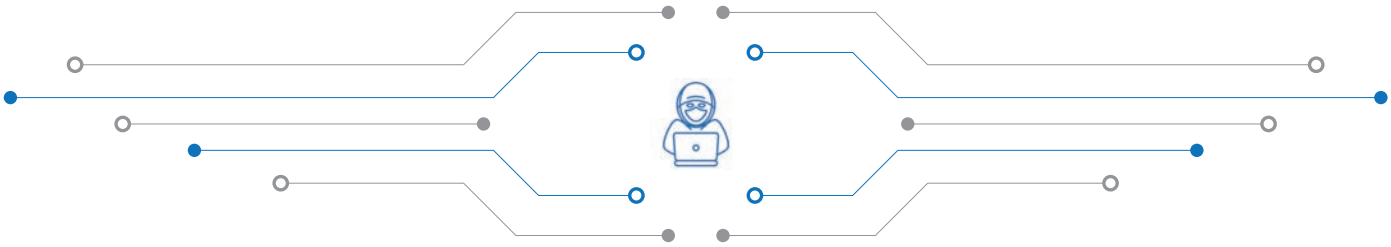
Existencia a ľahšia dostupnosť nových technológií, napríklad aplikácií umelej inteligencie a internetu vecí (IoT), umožňuje útočníkom vykonávanie sofistikovanejších kybernetických útokov, spôsobuje ich väčší dosah a dovoľuje efektívnejšie zahladzovanie stôp po páchateľovi či sťaženie analytických činností pri riešení kybernetického bezpečnostného incidentu.

3.9 Slabá detekcia

Detekcia kybernetických bezpečnostných incidentov, pokusov o útok alebo úspešných útokov je náročný proces, vyžadujúci dostatočnú personálnu a technickú kapacitu. Na národnej úrovni do tohto procesu vstupujú viaceré faktory, od legislatívneho rámca, ktorý štátu umožňujú realizovať aktivity súvisiace s detegovaním incidentov až po ochotu subjektov oznamovať kybernetické bezpečnostné incidenty. Ak úroveň detekcie a hlásenia kybernetických bezpečnostných incidentov nebude kontinuálne rásť, môže prísť k mylným záverom vedúcim k znižovaniu investícií do kybernetickej bezpečnosti a tým k zvýšeniu zraniteľnosti používateľov v kybernetickom priestore.

3.10 Zneužívanie pokročilých techník šifrovania pri kybernetických útokoch

Útočníci využívajú šifrovanie dát a komunikácie vo viacerých rovinách. V prvom rade pri zabezpečení komunikácie vlastnej útočnej infraštruktúry, vrátane zariadení obetí tak, aby bolo veľmi ťažké v reálnom čase takúto komunikáciu dešifrovať a odhaliť jej účel. Šifrovanie sa však využíva aj pri čoraz frekventovanejších útokoch typu ransomvér, pri ktorých útočník zašifruje dáta obete tak, aby k nim nemala prístup. To môže spôsobiť nielen nedostupnosť dát, ale aj služieb, ktoré sú na zariadeniach poskytované.



3.11 Pomalý výkon trestného práva v oblasti počítačovej kriminality s neistým výsledkom

Pojem počítačová kriminalita, alebo kybernetická kriminalita nie je explicitne definovaný v Trestnom zákone alebo v obdobnom normatívnom právnom akte. Platný Trestný zákon však definuje niektoré skutkové podstaty trestných činov, ktoré spoločne tvoria počítačovú kriminalitu. Na účely trestnoprávnej praxe sa používa definícia obsiahnutá v Dohovore Rady Európy o počítačovej kriminalite ratifikovaný Slovenskou republikou.

Nie každý kybernetický bezpečnostný incident je skutkom počítačovej kriminality, no každý skutok počítačovej kriminality je kybernetickým bezpečnostným incidentom. Statistické systémy orgánov činných v trestnom konaní však nedostatočne evidujú trestné činy pre skutkové podstaty trestných činov v oblasti počítačovej kriminality, čo znižuje reálny pohľad na rozsah tohto druhu trestnej činnosti. To má za následok nie len pomalý vývoj trestného práva v oblasti počítačovej kriminality, ale aj poddimenzovanie personálneho stavu, ktorý má takúto trestnú činnosť odhaľovať a objasňovať.

Nedostatočná spôsobilosť vyšetrovateľov pre vyšetrovanie trestných činov v oblasti počítačovej kriminality spolu s pomalým špecializovaným systémom vzdelávania orgánov činných v trestnom konaní a sudcov vedie k nedostatočnej rýchlosti trestného konania, čo častokrát znižuje šancu odhaliť páchateľa počítačovej trestnej činnosti. Tomu napomáha aj nedostatok znalcov a znaleckých organizácií zapísaných v príslušných znaleckých odvetviach. Ďalším závažným problémom je, že značný počet trestných činov spojených s počítačovou kriminalitou nie je obeťami oznamovaný, čo takisto prináša skreslený pohľad na rozsah takejto kriminality v slovenskom kybernetickom priestore.

3.12 Útoky na kritickú infraštruktúru štátu, orgány štátu a obranné mechanizmy s mocensko-politickým pozadím

Kybernetické útoky sa čoraz častejšie stávajú nástrojom mocenského súperenia medzi štátmi. Útoky štátnych, ale aj neštátnych aktérov na kritické aktíva a štátne inštitúcie, sú reálnou hrozbou, ktorá môže vážne narušiť spôsobilosti štátu v oblasti bezpečnosti, narušiť spoločenskú stabilitu alebo spôsobiť vysoké ekonomické a hospodárske škody. Kybernetické útoky sú takisto nástrojom špionáže, ktorej účelom je získavať citlivé alebo utajované informácie cudzieho štátu a získať nad ním ekonomickú, vojenskú alebo inú prevahu. Čoraz viac štátov buduje ofenzívne spôsobilosti v kyberpriestore, čo im umožňuje získať mocenskú alebo politickú prevahu.

3.13 Nelegálne aktivity, presahujúce kybernetický priestor

Kybernetický priestor je využívaný aj na spektrum aktivít, ktoré ho presahujú. Ide napríklad o šírenie detskej pornografie, prevádzka elektronických obchodov s nelegálnym a zakázaným tovarom, šírenie toxikománie či extrémistických materiálov, ako aj dezinformácií a propagandy. Kybernetický priestor je síce len prostriedkom na šírenie a zdieľanie takéhoto obsahu, no nedostatočné riešenie tejto problematiky na strategickej úrovni vedie k nekontrolovanému a rozsiahlemu šíreniu nelegálneho obsahu. Kybernetický priestor je takisto doménou v rámci hybridných hrozieb, ktoré sú spôsobilé ohroziť základné fungovanie štátnych procesov, oslabiť dôveru občanov v štát alebo narušiť verejný poriadok.

4. Strategické ciele

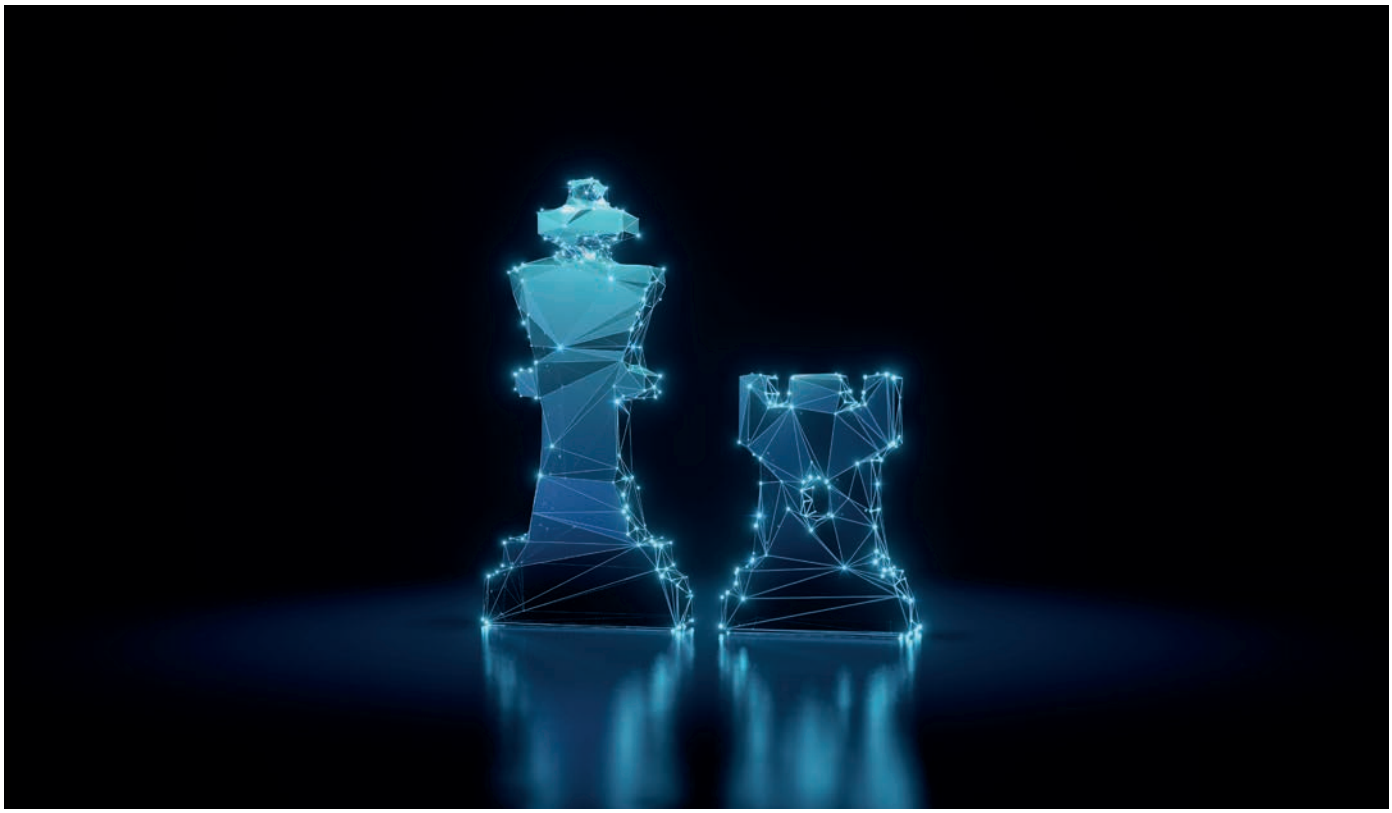
Riadenie systému kybernetickej bezpečnosti nevyžaduje len dobre nastavené pravidlá a vykonávanie potrebných bezpečnostných opatrení. Na národnej úrovni musí byť kybernetická bezpečnosť vnímaná ako strategický záujem štátu, ktorý chráni nielen štátne aktíva, ale taktiež ako jedna z kľúčových služieb, ktorú poskytuje štát svojim občanom a podnikateľským subjektom. Samotné vykonávanie aktivít štátu v oblasti kybernetickej bezpečnosti musí byť založené predovšetkým na základných strategických princípoch a zároveň musí nadčasovo reflektovať hrozby, ktoré ohrozujú a môžu ohroziť kybernetickú bezpečnosť a systém, ktorý ju na národnej úrovni riadi.

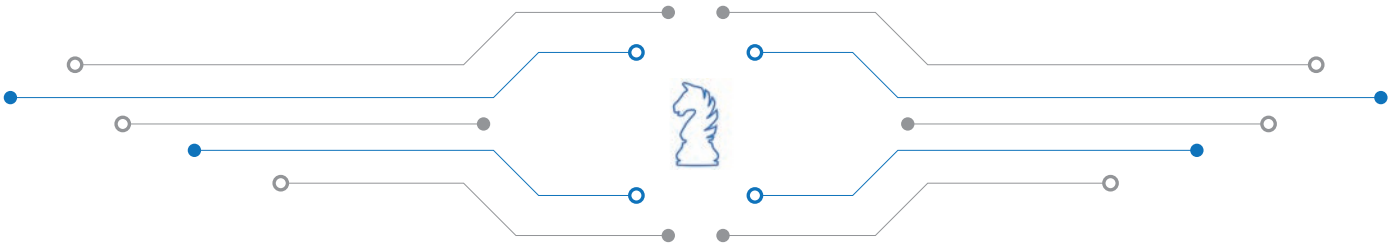
Aby mohli byť naplnené strategické princípy kybernetickej bezpečnosti a reakcia na hrozby bola dostatočná, musia byť určené jednoznačné a merateľné strategické ciele, pričom po ich naplnení bude možné objektívne zhodnotiť ich dopad na zlepšenie systému kybernetickej bezpečnosti v Slovenskej republike.

Na základe strategických princípov a definovaných hrozieb boli určené nasledujúce strategické ciele.

4.1 Dôveryhodný štát pripravený na hrozby

Kybernetická bezpečnosť je zodpovednosťou každého obyvateľa Slovenskej republiky, no bezpečnosť nemôže fungovať bez existencie mechanizmov na národnej úrovni, ktoré určujú politiku kybernetickej bezpečnosti, systém jej riadenia, ale aj procesy na detekciu a riešenie kybernetických bezpečnostných incidentov, budovanie odborných kapacít a šírenie situačného a bezpečnostného povedomia. Zároveň štát musí pri budovaní dôveryhodnosti vykonávať vyššie uvedené aktivity v súlade s Ústavou Slovenskej republiky a ostatnými zákonmi a vstupovať do základných ľudských práv a slobôd len v nevyhnutnej miere.





4.1.1 Východiskový stav

Štát postupne buduje kapacity a spôsobilosti v oblasti kybernetickej bezpečnosti, pričom rieši najmä nedostatok odborného personálu.

Štát sa spolieha na samotného občana ako koncového používateľa akýchkoľvek služieb v oblasti bezpečnosti, pričom mu neposkytuje dostatočné informácie, ako tieto služby bezpečne používať.

Štát postupne rozvíja kompetencie a spôsobilosti v oblasti certifikácie výrobkov, procesov a služieb v oblasti kybernetickej bezpečnosti.

Štát postupne buduje spôsobilosti na detekciu a riešenie kybernetických bezpečnostných incidentov, pričom sa zameriava na budovanie spôsobilostí najmä na národnej, nie sektorovej úrovni.

Neexistuje jednotný proces na atribúciu kybernetických bezpečnostných incidentov a následné diplomatické a právne mechanizmy.

Detekcia incidentov v jednotlivých sektoroch a kritickej infraštruktúre a ich následné hlásenie autoritám má veľké nedostatky, čím sa znižuje viditeľnosť a vedomosť autority pre kybernetickú bezpečnosť o stave kybernetickej bezpečnosti.

Štát postupne buduje spôsobilosti na posudzovanie zhody a audit kybernetickej bezpečnosti.

Riadenie rizík kybernetickej bezpečnosti v jednotlivých sektoroch sa vykonáva nesystematicky alebo sa nevykonáva vôbec.

4.1.2 Cieľový stav

> Vybudovanie dostatočného odborného personálneho základu pre systém riadenia informačnej a kybernetickej bezpečnosti nielen na národnej, ale aj sektorovej úrovni.

Spolupráca štátu s občanom na úrovni poskytovania dostatočných informácií a odporúčaní a realizácia krokov, ktoré občan reálne pocíti ako zvýšenie vlastnej bezpečnosti a bezpečnosti národného kybernetického priestoru.

Vytvorenie a používanie certifikačných schém na široké portfólio typov výrobkov, procesov a služieb.

Kvalitnejšie technické, organizačné a personálne zabezpečenie, založené na využívaní moderných prístupov ku kybernetickej bezpečnosti pri detekcii a riešení kybernetických bezpečnostných incidentov.

Vybudovanie spôsobilostí na detekciu a riešenie kybernetických bezpečnostných incidentov na všetkých úrovniach.

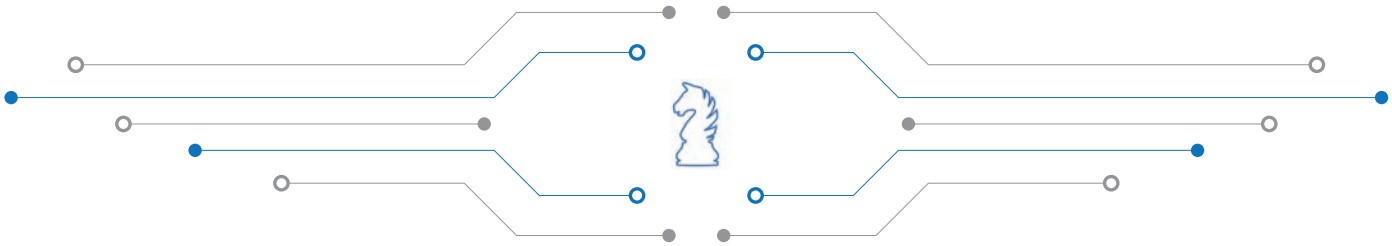
Efektívna spolupráca zainteresovaných subjektov na všetkých úrovniach riešenia informačnej a kybernetickej bezpečnosti.

Dobre nastavený proces technickej, ale aj politickej atribúcie kybernetických bezpečnostných incidentov.

Systematické a kontinuálne riadenie rizík kybernetickej bezpečnosti v jednotlivých sektoroch.

Zlepšenie detekcie a zisťovania kybernetických bezpečnostných incidentov na sektorovej úrovni, zlepšenie a zjednodušenie nahlasovania kybernetických bezpečnostných incidentov nielen zo strany povinných subjektov, ale aj v rovine dobrovoľných hlásení.

Podpora spôsobilostí subjektov v oblasti riadenia kontinuity činností.



4.1.3 Cesta k cieľovému stavu

Pre dosiahnutie cieľového stavu tohto strategického cieľa je potrebné zamerať sa na:

- vytvorenie konceptu „bezpečného internetu pre všetkých", v ktorom sa kombinuje enormné úsilie štátu zabezpečiť vysokú mieru kybernetickej bezpečnosti so zodpovednosťou jednotlivca za realizáciu aktivít smerujúcich k jeho vlastnej bezpečnosti,
- flexibilná reakciu štátu na nové technológie tak, aby bola vždy vykonaná analýza rizík a definované možné bezpečnostné dopady týchto technológií na základné a kritické aktíva štátu, ako aj na samotného občana,
- prípravu legislatívnych návrhov v znení, ktoré bude zrozumiteľné, reálne aplikovateľné a nebudú prinášať povinným subjektom cieľu neúmerné ekonomické, personálne alebo organizačné náklady,
- zjednotenie existujúcich regulácií v oblasti kybernetickej bezpečnosti tak, aby jednotlivé subjekty nemuseli aplikovať viacero právnych predpisov v rovnakej problematike,
- vedenie odborného dialógu štátu so zainteresovanými stranami a odbornými združeniami pri zmene legislatívy a pravidiel regulácie,
- zavedenie funkčných procesov riadenia rizík kybernetickej bezpečnosti,
- rozvoj certifikácie ako nástroja pre dôveryhodnejšie výrobky, procesy a služby v oblasti kybernetickej bezpečnosti,
- implementáciu európskych certifikačných schém v oblasti kybernetickej bezpečnosti do národných certifikačných postupov,
- uplatňovanie ucelenej koncepcie krízového riadenia v oblasti kybernetickej bezpečnosti s prepojením na integrované vnútroštátne a medzinárodné mechanizmy,
- kontinuálne posilňovanie technických, organizačných a personálnych kapacít pre detekciu a riešenie kybernetických bezpečnostných incidentov na národnej úrovni a v rámci jednotlivých sektorov, vrátane kritickej infraštruktúry,
- rozvoj schopností v oblasti detekcie a zberu bezpečnostne relevantných udalostí v národnom kybernetickom priestore, ako aj rozvoj schopností v oblasti vyhodnocovania udalostí a detekcie incidentov modernými technikami v národnom kybernetickom priestore rôznymi formami, algoritmami a technológiami, vrátane umelej inteligencie,
- rozvoj schopností v oblasti riešenia bezpečnostných incidentov a automatizácie procesov v tejto oblasti s využitím moderných technológií strojového učenia, ako aj rozvoj schopností reagovať na závažné bezpečnostné incidenty na mieste, u poskytovateľov základných služieb s potrebným vybavením a kapacitami,
- zjednotenie existujúcich eskalačných procedúr pre ohlasovanie incidentov tak, aby jednotlivé subjekty nemuseli aplikovať viacero právnych predpisov v rovnakej problematike,
- vytvorenie procesu technickej a politickej atribúcie incidentov spolu s určením zodpovedných inštitúcií a právnych mechanizmov a mechanizmov kybernetickej diplomacie,
- posilňovanie analytických kapacít v oblasti bezpečnostných hrozieb so špecializáciou na atribúciu kybernetických bezpečnostných incidentov,
- efektívny výkon aktívneho aj pasívneho kybernetického spravodajstva zameraného na získavane, sústreďovanie a vyhodnocovanie informácií o aktivitách v kybernetickom priestore ohrozujúcich bezpečnosť Slovenskej republiky,
- nastavenie pravidiel a využívanie inštitútu blokovania škodlivého obsahu, najmä riadiacich serverov útočníkov, zariadení šíriacich škodlivý kód a zariadení útočiacich na cudziu infraštruktúru za účelom zneprístupnenia služby,
- pri poskytovaní služieb v oblasti kybernetickej bezpečnosti dbať na ich efektivitu a opodstatnenosť pre občana,
- nastavenie funkčného systému kontinuálneho budovania odborných personálnych kapacít,
- Vypracovanie koncepcie vzdelávania personálu vo verejnej správe zameranú na prijímanie, udržanie, zabezpečenie a kariérny rast, ako aj zvyšovanie a udržiavanie jeho odbornej spôsobilosti,
- Vytvorenie vhodných motivačných a odmeňovacích nástrojov pre odborný personál vo verejnej správe s cieľom vyrovnať podmienky verejnej správy a súkromného sektora.

4.2 Efektívne odhaľovanie a objasňovanie počítačovej kriminality

Počet kybernetických bezpečnostných incidentov, ktoré sú aj trestnými činmi počítačovej kriminality neustále narastá. Útočníci sú sofistikovanejší a útoky ťažšie odhaliteľné. Obetiam vznikajú veľké škody, častokrát ohrozujúce ich ekonomickú existenciu. Kybernetické útoky sú veľmi dobre organizované a načasované a útočníci väčšinou veľmi dobre po sebe zametú stopy a ich odhalenie je veľmi náročné. Atribúcia útočníkov je veľmi náročný proces, ktorý si vyžaduje dostatočné personálne kapacity a dobre nastavené procesy.

4.2.1 Východiskový stav

Počítačová kriminalita, resp. trestné činy počítačovej kriminality sú síce v legislatíve ustálené, no praktický výkon práva v tejto oblasti naráža na legislatívne prekážky, ktoré sťažujú operatívne odhaľovanie a objasňovanie tohto druhu kriminality.

Trestné činy počítačovej kriminality častokrát nie sú oznamované a preto nie je viditeľný reálny rozsah tohto druhu kriminality na národnej úrovni.

Legislatíva na medzinárodnej úrovni nie je zjednotená.

Orgány činné v trestnom konaní nemajú dostatočné kapacity na boj proti počítačovej kriminalite, a to najmä na úrovni základných útvarov pri oznamovaní takéhoto druhu trestnej činnosti.

Na národnej úrovni funguje Národná expertná skupina pre boj proti počítačovej kriminalite, ktorá združuje štátne organizácie aj niektoré organizácie zo súkromného sektora.

Existuje vnútroštátna sieť prokurátorov na boj proti počítačovej kriminalite. Slovenská prokuratúra je zapojená aj v Európskej justičnej sieti na boj proti počítačovej kriminalite, spolupracuje s Eurojustom a ostatnými národnými a medzinárodnými organizáciami.

Vzdelávanie v oblasti počítačovej kriminality prebieha prostredníctvom špecifických aktivít prokuratúry, policajného zboru a Justičnej akadémie Slovenskej republiky.

4.2.2 Cieľový stav

Dostatočné kapacity vyčlenené na boj proti počítačovej kriminalite, efektívna spolupráca zainteresovaných subjektov, rýchlosť trestného konania, adekvátna potrebám odhaľovania a objasňovania počítačovej kriminality.

Viac oznámených a vyšetrených trestných činov počítačovej kriminality.

Lepšia koordinácia postupov v oblasti počítačovej kriminality a ich zjednotenie na medzinárodnej úrovni.

Aktívna spolupráca v oblasti počítačovej kriminality medzi zainteresovanými subjektami na národnej úrovni a zdieľanie relevantných informácii.

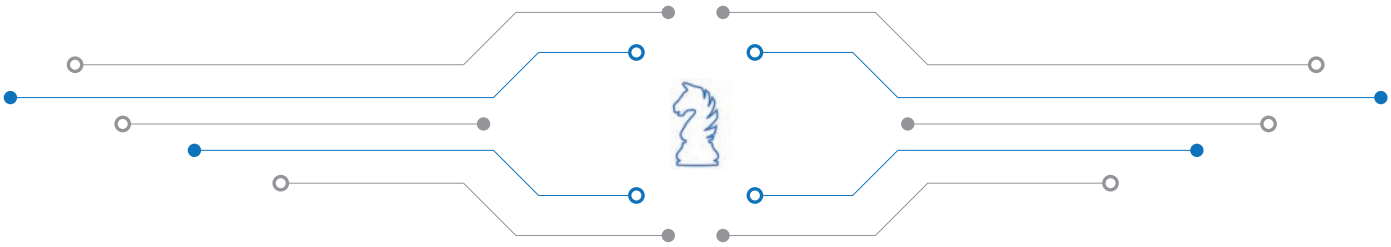
Špecializácia orgánov činných v trestnom konaní v oblasti počítačovej kriminality od základných útvarov polície až po prokuratúru a súdy.

Rozvoj vzdelávacích aktivít v oblasti počítačovej kriminality.

4.2.3 Cesta k cieľovému stavu

Pre dosiahnutie cieľového stavu tohto strategického cieľa je potrebné zamerať sa na:

- zefektívnenie a zrýchlenie operatívnych a vyšetrovacích postupov v oblasti odhaľovania a objasňovania kybernetickej kriminality,
- vyčlenenie dostatočných personálnych kapacít na riešenie kybernetickej kriminality na úrovni krajov a okresov tak, aby existoval dostatočný počet špecialistov spomedzi operatívnych pracovníkov, vyšetrovateľov, prokurátorov a sudcov špecializovaných na túto oblasť,
- zlepšovanie spolupráce subjektov, ktoré sú zainteresované v oblasti kybernetickej kriminality,
- zrýchlenie reakcie právneho systému na novovznikajúce hrozby v oblasti kybernetickej kriminality,
- zadefinovanie pojmu počítačová kriminalita do trestného zákona,
- Pokračovanie dialógu o zjednotení procesov v oblasti kybernetickej kriminality na medzinárodnej úrovni,
- zdokonalenie rámca vzdelávania pre orgány činné v trestnom konaní a súdy v oblasti kybernetickej kriminality,
- kontinuálne zvyšovanie bezpečnostného povedomia v oblasti kybernetickej kriminality so zameraním sa na široké vrstvy obyvateľstva a najzraniteľnejšie skupiny (deti, seniori).



4.3 Odolný súkromný sektor

Prevádzkovatelia základných služieb v súkromnom sektore sú nosným prvkom poskytovania širokého portfólia služieb pre občanov, súkromný sektor ale aj verejnú správu. Prvky kritickej infraštruktúry sú podľa zákona o kybernetickej bezpečnosti a zákona o kritickej infraštruktúre automaticky základnými službami a ich prevádzkovatelia sú prevádzkovateľmi základných služieb. Tieto služby a ich prevádzkovatelia sú pre zabezpečenie bezproblémového chodu spoločnosti mimoriadne kritické. Ide o spoločnosti, ktoré majú veľký počet zákazníkov alebo významný ekonomický vplyv, významné postavenie pri ochrane života a zdravia ľudí, vplyv na verejný poriadok a bezpečnosť a vplyv na mobilitu osôb alebo transport tovaru. Ich bezpečnosť je teda dôležitým faktorom, umožňujúcim nie len kontinuálne poskytovanie dôležitých služieb, ale aj ich rozvoj.

4.3.1 Východiskový stav

Existujú veľké rozdiely v oblasti kybernetickej bezpečnosti a implementácie bezpečnostných opatrení prevádzkovateľov základných služieb naprieč rôznymi sektormi. Prevádzkovatelia základných služieb aj v súkromnom sektore berú kybernetickú reguláciu len ako ďalšiu zákonnú povinnosť. Prevádzkovatelia základných služieb vo veľkej miere pristupujú k aplikácii zodpovedajúcich bezpečnostných opatrení nevýrazne, čo pramení najmä z ich slabého bezpečnostného povedomia v oblasti kybernetickej a informačnej bezpečnosti.

Zákon o kybernetickej bezpečnosti má prierezový charakter naprieč všetkými sektormi a preto prináša len minimálne bezpečnostné požiadavky, ktoré sú implementovateľné jednotne vo všetkých sektoroch. Tieto jednotné minimálne požiadavky ale nie sú vo viacerých sektoroch dostatočné.

4.3.2 Cieľový stav

> Adresné sektorové bezpečnostné požiadavky doplňujúce základné minimálne požiadavky zo zákona zabezpečujúce kybernetická bezpečnosť na vysokej úrovni s ohľadom na sektorové potreby a špecifiká.

Povedomie prevádzkovateľov základných služieb a prevádzkovateľov kritickej infraštruktúry v súkromnom sektore o kybernetickej bezpečnosti ako o základnej súčasti ich fungovania, nie len ako o ďalšej regulácii zo strany štátu.

Dobre fungujúca spolupráca verejného a súkromného sektora nie len v oblasti regulácie, ale najmä pri zdieľaní bezpečnostných informácii, skúseností a aj v oblasti ďalšieho rozvoja.

4.3.3 Cesta k cieľovému stavu

Pre dosiahnutie cieľového stavu tohto strategického cieľa je potrebné zamerať sa na:

- adresný prístup k jednotlivým sektorom v oblasti kybernetickej bezpečnosti so zameraním sa na špecifiká jednotlivých sektorov,
- poskytovanie podpory prevádzkovateľom základných služieb aj prevádzkovateľom kritickej infraštruktúry v súkromnom sektore pri aplikácii vhodných bezpečnostných opatrení,
- rozvoj efektívnej spolupráce, zdieľania informácii a odbornej diskusie verejného sektora so súkromným sektorom.

4.4 Kybernetická bezpečnosť ako základná súčasť verejnej správy

V kybernetickom priestore musia dobre fungovať nielen služby súkromných spoločností, ale aj tie poskytované štátom. Služby, ktoré štát ponúka svojim občanom, musia byť dostatočne zabezpečené, aby nedošlo k zneužitiu citlivých alebo osobných údajov v kontexte Nariadenia Európskeho parlamentu a Rady (EÚ) č. 2016/679. Osobitnou kategóriou prevádzkovatelia základných služieb prevádzkované v rámci verejnej správy, ktorých bezpečnosť musí byť základnou súčasťou ich samotnej existencie.

4.4.1 Východiskový stav

Prevádzkovatelia základných služieb vo verejnom sektore na povinnosť aplikácie vhodných bezpečnostných opatrení častokrát reagujú vágne, čo je spôsobené najmä nedostatočnou úrovňou bezpečnostného povedomia prevádzkovateľov a ich dodávateľov v oblasti kybernetickej a informačnej bezpečnosti. Kybernetická bezpečnosť vo verejnej správe má doplnkovú bezpečnostnú reguláciu určenú zákonom o informačných technológiách verejnej správy, táto regulácia však často tiež nie je implementovaná alebo dostatočne impolementovaná. Pri dizajne IT infraštruktúry štátu sa väčšinou nedodržiavali resp. nedodržiavajú bezpečnostné pravidlá a pri jej prevádzke je situácia rovnaká.

Bezpečnosť elektronických služieb štátu nie je dlhodobo vyhodnocovaná a občanovi sa aspekt bezpečnosti neprezentuje dostatočne.

4.4.2 Cieľový stav

> Pravidlo „security by design" ako povinné pri návrhu, obstarávaní, tvorbe, implementácii a prevádzke systémov a služieb štátu.

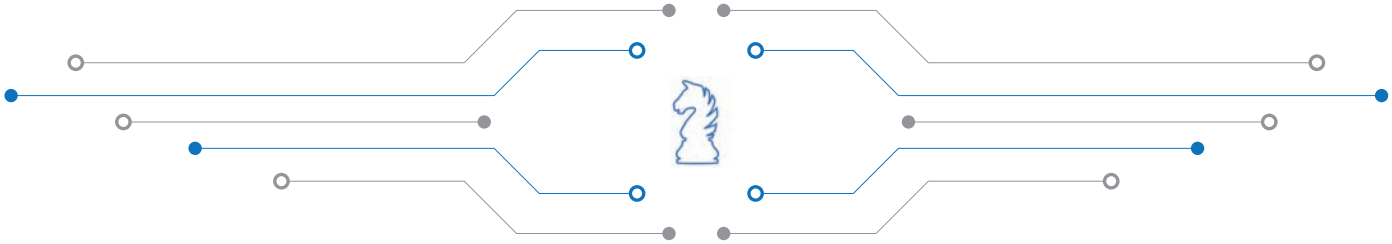
Občan musí vnímať, že služby poskytované štátom, ale aj jeho vlastné aktivity, sú bezpečné.

Riadenie rizík kybernetickej a informačnej bezpečnosti vo verejnej správe musí byť funkčný proces minimalizujúci riziká vo všetkých fázach životného cyklu systémov od prípravy špecifikácie, obstarávania, návrhu architektúry, implementácie, prevádzky a údržby až po vyraďovanie z používania. Riadenie kybernetickej a informačnej bezpečnosti musí byť prirodzená súčasť riadenia informačných systémov verejnej správy.

4.4.3 Cesta k cieľovému stavu

Pre dosiahnutie cieľového stavu tohto strategického cieľa je potrebné zamerať sa na:

- uplatňovanie systematického prístupu ku kybernetickej bezpečnosti založeného na analýze a riadení rizík v každej dôležitej oblasti, pričom každá analýza musí vychádzať z plánu a metodiky jednotnej analýzy a riadenia rizík,
- doplnenie odborných kapacít vo verejnej správe,
- zvýšenie ochrany prevádzkovateľov základných služieb vo verejnej správe z hľadiska kybernetickej bezpečnosti tak, aby ich audit a pravidelné kontroly vykonávaných opatrení trvalo preukazovali pozitívny trend zlepšovania stavu kybernetickej bezpečnosti vo verejnej správe,
- poskytovanie bezpečných a dostupných elektronických služieb štátu každému občanovi s umožnením plnohodnotného rovného využitia elektronických nástrojov,
- poskytovanie kontinuálnej a komplexnej podpory riešenia a riadenia kybernetickej bezpečnosti organizáciám verejnej správy z centrálnej úrovne,
- skvalitnenie procesu návrhu, obstarávania, tvorby, implementácie a prevádzky IT infraštruktúry štátu, od začiatku dbať na kybernetickú bezpečnosť tak, aby neprichádzalo k vzniku zraniteľností alebo hrozieb pri používaní týchto služieb (dbať na zásadu „security by design"),
- nastavenie pravidiel bezpečnosti dodávateľského reťazca pre štátnu IT infraštruktúru tak, aby nedochádzalo k nepredpokladaným bezpečnostným incidentom a dodávateľ nezískal špecifické resp. výhradné postavenie, ktoré by mohlo ohroziť bezpečnosť prevádzky IT infraštruktúry štátu.



4.5 Silné partnerstvá

Bezpečnosť všeobecne je jeden z primárnych záujmov každého demokratického a právneho štátu. Oblasť kybernetickej bezpečnosti nie je výnimkou, pričom je viac globalizovaná, keďže kybernetické útoky nepoznajú hranice štátov a útočníci nemusia byť explicitne len občania krajiny, v ktorej útok prebieha. Preto je veľmi dôležité, aby štát vytváral na medzinárodnej úrovni veľmi silné partnerstvá, vymieňal si skúsenosti, vedomosti a informácie a tie potom následne aplikoval na národnej úrovni. Vzájomná spolupráca a posilňovanie dôvery medzi subjektami verejnej správy, súkromného sektora a akademickej obce zabezpečujú rozvoj v oblasti kybernetickej bezpečnosti.

4.5.1 Východiskový stav

Štát postupne buduje a udržiava vzťahy v oblasti kybernetickej bezpečnosti, najmä na úrovni Európskej únie (EÚ), Organizáciu spojených národov (OSN), Severoatlantickej aliancie (NATO), Rade Európy a Organizácie pre bezpečnosť a spoluprácu v Európe (OBSE). Takisto má uzatvorené bilaterálne memorandá s niektorými konkrétnymi štátmi a podporuje vybrané medzinárodné iniciatívy s cieľom posilňovania medzinárodnej kybernetickej bezpečnosti.

Slovenská republika aktívne participuje na procesoch tvorby politík a strategických dokumentov v medzinárodnom prostredí. Zapája sa aj do spoločných mechanizmov na budovanie dôvery a kapacít.

Národné centrum kybernetickej bezpečnosti SK-CERT je členom európskej siete národných CSIRT jednotiek, v ktorej aktívne pôsobí. Rôzne slovenské CSIRT jednotky sú členmi medzinárodných CSIRT organizácií, v ktorých aj aktívne pôsobia.

Na národnej úrovni štát buduje vzťahy s prevádzkovateľmi základných služieb a poskytovateľmi digitálnych služieb prostredníctvom formálnych aj neformálnych kanálov.

Štát aktívne pôsobí prostredníctvom svojich zástupcov aj v Európskej agentúre pre kybernetickú bezpečnosť (ENISA) a rozvíja pôsobenie v sieti národných kompetenčných centier kybernetickej bezpečnosti.

Slovenská republika aktívne spolupracuje s Centrom excelentnosti NATO pre kooperatívnu kybernetickú obranu.

4.5.2 Cieľový stav

Slovenská republika ako rešpektovaný štát s dobrou reprezentáciou v zahraničí prostredníctvom odborne zdatných zástupcov na technickej aj politickej úrovni.

Na národnej úrovni vytvorená zdravá a silná partnerská sieť medzi štátnymi orgánmi, štátom a súkromným sektorom a takisto aj s akademickou obcou a odbornou verejnosťou.

Na Európskej úrovni vytvorená sieť kompetenčných centier kybernetickej bezpečnosti so zapojením slovenského Kompetenčného a certifikačného centra kybernetickej bezpečnosti ako národného zástupcu v správnej rade európskych kompetenčných centier.

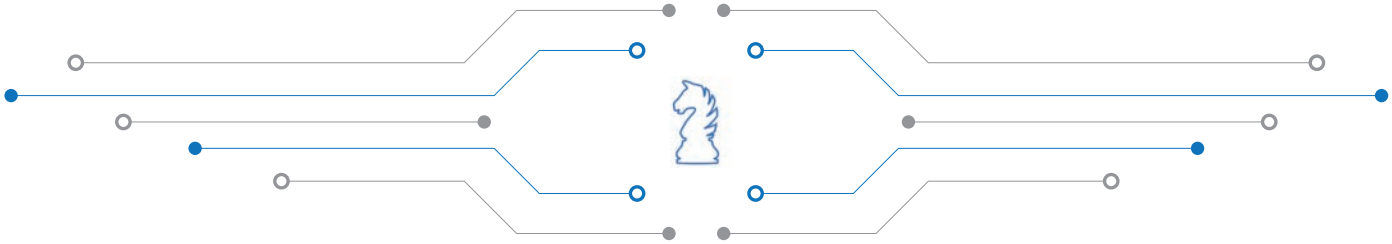
Intenzívnejšie zapojenie Slovenskej republiky do aktivít Európskej organizácie kybernetickej bezpečnosti (ECSO).

Definovanie hlavných zahraničnopolitických partnerov v oblasti kybernetickej bezpečnosti.

4.5.3 Cesta k cieľovému stavu

Pre dosiahnutie cieľového stavu tohto strategického cieľa je potrebné zamerať sa na:

- posilňovanie existujúcich medzinárodných partnerstiev a vytváranie nových, najmä so štátmi, ktorých politický a bezpečnostný systém je založený na slobode a demokracii,
- rozvoj politickej spolupráce v oblasti kybernetickej bezpečnosti,
- rozvoj kybernetickej diplomacie prostredníctvom budovania pozícií tzv. kyber-atašé, ako aj využívaním aktuálnych kapacít zastupiteľských úradov SR v zahraničí,
- budovanie silných partnerstiev na národnej úrovni medzi jednotlivými zainteresovanými štátnymi orgánmi,
- aktívne pôsobenie v medzinárodnom prostredí zamerané na presadenie noriem zodpovedného správania sa v kybernetickom priestore,
- rozvoj spolupráce štátu s prevádzkovateľmi základných služieb a poskytovateľmi digitálnych služieb,
- budovanie spolupráce štátu so súkromným sektorom, najmä so spoločnosťami, ktoré sa zameriavajú na riešenia v oblasti kybernetickej bezpečnosti a inovatívne technológie,
- prehlbovanie partnerstva štátu s akademickou obcou,
- posilňovanie výmeny informácií a skúseností s partnermi, vytváranie organizačných a technických platforiem,
- zriadenie a udržiavanie národnej CSIRT siete, ktorá bude združovať slovenské CSIRT jednotky (spravované štátom aj súkromné),
- zapojenie Kompetenčného a certifikačného centra kybernetickej bezpečnosti ako národného zástupcu v správnej rade európskych kompetenčných centier,
- zriadenie a koordináciu sektorových ISAC,
- úzku spoluprácu s autoritou pre kybernetickú obranu štátu, ktorou je Centrum pre kybernetickú obranu Slovenskej republiky,
- prehlbovanie spolupráce štátov v oblasti kybernetickej bezpečnosti so zameraním sa na tvorbu záväzných bezpečnostných štandardov pre výrobcov informačných technológií,
- zintenzívnenie informovanosti a komunikácie s verejnosťou v oblasti priorít kybernetickej bezpečnosti.



4.6 Vzdelaní odborníci a vzdelaná verejnosť

V oblasti kybernetickej bezpečnosti je vzdelávanie jednou z hlavných oblastí, ktoré umožňujú rozvoj a lepšie schopnosti pri komplexných činnostiach systému kybernetickej bezpečnosti. Situačné a bezpečnostné povedomie, budované smerom k bežným používateľom, pôsobí preventívne proti vzniku kybernetických bezpečnostných incidentov, pretože vzdelaný používateľ vie lepšie reagovať na bezpečnostné hrozby a riziká v kybernetickom priestore a správa sa dostatočne zodpovedne na to, aby nedochádzalo z dôvodu jeho slabého povedomia k úspešným útokom. Je dôležité chápať zvyšovanie bezpečnostného povedomia ako celkový pedagogický proces, kedy vzdelávaná osoba problematike nielen porozumie, ale sa s ňou aj stotožní.

4.6.1 Východiskový stav

Odborné vzdelávanie v oblasti kybernetickej bezpečnosti nie je systematicky riešené, existuje veľmi málo vysokoškolských programov kybernetickej bezpečnosti. S tým súvisí aj nedostatok učiteľov v témach kybernetickej bezpečnosti. Na komerčnom trhu je viacero odborných kurzov a školení, no tie nedokážu nahradiť systematické vzdelávanie.

Absentuje budovanie bezpečnostného povedomia a základného bezpečnostného vzdelania v oblasti bezpečného správania sa na internete už od primárneho vzdelávania až po stredné školstvo, pričom už na týchto úrovniach vzniká veľké množstvo používateľov technológií.

Vzdelávanie zamestnancov verejnej správy nie je systematické, neexistuje systém základného bezpečnostného vzdelávania pre úradníkov verejnej správy, ktorí denne pracujú s informačnými systémami verejnej správy a prichádzajú do kontaktu s citlivými a osobnými údajmi.

Vzdelávaniu a šíreniu bezpečnostného povedomia v oblasti kybernetickej bezpečnosti na rôznych stupňoch vzdelávania a v rôznych sektoroch sa v decentralizovanej forme venuje súkromný a tretí sektor.

Situačné a bezpečnostné povedomie je budované nesystematicky, častokrát len vo forme reakcie na aktuálne vzniknuté problémy, pričom má malý dosah.

4.6.2 Cieľový stav

> Trvalo udržateľný systém odborného vysokoškolského vzdelávania a odborného špecializovaného vzdelávania ako formy ďalšieho vzdelávania v oblasti kybernetickej a informačnej bezpečnosti.

Koncept základného bezpečnostného vzdelávania na všetkých úrovniach vzdelávania, od základných škôl až po vysoké školstvo.

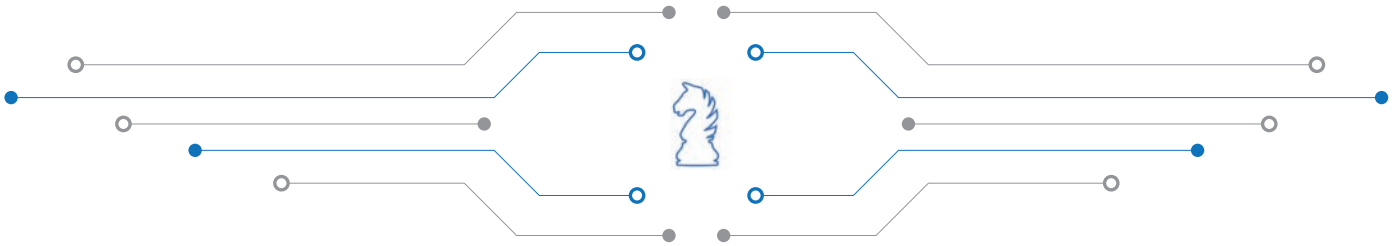
Systematické, širokospektrálne a plánované šírenie situačného a bezpečnostného povedomia založeného na dobrom systéme, ktorý bude flexibilne reagovať na zmeny v kybernetickom priestore.

Vzdelaní zamestnanci verejnej správy, ktorí vedia bezpečne poskytovať služby a používať systémy verejnej správy bez vzniku kybernetických bezpečnostných incidentov, ktoré vznikli kvôli ich nízkemu bezpečnostnému povedomiu.

4.6.3 Cesta k cieľovému stavu

Pre dosiahnutie cieľového stavu tohto strategického cieľa je potrebné zamerať sa na:

- vytvorenie systému odborného vysokoškolského a stredoškolského vzdelávania, ktoré zabezpečí výchovu nových odborníkov,
- vytvorenie systému odborného špecializovaného vzdelávania pre odborníkov v oblasti kybernetickej a informačnej bezpečnosti,
- vytvorenie konceptu minimálnych požiadaviek na bezpečnostné povedomie pre všetky stupne vzdelávania,
- vytvorenie systému šírenia bezpečnostného a situačného povedomia o hrozbách, zraniteľnostiach, incidentoch a postupoch na ochranu v kybernetickom priestore,
- zapracovanie rolí v oblasti kybernetickej a informačnej bezpečnosti do Národného kvalifikačného rámca,
- realizáciu spoločných vzdelávacích aktivít a aktivít podporujúcich zvyšovanie bezpečnostného povedomia s orgánmi verejnej moci, akademickou obcou a súkromným sektorom,
- rozvoj schopností v oblasti cvičení a tréningov v technických a procesných oblastiach rôznymi formami spolu s vytvorením vhodnej technickej a organizačnej platformy na organizovanie takýchto cvičení,
- podporu projektov a programov v oblasti vzdelávania a šírenia bezpečnostného a situačného povedomia.
- vytvorenie systému vzdelávania zamestnancov verejnej správy tak, aby spĺňali minimálne vedomostné štandardy v oblasti kybernetickej a informačnej bezpečnosti,
- doplnenie a udržiavanie kompetencií v kybernetickej a informačnej bezpečnosti prostredníctvom Slovenského kvalifikačného rámca (SKKR) a Národnej sústavy kvalifikácií SR (NSK).



4.7 Rozvoj výskumu a vývoja v oblasti kybernetickej bezpečnosti

Hrozby a zraniteľnosti v kybernetickom priestore sa neustále vyvíjajú kontinuálne s technologickým rozvojom a digitalizáciou spoločnosti. Výskum a vývoj v oblasti kybernetickej bezpečnosti je vhodným mechanizmom, ako reagovať na zmenu bezpečnostného prostredia a implementovať vhodné opatrenia na minimalizáciu hrozieb, ošetrovanie zraniteľností a detekciu a riešenie kybernetických bezpečnostných incidentov.

4.7.1 Východiskový stav

Výskum a vývoj v oblasti kybernetickej bezpečnosti je decentralizovaný a minimálny, riešia ho najmä súkromné spoločnosti v rámci svojej podnikateľskej činnosti a akademická obec.

Štát nemá ucelený koncept štátnej podpory výskumu a vývoja v oblasti kybernetickej bezpečnosti, nemá stanovené jednotné ciele v tejto oblasti.

4.7.2 Cieľový stav

Dobre fungujúci a štátom podporovaný výskum a vývoj v oblasti kybernetickej bezpečnosti.

Dobrá komunikácia medzi verejným, súkromným sektorom a akademickou obcou v oblasti výskumu a vývoja s jasnými výsledkami.

Efektívny systém spolupráce verejného sektora, súkromného sektora a akademickej obce.

Štátna podpora projektov v oblasti kybernetickej bezpečnosti a aktívna asistencia štátu pri využívaní prostriedkov z Európskych fondov.

4.7.3 Cesta k cieľovému stavu

Pre dosiahnutie cieľového stavu tohto strategického cieľa je potrebné zamerať sa na:

- vytvorenie ucelenej koncepcie štátnej podpory výskumu a vývoja v oblasti kybernetickej bezpečnosti pre Slovenskú akadémiu vied, vysoké školy aj komerčné organizácie,
- alokáciu finančných zdrojov pre štátnu podporu výskumu a vývoja na najbližších 5 rokov,
- podpora výskumných centier v oblasti kybernetickej bezpečnosti na vysokých školách,
- koordináciu podpory vedy a výskumu prostredníctvom Kompetenčného a certifikačného centra kybernetickej bezpečnosti,
- podporu vedecko-výskumných projektov súkromných spoločností a výskumných centier na národnej úrovni,
- pomoc a podporu subjektov pri ich zapájaní sa do vedecko-výskumných programov a grantov na národnej a medzinárodnej úrovni,
- participácia na propagácii národných výskumných programov a ich výsledkov,
- vybudovanie uzatvorenej výskumnej sieťovej infraštruktúry naprieč celou Slovenskou republikou zameranej na výskum, vývoj a testovanie v oblasti kybernetickej bezpečnosti,
- rozvoj spôsobilostí v oblasti národnej kryptografie.

5. Hlavní zahraničnopolitickí partneri

> Vzájomná prepojenosť kybernetického priestoru, v ktorom nezohrávajú hranice štátov prakticky žiadnu rolu, je na dosiahnutie želaných cieľov kybernetickej bezpečnosti rozhodujúcou práve medzinárodná spolupráca.

Slovenská republika je demokratický a právny štát, ktorý sa opiera o princípy dodržiavania základných práv a slobôd. Preto sa pri medzinárodnej spolupráci v oblasti kybernetickej bezpečnosti zameriava na politickú a technickú spoluprácu so štátmi a medzinárodnými organizáciami, ktoré rešpektujú a presadzujú rovnaké hodnoty.

Slovenská republika ako člen EÚ plne podporuje spoločnú zahraničnú a bezpečnostnú politiku, rešpektuje a spolupracuje s jednotlivými členskými štátmi a rozvíja spoločné spôsobilosti v oblasti kybernetickej bezpečnosti na celoeurópskej úrovni. Na technickej úrovni je to najmä jej členstvo v európskej sieti CSIRT jednotiek, na politicko-strategickej členstvo v Horizontálnej pracovnej skupine pre kybernetické záležitosti či v pracovných skupinách Európskej komisie.

Členstvo Slovenskej republiky v NATO je z hľadiska bezpečnosti dobrým modelom, ktorý zaisťuje kolektívnu obranu jej členov a partnerov a fakticky udržuje mier nielen v Európe už niekoľko desaťročí. NATO sa zameriava najmä na problematiku kybernetickej obrany a zvyšujúci sa počet kybernetických útokov, ale aj útokov hybridnej povahy postavilo Alianciu pred nové výzvy, na ktoré je potrebné reagovať odstrašujúcimi obrannými schopnosťami, ale aj kontinuálnym budovaním spôsobilostí nielen na úrovni členských a partnerských štátov, ale aj v rámci spoločných aktivít, napríklad prostredníctvom Centra excelentnosti NATO pre kooperatívnu kybernetickú obranu.

Členstvo Slovenskej republiky v OSN a OBSE dovoľuje aktívne participovať na aktivitách a projektoch v oblasti kybernetickej bezpečnosti, ktoré menované organizácie organizujú a vytvárajú.

Postoje SR na medzinárodných fórach, ktoré sa venujú problematike kybernetickej bezpečnosti, vychádzajú z princípov globálneho, otvoreného, slobodného, stabilného a bezpečného kybernetického priestoru pri plnom rešpektovaní základných princípov právneho štátu, ľudských práv a základných slobôd, rodovej a digitálnej rovnosti ako a trvalého rozvoja. SR spolu s partnermi v rámci EÚ zdôrazňuje význam medzinárodných noriem a pravidiel pre zodpovedné správanie v kybernetickom priestore, rozvoj a implementáciu opatrení na posilnenie dôvery a budovania potrebných kapacít v oblasti kybernetickej bezpečnosti.

Slovenská republika bude využívať nástroje kybernetickej diplomacie voči vykonávateľom kybernetických útokov zameraných voči SR a jej záujmom a v súlade s jej záväzkami voči EÚ, NATO a jej spojencom.

6. Implementácia a merateľnosť

> Aby mohli byť úspešne naplnené strategické ciele Národnej stratégie, musí byť vytvorený jej zodpovedajúci akčný plán, ako aj riadiaci výbor, na úrovni ktorého sa bude koordinovať postup jednotlivých zainteresovaných subjektov.

6.1 Vytvorenie akčného plánu

Akčný plán implementácie Národnej stratégie kybernetickej bezpečnosti na roky 2021 až 2025 určí:

- konkrétne úlohy a aktivity rozdelené podľa strategických cieľov,
- spôsob realizácie jednotlivých úloh a aktivít,
- časový horizont plnenia úloh,
- zodpovedné subjekty v roli gestorov a participujúcich subjektov,
- dopady, resp. náklady vyvolané jednotlivými úlohami.

Za vypracovanie Akčného plánu zodpovedá Národný bezpečnostný úrad, ktorý do jeho prípravy zapojí všetky zainteresované subjekty.

6.2 Vytvorenie riadiaceho výboru pre implementáciu Národnej stratégie a Akčného plánu

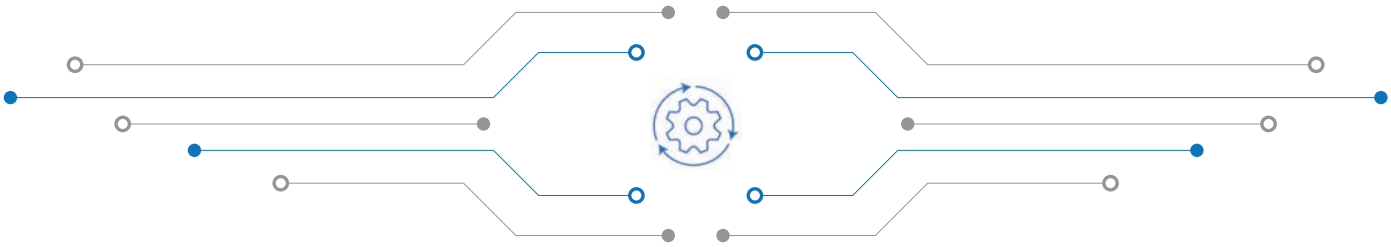
Pre lepšie riadenie jednotlivých úloh a aktivít bude vytvorený riadiaci výbor, ktorý bude koordinačným orgánom pre všetky zainteresované subjekty, ktoré si do riadiaceho výboru môžu určiť svojho zástupcu.. Na platforme tejto pracovnej skupiny sa bude komunikovať postup realizácie jednotlivých úloh a aktivít a takisto sa na nej budú riešiť problémy, ktoré vzniknú počas implementácie Akčného plánu. Riadiaci výbor bude zároveň pripravovať pravidelnú správu o odpočte Akčného plánu. Za organizáciu a riadenie riadiaceho výboru bude zodpovedný Národný bezpečnostný úrad.

6.3 Implementácia

Národná stratégia bude implementovaná prostredníctvom Akčného plánu a jeho úloh a aktivít. Za realizáciu jednotlivých úloh a aktivít budú zodpovedné subjekty, ktoré určí Akčný plán či už ako gestorský alebo spolupracujúci subjekt.

6.4 Meranie

Za odpočet jednotlivých úloh a aktivít budú zodpovedné určené subjekty, za meranie plnenia akčného plánu bude zodpovedný Národný bezpečnostný úrad. Kontrola a hodnotenie plnenia Akčného plánu sa bude robiť raz ročne.



6.5 Zainteresované subjekty

Medzi hlavné zainteresované subjekty v systéme kybernetickej bezpečnosti Slovenskej republiky patria najmä:

- Úrad vlády Slovenskej republiky,
- Národný bezpečnostný úrad,
- Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky,
- Ministerstvo financií Slovenskej republiky,
- Ministerstvo zahraničných vecí a európskych záležitostí Slovenskej republiky,
- Ministerstvo obrany Slovenskej republiky,
- Ministerstvo školstva, vedy, výskumu a športu Slovenskej republiky,
- Ministerstvo vnútra Slovenskej republiky,
- Ministerstvo spravodlivosti Slovenskej republiky,
- Ministerstvo zdravotníctva Slovenskej republiky,
- Generálna prokuratúra Slovenskej republiky,
- Úrad na ochranu osobných údajov,
- Prezídium policajného zboru Slovenskej republiky,
- Vojenské spravodajstvo,
- Slovenská informačná služba,
- vysoké školy a iné vzdelávacie inštitúcie,
- Kompetenčné a certifikačné centrum kybernetickej bezpečnosti,
- prevádzkovatelia základných služieb,
- poskytovatelia digitálnych služieb.

7. Financovanie

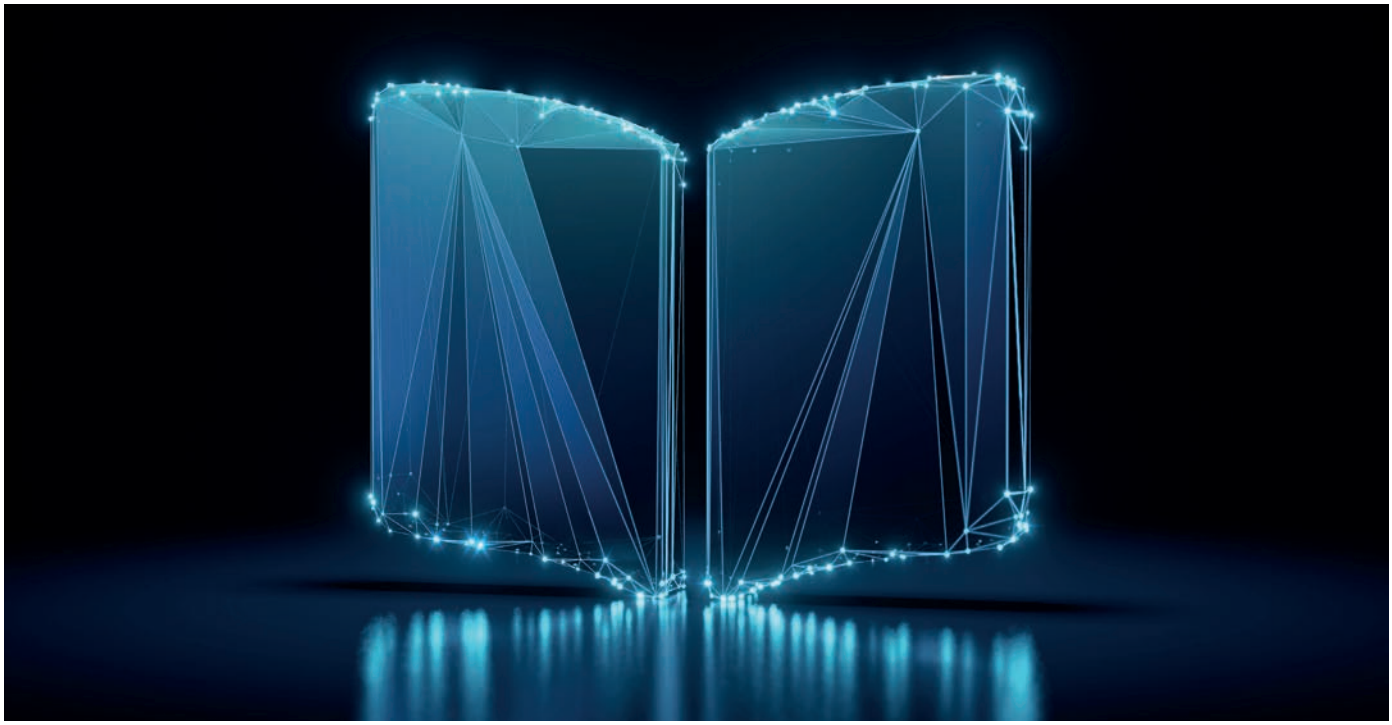
Každý zo zodpovedných subjektov v rámci systému kybernetickej bezpečnosti, ktoré sú definované aj v nadväzujúcom akčnom pláne, musia v rámci svojich rozpočtových kapitol vyčleniť dostatočné finančné prostriedky tak, aby bolo možné splniť úlohy a aktivity vychádzajúce z nimi schváleného Akčného plánu, ako aj z princípov systému kybernetickej bezpečnosti. Pri hľadaní finančných zdrojov je potrebné opierať sa nielen o prostriedky zo štátneho rozpočtu, ale aj zdroje z operačných programov fondov Európskeho spoločenstva.

Záujmom štátu a jeho organizácií a inštitúcií musí byť vyčlenenie dostatočných finančných prostriedkov na kybernetickú bezpečnosť na všetkých úrovniach tak, aby mohli byť naplnené strategické ciele kybernetickej bezpečnosti definované v Národnej stratégii.

8. Záver

Kybernetické hrozby už dávno nie sú len záležitosťou špeciálnych systémov a profesionálov v oblasti informačných technológii. Týkajú sa každého z nás. Kybernetická bezpečnosť musí byť spoločnou zodpovednosťou štátu a jeho občanov. Útoky cudzích mocností, ale aj aktivity kybernetických zločincov majú signifikantný dopad na naše bežné fungovanie. K základným strategickým záujmom Slovenskej republiky musí patriť udržiavanie a zdokonaľovanie systému kybernetickej bezpečnosti tak, aby hrozby, zraniteľnosti a incidenty mali čo najmenší dopad na štát a jeho občanov, ako aj na fungovanie spoločenského zriadenia.

Národná stratégia kybernetickej bezpečnosti na roky 2021 až 2025 je strednodobý dokument. Prijíma sa na obdobie 5 rokov. V prípade zmeny bezpečnostného prostredia alebo iných vplyvov, ktoré by mohli výrazne ovplyvniť fungovanie systému kybernetickej bezpečnosti v Slovenskej republike, sa môže dokument aktualizovať aj skôr.



NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

NÁRODNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI SK-CERT

Budatínska 30, 851 06 Bratislava

www.nbu.gov.sk

www.sk-cert.sk

Copyright © 2021 Národný bezpečnostný úrad