

Správa o kybernetickej bezpečnosti v Slovenskej republike v roku 2019

Obsah

ROK 2019 V KOCKE	4
KYBERNETICKÁ BEZPEČNOSŤ	5
AKTÉRI	6
INCIDENTY A HROZBY	7
Kategórie incidentov	8
Incidenty na časovej osi	9
Povinné a dobrovoľné hlásenia incidentov	9
Hrozby	10
SEKTOROVÝ POHĽAD	16
Bankovníctvo	16
Elektronická komunikácia a digitálna infraštruktúra	17
Energetika	18
Verejná správa	19
Zdravotníctvo	21
Ostatné sektory	22
AKTIVITY A OPATRENIA	23
Legislatíva	23
Spolupráca s prevádzkovateľmi a poskytovateľmi	24
Národné a medzinárodné aktivity a spolupráca	26
Národné centrum kybernetickej bezpečnosti SK-CERT	27
Kompetenčné a certifikačné centrum kybernetickej bezpečnosti	27
Distribúcia bezpečnostných bulletinov a varovaní	28
Cvičenia	30
Kybernetická bezpečnosť 5G sietí	32
Návod na oznamovanie zraniteľností	32
PREDIKCIA VÝVOJA KYBERNETICKEJ BEZPEČNOSTI NA ROK 2020	32

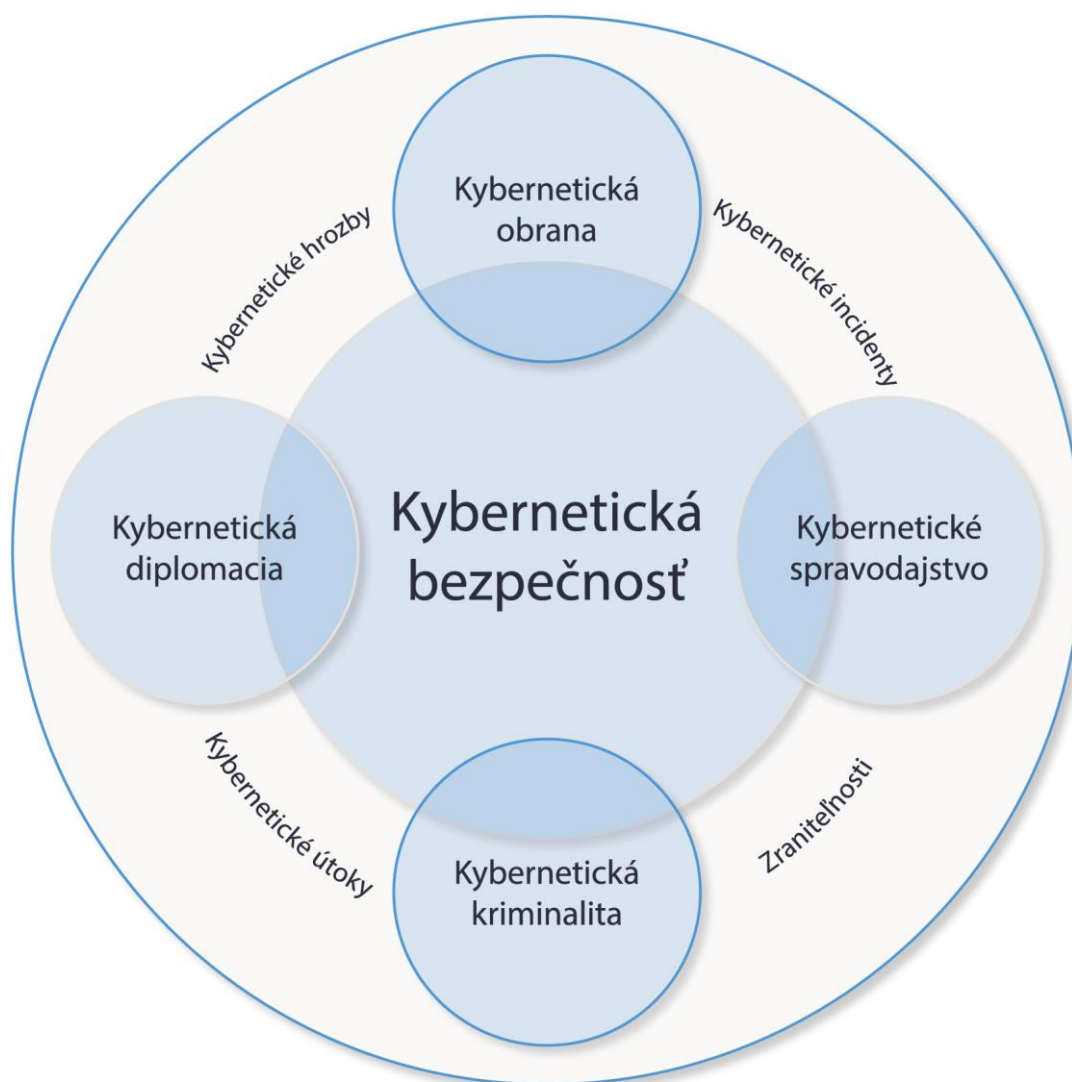
Rok 2019 v kocke

Bezpečnosť 5G sietí Európska komisia vydala odporúčanie pre kybernetickú bezpečnosť 5G sietí. Slovenská republika aktívne participovala na tvorbe spoločného posúdenia rizík 5G sietí.	Národné centrum kybernetickej bezpečnosti SK-CERT Dňa 1.9.2019 vzniklo na Národnom bezpečnostnom úrade Národné centrum kybernetickej bezpečnosti SK-CERT transformáciou Národnej jednotky SK-CERT.		
Phishing na vzostupe Globálne vzrástol počet phishingových kampaní o 65 percent.	Národné Table-top cvičenia Národné centrum kybernetickej bezpečnosti začalo organizovať sériu Národných Table-top cvičení.		
	Návod na oznamovanie zraniteľností Národné centrum kybernetickej bezpečnosti vydalo návod na oznamovanie bezpečnostných zraniteľností.	244 bezpečnostných varovaní vydaných SK-CERTom.	52 bezpečnostných bulletinov vydaných SK-CERTom. 8815 vyriešených incidentov.

Kybernetická bezpečnosť

Kybernetická bezpečnosť zahŕňa procesy, postupy, technologické a personálne zabezpečenie ochrany systémov, sietí a zariadení pred incidentami v kybernetickom priestore.

Môžeme ju tiež definovať ako stav pripravenosti na odhaľovanie útokov, riešenie kybernetických bezpečnostných incidentov a minimalizáciu následkov po incidente.



Legislatívny základ ochrany kybernetického priestoru v Slovenskej republike tvorí zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti, ktorý je transpozíciou Smernice 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 (tzv. smernica NIS).

Národný bezpečnostný úrad je národnou autoritou pre kybernetickú bezpečnosť a z tejto pozície riadi a koordinuje výkon štátnej správy v oblasti kybernetickej bezpečnosti, určuje štandardy a vydáva politiku správania sa v kybernetickom priestore. Úrad je hlavným kontaktným bodom pre zahraničie v oblasti kybernetickej bezpečnosti, spolupracuje s ústrednými orgánmi, prevádzkovateľmi základných služieb a poskytovateľmi digitálnych služieb a takisto plní úlohu národnej jednotky CSIRT (jednotky pre riešenie kybernetických bezpečnostných incidentov).

Aktéri

Aj napriek tomu, že kybernetické útoky prebiehajú vo virtuálnom priestore, za každým jedným z nich stojí fyzická osoba – útočník alebo skupina útočníkov. Ľudovo sú označovaní ako hackeri. Na základe spôsobu útoku a motivácie rozdeľujeme útočníkov do niekoľkých kategórií.

Script kiddies

Ide o neskúsených útočníkov, skôr by sme ich mohli nazvať začiatocníkmi alebo „hobby hackermi“. Vyznačujú sa zväčša nižším vekom a nie vždy uchopiteľnou motiváciou: častokrát im ide skôr o zábavu a adrenalín.

V drvivej väčšine prípadov využívajú nástroje, ktoré vytvorili skúsenejší útočníci a ktoré sa dajú stiahnuť alebo kúpiť na darkwebe.¹ Preferujú jednoduchšie formy útokov, najmä šírenie škodlivého kódu, ransomvéru alebo jednoduchého phishingu.

Kyberkriminálni

Nakoľko sú neskúsení, sú aj veľmi ľahko vystopovateľní. Sú nebezpeční pre bežných používateľov, ale vyskytli sa už aj prípady pokusov útokov na väčšie ciele, napríklad na verejné inštitúcie. Ak je však používateľ obozretný, sú takmer neškodní. Avšak s narastajúcou dostupnosťou profesionálnych nástrojov, ktoré sú voľne dostupné na internete alebo darkwebe, rastie aj dopad ich aktivít – čoraz častejšie vedú spôsobiť aj značné škody.

Útočníci s jasnou motiváciou, ktorí zvyčajne operujú v skupinách, vyskytujú sa však aj prípady samostatných útočníkov. Ich motiváciou je finančný zisk – či už priamy (prístup k finančným službám obete) alebo nepriamy (napríklad formou ransomvéru alebo inej formy digitálneho vydierania).

Vyžívajú voľne dostupné, ale aj vlastné, resp. modifikované nástroje, ktoré si vyberajú špeciálne na určité typy útokov pre jednotlivé ciele. Ich spôsoby útokov sú rôznorodé – od phishingových kampaní až po vytváranie tzv. botnet sietí.

Vystopovať skúseneho kyberkriminála býva veľmi náročné (no nie nemožné). Väčšina z nich vyrástla zo script kiddies. Pre bežných používateľov sú najnebezpečnejší, nakoľko využívajú sofistikované spôsoby útokov.

Haktivisti

Ide o útočníkov operujúcich v skupinách, ale aj decentralizovane (napríklad skupina Anonymous). Nemajú finančnú motiváciu, ide im o „etický aspekt“ a „konanie dobra“ vo virtuálnom priestore, ktoré má presah aj do reálneho sveta.

Využívajú rôzne formy nástrojov, ktoré si aj sami vytvárajú. Zameriavajú sa najmä na získavanie citlivých alebo utajených informácií z vládnych inštitúcií, armády alebo tajných služieb (skupiny ako Shadow Brokers alebo WikiLeaks), „nápravu krívd“ v kybernetickom prostredí (skupina Anonymous) alebo pokusy o prienik do informačných systémov s cieľom poukázať na existujúce zraniteľnosti.

Nezameriavajú sa na bežných používateľov, ale na štátne inštitúcie, resp. na predstaviteľov vlád. V mnohých prípadoch sa k útoku skupina prihlási, avšak vystopovať konkrétnu osobu, ktorá útok spáchala, je veľmi náročné.

Štátom sponzorované skupiny

¹ Časť internetu, do ktorého sa dá dostať len špeciálnymi nástrojmi; čierny trh s rôznym fyzickým, ale i virtuálnym tovarom.

Ide o profesionálnych hackerov v službách štátu. Ich vzťah so štátom môže byť priamy – členovia skupiny sú „zamestnancami“ štátu (príslušníci tajných služieb alebo armády) alebo nepriamy – skupinu štát skryte finančne a materiálne podporuje. Ak príde k atribúcii útoku, ktorá poukazuje na konkrétnu skupinu, štáty popierajú akúkoľvek spojitosť s útokom a útočníkmi. K štátom podporovaným skupinám patria napríklad Fancy Bear (APT28, Rusko), Cozy Bear (APT29, Rusko), Comment Crew (APT1, Čína), Stone Panda (APT10, Čína), Turla (Rusko), Lazarus Group (Severná Kórea), Cutting Kitten (Irán) a iné.²

Nástroje, ktoré používajú sú na vysokej úrovni. Medzi ich devízy patria najmä tzv. zraniteľnosti nulového dňa (0-day vulnerabilities), ktoré používajú na útoky na špeciálne, dobre zabezpečené ciele. Ich zámerom je najmä získavanie citlivých a utajených informácií, získavanie výhod pre „domovský“ štát, ovplyvňovanie verejnej mienky, volieb a referendum, vytváranie a distribúcia falošných správ (fake news, hoax), ovplyvňovanie rozhodovania štátnych orgánov, destabilizácia verejného poriadku, ovplyvňovanie ekonomickej stability, či narušanie demokratických procesov.

Ich útoky sú vysoko sofistikované a vedia po sebe dobre zahľadiť stopy. Ich odhalenie podlieha náročnej atribúcii, ktorá nie vždy býva úspešná. Výsledkom úspešnej atribúcie bývajú politické rozhodnutia. Ich motivácia býva rôzna – buď ide o ekonomickú motiváciu, nakoľko takíto hackeri sú veľmi dobre platení, alebo ide o politicko-vlasteneckú motiváciu – hackeri sú lojálni k režimu.

Kyberteroristi

Nebezpeční profesionáli v službách teroristických organizácií. Ich cieľom je útokmi v kybernetickom priestore navodiť strach, vydierať štátnych aktérov alebo priamo zasiahnuť armádne a aj civilné ciele – napríklad znefunkčnením prvkov kritickej infraštruktúry. Často sa k takýmto útokom priznávajú. Ich motiváciou sú buď peniaze, nakoľko teroristické organizácie ich dokážu dobre zaplatiť, alebo náboženstvo – sú lojálni až sfanatizovaní.

Incidenty a hrozby

Kybernetickým bezpečnostným incidentom je akákoľvek udalosť, ktorá má z dôvodu narušenia bezpečnosti siete a informačného systému, porušenia bezpečnostnej politiky alebo záväznej metodiky negatívny vplyv na kybernetickú bezpečnosť alebo ktorej následkom je

1. strata dôvernosti údajov, zničenie údajov alebo narušenie integrity systému,
2. obmedzenie alebo odmietnutie dostupnosti základnej služby alebo digitálnej služby,
3. vysoká pravdepodobnosť kompromitácie činností základnej služby alebo digitálnej služby,
4. ohrozenie bezpečnosti informácií.

ČO JE TO INCIDENT?

Incidentom nemusí byť len kybernetický útok. Ide o akúkoľvek udalosť, ktorá spĺňa vyššie uvedené kritériá. Avšak cieľ a motivácia útočníka, resp. spôsob, akým vyšiel incident najavo, udáva niekoľko typov incidentov, podľa ktorých je jednoduchšie zvoliť napríklad spôsob reakcie alebo spôsob detekcie.

² Zoznam APT skupín aj s ich popisom je dostupný napríklad na: <https://attack.mitre.org/groups/>

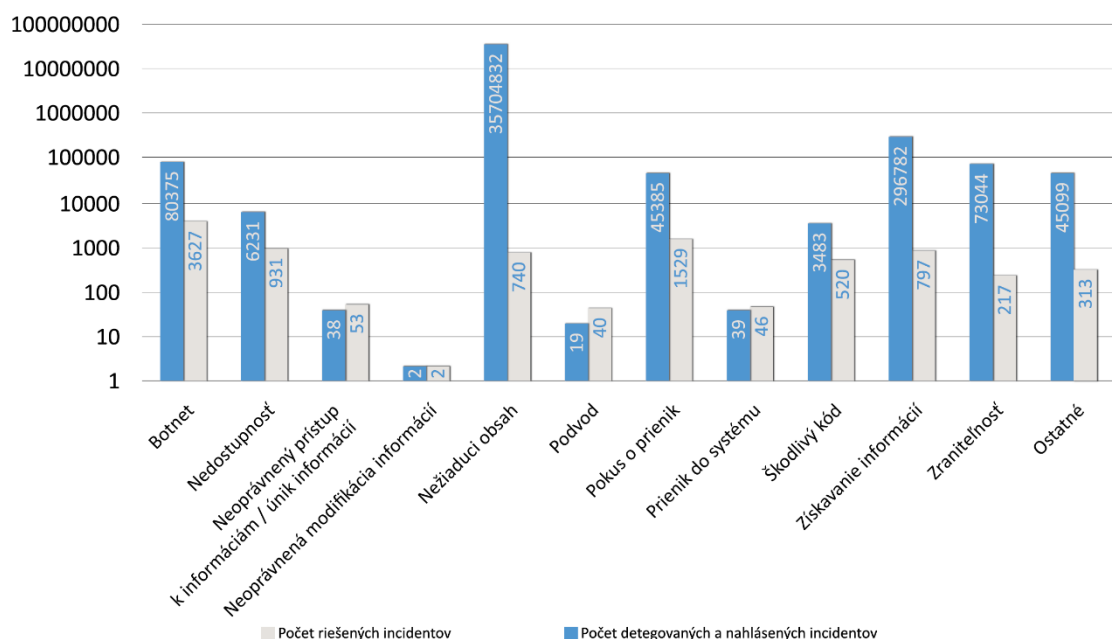
Kategórie incidentov

SK-CERT v priebehu roka 2019 zbieral informácie o incidentoch v slovenskom kybernetickom priestore. Zdrojom údajov bola vlastná detekcia, povinné a dobrovoľné hlásenia prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb a informácie od partnerov a partnerských organizácií.

Botnet Útok, pri ktorom útočník infikuje zariadenie obete a využíva ho na ďalšie útoky.	Neoprávnená modifikácia informácií Zmena alebo zmazanie informácie v systéme/službe.	Nežiaduci obsah Sem zaraďujeme najmä spam, scam, defacement stránok a podobne.	Podvod Podvodné konanie útočníka, na ktoré využíva rôzne nástroje v kybernetickom priestore.
Nedostupnosť Zneprístupnenie služby útočníkom pomocou viacerých nástrojov, vrátane distribuovaných útokov (napr. využitie zariadení v botnete).	Pokus o prienik Pokusy dostať sa do chránených sietí a zariadení.	Škodlivý obsah Šírenie tzv. malvéru - napríklad ransomvér, trójske kone, advér a podobne.	Získavanie informácií Využívanie sociálneho inžinierstva na získavanie informácií (najčastejšie phishing, spear-phishing a podobne).
Neoprávnený prístup k informáciám/únik informácií Útočník sa neoprávnene dostane k citlivým alebo utajeným informáciám.	Prienik do systému Úspešné preniknutie do systému alebo zariadenia. Sem zaraďujeme aj APT útoky.	Zraniteľnosť Zneužívanie, ale aj samotná existencia zraniteľností na systémoch a službách, ktoré môže útočník využiť na úspešný útok.	Ostatné Všetky ostatné incidenty, ktoré nespádajú do ostatných kategórií.

Získané dáta umožňujú vytvoriť ucelený pohľad na počet nahlásených, detegovaných a riešených incidentov podľa jednotlivých kategórií. Najviac detegovaných a nahlásených incidentov bolo v kategórii „Nežiaduci obsah“, najviac riešených incidentov bolo v kategórii „Botnet“.

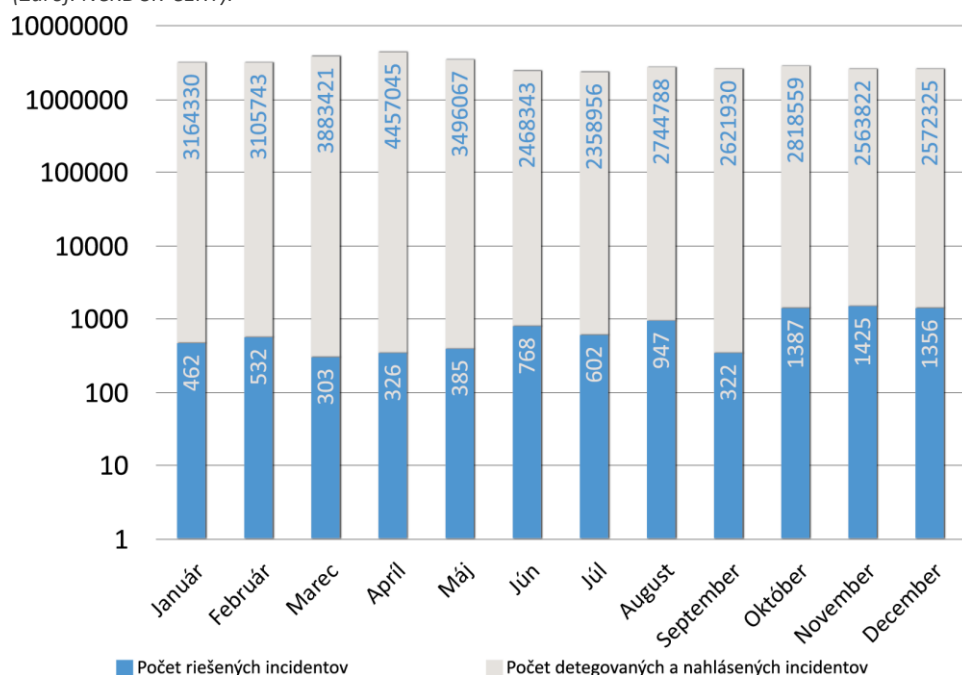
Graf č. 1: Počet detegovaných, nahlásených a riešených incidentov v roku 2019. (Zdroj: NCKB SK-CERT).



Incidenty na časovej osi

Najviac incidentov bolo v roku 2019 detegovaných a nahlásených v mesiaci apríl, najviac riešených bolo v mesiaci november. Vstupy do tejto štatistiky pochádzajú zo zdrojov SK-CERT a od jeho CSIRT partnerov v Slovenskej republike.

Graf č. 2: Počet detegovaných, nahlásených a riešených incidentov v roku 2019 na časovej osi.
(Zdroj: NCKB SK-CERT).

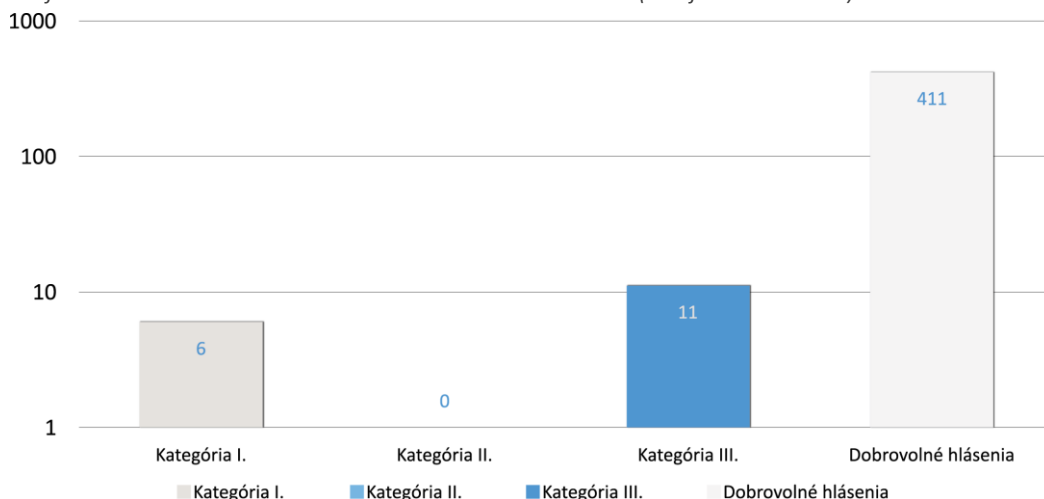


Povinné a dobrovoľné hlásenia incidentov

Prevádzkovatelia základných služieb a poskytovatelia digitálnych služieb majú zo zákona o kybernetickej bezpečnosti dňom zápisu povinnosť hlásiť úradu každý závažný kybernetický bezpečnostný incident.

Podľa príslušnej vykonávacej vyhlášky sú kategórie závažných kybernetických bezpečnostných incidentov rozdelené na tri kategórie. Ak kybernetický bezpečnostný incident nepresiahne hraničné kritériá pre jednu z kategórií závažných kybernetických bezpečnostných incidentov, prevádzkovateľ základnej služby alebo poskytovateľ digitálnej služby môžu kybernetický bezpečnostný incident hlásiť úradu aj na dobrovoľnej báze.

Graf č. 3: Povinné a dobrovoľné hlásenia incidentov v roku 2019. (Zdroj: NCKB SK-CERT).



Hrozby

Kybernetické hrozby sa v minulom roku vyznačovali používaním nových techník a vektorov útokov. Pre útočníkov boli cieľmi bežní používatelia, ale aj veľké spoločnosti a štátne organizácie. Ich motiváciou boli prihlasovacie údaje do finančných služieb, ako aj citlivé údaje organizácií a firiem. Podľa počtu riešených incidentov a analýzy otvorených zdrojov boli v roku 2019 zdrojom najnebezpečnejších hrozieb phishingové kampane, botnety, úniky dát, útoky na dostupnosť služieb (DoS a DDoS) a zraniteľnosti.

Phishing

Phishing patrí k najčastejšie používaným spôsobom útokov. Jeho princíp spočíva vo využívaní nástrojov sociálneho inžinierstva na získavanie citlivých údajov občanov a firiem, prístupových hesiel alebo iných informácií o obeti. Útočník môže získané údaje zneužiť vo svoj prospech alebo pri ďalších druhoch útokov. Pri phishingu využívajú útočníci najčastejšie e-mailové správy, správy na sociálnych sieťach, ale aj špeciálne vytvorené webové stránky alebo telefonáty. Podstata takéhoto útoku spočíva v presvedčení obete, aby poskytla útočníkovi žiadané informácie a to buď priamo, stiahnutím prílohy, alebo kliknutím na odkaz so škodlivým kódom.

CIELE	ÚTOČNÍCI	DOPAD
bežní používatelia, bankový sektor, verejná správa, kritická infraštruktúra (často ako prvotná fáza APT útoku)	script kiddies, kyberkriminálnici, štátom sponzorované skupiny	získanie citlivých údajov, získanie prihlasovacích údajov do finančných služieb, získanie prihlasovacích údajov k citlivým systémom

Phishingové kampane 2019 vo svete

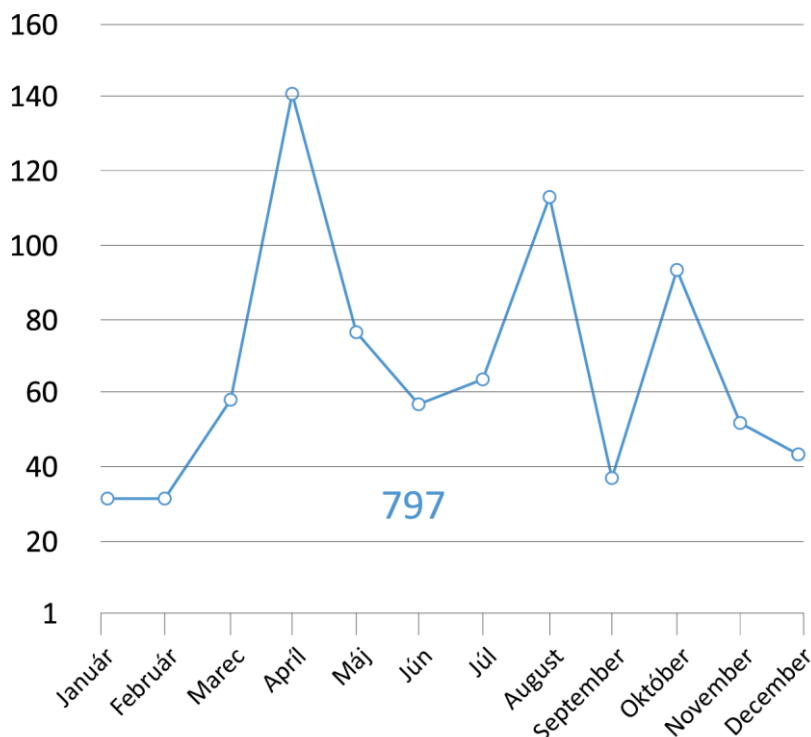
V roku 2019 pokračovali škodlivé phishingové kampane, ktoré využívali aj nové vektory útoku. Útočníci často zneužívali značky známych spoločností (napríklad Facebook) na legitimizáciu phishingových e-mailov a obsahu. Zameriavali sa pri tom na získavanie prihlasovacích údajov do sociálnych sietí, ale aj do personálnych bankových účtov obetí. Ich cieľom bolo naďalej získavať citlivé údaje občanov a firiem, údaje k bankovým kontám a takisto iné používateľské údaje, napríklad telemetrické alebo biometrické údaje. Jedným z cieľov sofistikovaných phishingových aktivít bolo takisto aj získanie prístupov do rôznych systémov a služieb. Podľa verejne dostupných štatistík vzrástol počet phishingových útokov oproti roku 2018 o 65 %.³

Slovenská republika

V priebehu roka 2019 bola zaznamenaná rozsiahla phishingová a malwertisingová (distribúcia reklamy s cieľom šíriť škodlivý kód) kampaň, ktorá cieľila na zákazníkov jedného z dodávateľov elektrickej energie. Správy obsahovali výzvy na úhradu nedoplatku, pričom príloha obsahovala škodlivý kód, ktorý po spustení vykonával exfiltráciu prihlasovacích údajov, hesiel, a tzv. screenshotov obrazovky obete. Cieľom škodlivého kódu boli prevažne prihlasovacie údaje do bankových a finančných služieb, sociálnych sietí a na e-mailové služby. Infraštruktúra útočníka bola unikátna a sofistikovaná a vyznačovala sa vysokou mierou automatizácie počas kompilácie a následnej distribúcie škodlivého obsahu. V rámci riešenia incidentu podali poškodení trestné oznámenie na neznámeho páchatela.

³ <https://retruster.com/blog/2019-phishing-and-email-fraud-statistics.htm>

Graf č. 4: Phishing - počet riešených incidentov v roku 2019. (Zdroj: NCKB SK-CERT).



Botnet

Botnetom rozumieme rozsiahlu sieť zloženú z rôznych zariadení od počítačov, mobilných telefónov až po servery ale napríklad aj tlačiarne. Sieť ovláda útočník prostredníctvom jedného alebo viacerých riadiacich serverov.

Obeť takéhoto útoku si veľa krát ani neuvedomí, že jeho zariadenie je súčasťou botnetovej siete. Útočník môže zariadenie obete získať a prevziať nad ním kontrolu, napríklad dorúčením malvéru v legítimnej softvérovej aplikácii alebo zaslaním phishingového e-mailu so škodlivým kódom.

Útočník takúto sieť využíva na rôzne typy aktivít. Medzi najčastejšie patria distribuované útoky na zneprístupnenie služieb (DDoS), šírenie škodlivého kódu, zasielanie phishingových a spamových e-mailov, ťaženie kryptomien a podobne. Útočník môže množstvo z týchto úkonov automatizovať a následne len získavať výsledky útokov botnetových uzlov, ktoré sa v bezpečnostnom žargóne nazývajú aj „zombies“.

CIELE	ÚTOČNÍCI	DOPAD
všetci používatelia	kyberkriminálni, štátom sponzorované skupiny	zneužívanie počítača obete na ďalšie útoky, využívanie výpočtového výkonu počítača bez vedomia používateľa

Botnetové útoky 2019 vo svete

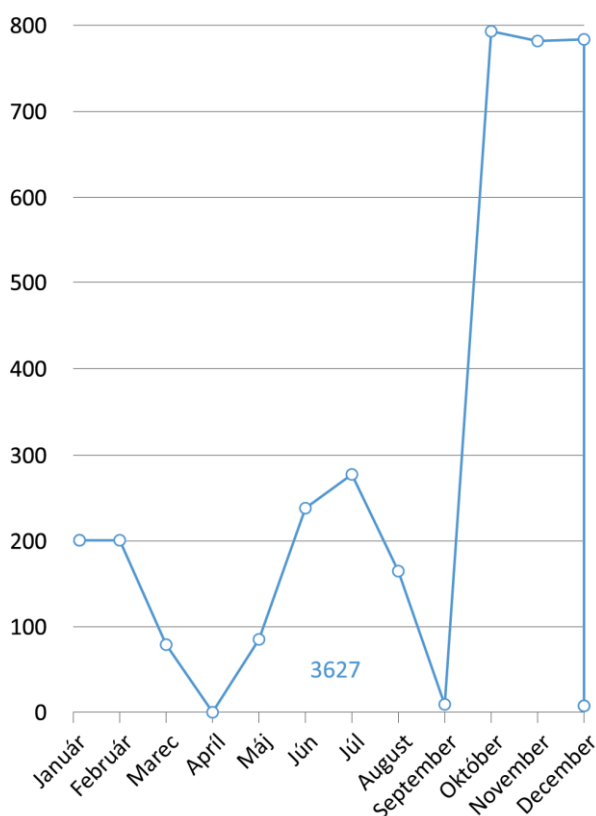
V roku 2019 pokračoval trend z predošlých rokov. Infekcia zariadení s cieľom ich pripojenia do botnetovej siete bola naďalej veľmi obľúbeným spôsobom útokov. Vzrástol počet zariadení typu IoT (Internet of Things, internet vecí) zasiahnutých malvérom, ktorý útočníkovi dovoľoval zariadenie

ovládať. V roku 2019 sa útočníci vo využívaní botnetov najviac zamerali na šírenie phishingového obsahu a následné získavanie prihlasovacích a iných citlivých údajov, na využívanie nástrojov vzdialeného prístupu (tzv. RAT), na šírenie škodlivého kódu na ťaženie kryptomien a takisto aj na šírenie ransoméru.

Slovenská republika

Incidenty typu „Botnet“ sa v roku 2019 vyskytovali najmä na zariadeniach bežných používateľov. Medzi najčastejšie prítomné botnetové rodiny patrili downadup, Qsnatch a Sality. SK-CERT získaval informácie o infikovaných zariadeniach monitoringom otvorených zdrojov a potenciálnych hrozieb v kybernetickom priestore SR, ako aj od partnerov a partnerských organizácií. Na základe týchto informácií boli zasielané adresné varovania poskytovateľom internetových služieb, ktorí následne informovali majiteľov alebo správcov infikovaných zariadení.

Graf č. 5: Botnet - počet riešených incidentov v roku 2019. (Zdroj: NCKB SK-CERT).



Úniky dát

Úniky dát sú vždy dôsledkom iných aktivít útočníka. Aj keď vo väčšine prípadov je motiváciou útočníka práve získanie obchodne, politicky, bezpečnostne či osobne citlivých údajov, využíva na to rôzne spôsoby. Či už ide o spear-phishingové aktivity (cielený phishing) na konkrétne ciele, alebo pokusy o prienik do systémov za zneužitia zraniteľností. Exfiltrácia dát môže byť jednorazová alebo dlhodobá podľa toho, na koho útočník cieľi a čo chce získať. Najčastejšie sa vyskytujú úniky citlivých údajov zákazníkov veľkých spoločností, ale aj citlivé alebo utajované dáta vládnych inštitúcií.

CIELE	ÚTOČNÍCI	DOPAD
veľké spoločnosti z rôznych sektorov, verejná správa	kyberkriminálni, hacktivistí, štátom sponzorované skupiny	únik citlivých údajov zákazníkov alebo zamestnancov, citlivé údaje o spoločnosti (napr. vnútorná komunikácia), obchodné či priemyselné tajomstvo, citlivé alebo utajované informácie

Úniky dát 2019 vo svete

V priebehu roka 2019 bolo zaznamenaných niekoľko masívnych únikov dát zo sektorovo rôznych inštitúcií a spoločností. Medzi tie najväčšie patrili:

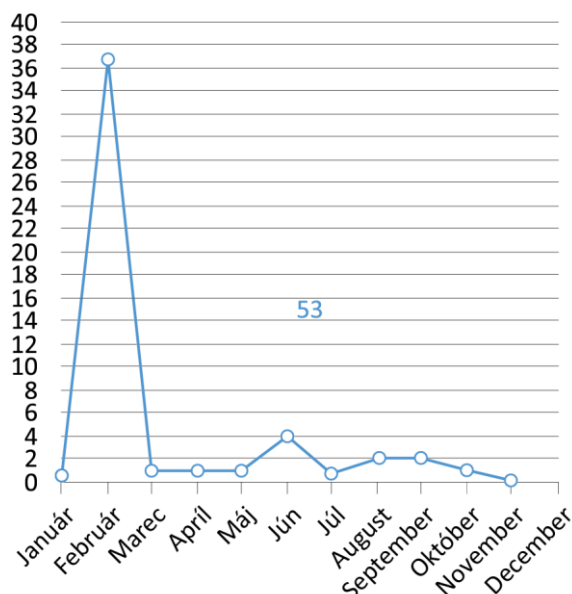
- únik dát z profilov sociálnych sietí, ktoré boli voľne dostupné na internete – viac ako 4 miliardy záznamov,
- uniknutá databáza používateľov spoločnosti Orvibo (riešenia pre inteligentnú domácnosť) – viac ako 2 miliardy záznamov a informácií o používateľoch, ktorých má platforma okolo 1 milióna,
- únik dát spoločnosti TrueDialog (americká telekomunikačná spoločnosť) – viac ako 1 miliarda záznamov vrátane mien a iných citlivých údajov zákazníkov,
- únik informácií o zákazníkoch spoločnosti First American – 885 miliónov záznamov, vrátane citlivých údajov a údajov o hypotékach a pôžičkách.

Slovenská republika

SK-CERT získal od zahraničného partnera zoznam uniknutých prihlasovacích údajov jedného veľkého poskytovateľa e-mailových služieb na Slovensku. Údaje boli získané z riadiaceho C&C (Command and Control) servera zapojeného do botnetu EMOTET. Samotný útočný vektor a ani spôsob získania prihlasovacích údajov sa nepodarilo identifikovať. V spolupráci s prevádzkovateľom zasiahnutej služby boli podniknuté všetky kroky pre úspešné riešenie incidentu a jeho prevencie do budúcnosti. Zasiahnuté subjekty boli bezodkladne o úniku informované.

Boli tiež zaznamenané viaceré väčšie či menšie úniky dát vrátane citlivých údajov z rôznych organizácií. Riešenie týchto incidentov je priebežne monitorované.

Graf č. 6: Úniky dát - počet riešených incidentov v roku 2019. (Zdroj: NCKB SK-CERT).



Útoky na dostupnosť služieb

Útoky na dostupnosť služieb sú veľmi častými a obľúbenými medzi útočníkmi. Denial of Service (DoS) je typ útoku, ktorého cieľom je znepriístupnenie konkrétnej služby pre jej používateľov. Môžu byť vykonávané nedistribúovanou a distribúovanou formou (DDoS – Distributed Denial of Service).

Princíp spočíva v zahltení cieľa dopytmi zo strany útočníka tak, aby služba nezvládla takýto nápor a nedokázala viac odpovedať na akýkoľvek dopyt. Pri nedistribuovanej forme útočník používa nástroje, ktoré dokážu vyprodukovať dostatočný počet dopytov, napríklad pomocou rôznych amplifikačných techník. Pri distribuovanej forme útočník najčastejšie využíva svoju botnetovú sieť a zvyšuje tak počet zariadení, ktoré posielajú dopyty cieľu. Botnetovú sieť si je v dnešnej dobe možné aj prenajať ako službu.

CIELE	ÚTOČNÍCI	DOPAD
kritická infraštruktúra, bankový sektor, verejná správa	hacktivistí štátom sponzorované skupiny kyberteroristi	spomalenie poskytovaných služieb, úplná nedostupnosť poskytovaných služieb

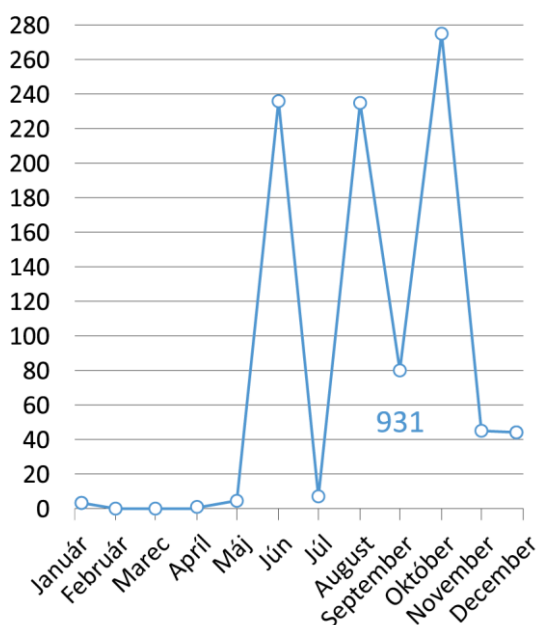
Útoky na dostupnosť služieb 2019 vo svete

V roku 2019 boli zaznamenané útoky využívajúce tzv. amplifikáciu, teda zosilnenie DoS útoku prostredníctvom jedného konkrétneho zariadenia alebo protokolu. Najčastejšie sa vyskytovali amplifikačné útoky, ktoré využívali NTP amplifikáciu (Network Time Protocol), DNS amplifikáciu (Domain Name System) a útoky prostredníctvom TCP SYN flood – útok, pri ktorom útočník posielal dotazy v podobe synchronizačného TCP paketu, čím sa snaží zahltiť cieľové zariadenia.

Slovenská republika

Počas roka 2019 bolo zaznamenaných viacero DDoS útokov najmä na informačné systémy verejnej správy, ale aj na bankový sektor a iné. Väčšina útokov viedla len k spomaleniu poskytovaných služieb. Detegovaný bol iba jeden významnejší incident, pri ktorom došlo k dočasnému prerušeniu dodávky služieb. Samotné útoky boli eliminované nasadením blokovania GEO (geografickej zóny IP adries) na úrovni operátora.

Graf č. 7: Útoky na dostupnosť služby - počet riešených incidentov v roku 2019. (Zdroj: NCKB SK-CERT).



Zneužívanie zraniteľností

Zraniteľnosť je slabé miesto informačného aktíva, procesu, alebo systému. Všeobecne je zraniteľnosťou každá okolnosť, ktorá znižuje odolnosť voči hrozbám. Zraniteľnosť je úmyselná, alebo neúmyselná chyba softvérového produktu, hardvéru alebo procesu, ktorá umožňuje neautorizovaným osobám alebo procesom prístup k aktívam (dáta, softvér, hardvér, ľudia, ...),

znemožňuje autorizovaný prístup k aktívam, či umožňuje neautorizovaným osobám a procesom vyhnúť sa detekcii. Útočníci zneužívajú existujúce a známe zraniteľnosti, ale aj tzv. zraniteľnosti nulového dňa, ktoré si dôkladne strážia a používajú len na útoky na špeciálne ciele. Zneužívanie zraniteľností je súčasťou aj iných typov útokov, ako je napríklad phishing, šírenie malvéru alebo pokusy a úspešné prieniky do systémov.

CIELE	ÚTOČNÍCI	DOPAD
bežní používatelia, Veľké spoločnosti v rôznych sektoroch, kritická infraštruktúra, verejná správa	script kiddies, kyberkriminálni, štátom sponzorované skupiny	možnosť vykonať ľubovoľný kód (neautorizovaný, neplánovaný, škodlivý...), získať administrátorské privilégia alebo privilégia inej používateľskej skupiny alebo užívateľa, zneprístupniť službu alebo produkt, získať neautorizovaný prístup k citlivým dátam na čítanie alebo ich modifikáciu

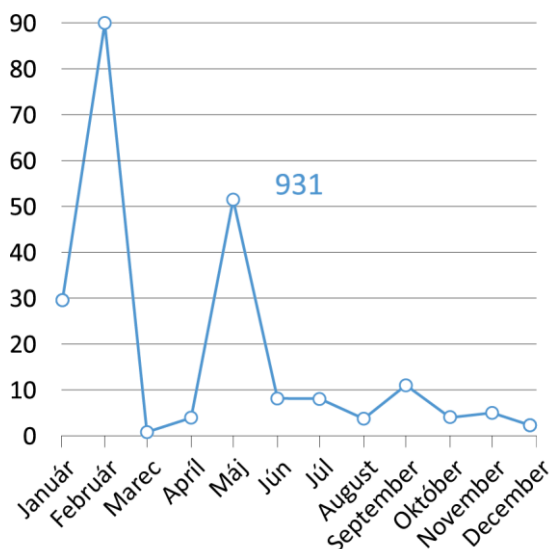
Zneužívanie zraniteľností 2019 vo svete

Na portáli National Vulnerability Database⁴, ktorý prevádzkuje inštitúcia NIST, bolo za rok 2019 uverejnených 17 311 zraniteľností, čo predstavuje v priemere 47 zraniteľností denne. Kritické zraniteľnosti sa vyskytovali naprieč výrobcami a platformami. S rastúcim trhom s inteligentnými a mobilnými zariadeniami došlo aj k objaveniu závažných zraniteľností v tomto segmente. Túto skutočnosť umocňuje fakt, že zneužitie zraniteľností napríklad v IoT segmente má priamy dopad na ich používateľa, častokrát výrobca daný produkt už nepodporuje, zraniteľnosť nie je riešená, pretrváva a informácie o nej sú voľne dostupné.

Slovenská republika

Špecializované spoločnosti zaoberajúce sa kybernetickou bezpečnosťou, najmä bezpečnostným monitoringom a penetračnými testami, nahlásili v priebehu roka 2019 viacero kritických bezpečnostných zraniteľností v aplikáciách používaných a implementovaných v rámci informačných systémov verejnej správy. V spolupráci s vývojármi, prevádzkovateľmi zasiahnutých služieb a jednotkami CSIRT sa podarilo predmetné zraniteľnosti odstrániť nasadením bezpečnostných aktualizácií. Preverovaním situácie nebolo potvrdené žiadne úspešné zneužitie zraniteľností.

Graf č. 8: Zneužívanie zraniteľností - počet riešených incidentov v roku 2019. (Zdroj: NCKB SK-CERT).



Sektorový pohľad

Zákon o kybernetickej bezpečnosti určuje 11 sektorov s dokopy 28 podsektormi. Organizácie v týchto sektoroch prevádzkujú niektoré služby, ktoré sú kritické v rámci informačnej a komunikačnej infraštruktúry – tzv. základné služby. Tieto organizácie (prevádzkovatelia základných služieb) v jednotlivých sektoroch majú podľa zákona o kybernetickej bezpečnosti viaceré povinnosti, ku ktorým patrí aj povinné nahlásovanie kybernetických bezpečnostných incidentov Národnému centru kybernetickej bezpečnosti SK-CERT.

Slovenská republika disponovala k 31. decembru 2019 nasledovnými samostatnými sektorovými jednotkami, akreditovanými podľa zákona o kybernetickej bezpečnosti:

- CSIRT.SK, sektorová CSIRT jednotka pre sektor „Verejná správa“, podsektor „Informačné systémy verejnej správy,
- Centrum kybernetickej obrany Slovenskej republiky.

Sektory Ministerstva hospodárstva Slovenskej republiky (energetika, priemysel) majú uzatvorenú zmluvu o poskytovaní služieb jednotky CSIRT s Národným centrom kybernetickej bezpečnosti SK-CERT a sektor bankovníctva má uzavretú zmluvu o poskytovaní služieb jednotky CSIRT s Úradom podpredsedu vlády Slovenskej republiky pre investície a informatizáciu. Zmluva Ministerstva zdravotníctva Slovenskej republiky s Národným centrom kybernetickej bezpečnosti SK-CERT pre sektor zdravotníctva je tesne pred podpisom.

V ostatných sektoroch a podsektoroch príslušné ústredné orgány nezriadili akreditované sektorové CSIRTy ani neuzatvorili s niektorým z iných sektorových CSIRTov zmluvu o zabezpečení sektora.

Nižšie uvedené sektory boli v roku 2019 z globálneho aj národného hľadiska najviac zasahované kybernetickými bezpečnostnými incidentami.

Bankovníctvo

Sektor bankovníctva je dlhodobo považovaný za kritický a udržiavajúci ekonomickú stabilitu. Pretože v tomto sektore dochádza k manipulácii s finančnými prostriedkami, je mimoriadne zaujímavý z pohľadu útočníkov usilujúcich sa o získanie prostriedkov na podporu svojich ďalších aktivít, vrátane nelegálnych. Vzhľadom na požadovanú vysokú úroveň klientov k bankám patrí bankový sektor medzi najflexibilnejšie a najrýchlejšie reagujúce odvetvia vo vzťahu k vznikajúcim bezpečnostným hrozbám.

Niektorým bankám v súčasnosti hrozí väčšie riziko výpadku poskytovaných služieb kvôli dlhodobému používaniu zastaranej hardvérovej a softvérovej infraštruktúry, než kvôli kybernetickému útoku.

Infraštruktúra

Banky často prevádzkujú svoju vnútornú infraštruktúru oddelenú alebo z väčšej časti oddelenú od internetu, čím sa znižuje riziko potenciálnych kybernetických útokov. V súčasnosti väčšina bánk postupne implementuje tzv. model nulovej dôvery (Zero Trust Model).⁵

Používatelia

Najčastejším vektorom útoku v bankovom sektore je sociálne inžinierstvo, resp. phishing na používateľov ale aj zamestnancov bánk. Útočníci z celého sveta vytvárajú falošné kópie webstránok bánk a snažia sa presvedčiť používateľov na uskutočnenie transakcií, prihlásenie sa do systému alebo o zdieľanie citlivých údajov, ktoré neskôr plánujú využiť na realizáciu ďalších útokov.

Rastúcim fenoménom je aj tzv. carding (nákup tovarov a služieb prostredníctvom ukradnutých údajov platobných kariet). Útočníci získajú údaje z platobnej karty, kúpia na internete tovar/objednajú službu a po reklamácii si nechajú odoslať peniaze na iný účet, prípadne, získaný tovar/službu ďalej predajú.

Aj napriek vysokej úrovni zabezpečenia bánk a promptným reakciám bankových jednotiek CSIRT, boli používatelia bankových služieb v roku 2019 najčastejším cieľom kybernetických útokov. Popularita útokov na klientov bánk je umocnená tým, že 47 % Slovákov využíva internet banking, čo útočníkov motivuje k snahám získavať bankové údaje pomocou keyloggerov (programov, ktoré zaznamenávajú každé stlačenie klávesy na klávesnici a teda napríklad heslá, čísla účtov či iné zaujímavé údaje). V roku 2019 bolo možné sledovať aj rast počtu ľudí na 71 % (Eurostat, 2019), ktorí využívajú mobilný internet. Je pritom všeobecným faktom, že používatelia mobilného internetu sú pri phishingových útokoch zraniteľnejší.

Incident 1

Server poskytujúci služby internetového bankovníctva bol terčom rozsiahleho DDoS útoku o intenzite 2Gbit/s, ktorý trval 6 minút. Počas útoku došlo k podstatnému spomaleniu poskytovaných služieb. Na základe analýzy útočného vektora išlo o NTP amplifikačný DDoS útok. Logy sieťových zariadení zaznamenali spojenia z niekoľko tisícok IP adries z celého sveta. V rámci reaktívnych opatrení bolo na základe geolokácie aktivované blokovanie prichádzajúcich spojení z nebezpečných zahraničných IP adries. V rámci riešenia incidentu boli taktiež rozposlané adresné upozornenia na príslušné ABUSE kontakty.

Incident 2

Neznámemu útočníkovi sa prostredníctvom sofistikovanej phishingovej kampane podarilo previesť finančné prostriedky vo výške rádovo 70 000 eur. Prvá fáza útoku zahrnila rozposielanie falošných phishingových správ v mene banky, v ktorých bol klient upozornený na zmenu v bezpečnostnej politike elektronického bankovníctva a požiadaný o prihlásenie do internet bankingu. Správy obsahovali odkaz na phishingovú stránku imitujúcu stránku banky slúžiacu na prihlasovanie do služieb internet bankingu. Útočník tak bol schopný odchytiť prihlasovacie údaje obete, nasimulovať prihlasovanie do reálneho internet bankingu a od používateľa v nasledujúcej fáze útoku získať aj potvrdzujúci SMS kód. Po získaní všetkých potrebných údajov útočník prostredníctvom mobilnej aplikácie vykonal viacero finančných transakcií, prevažne na zahraničné účty. V rámci reaktívnych opatrení banka zablokovala viacero podozrivých transakcií, boli podané viaceré trestné oznámenia a phishingový obsah bol v spolupráci s partnermi a CSIRT jednotkami odstránený. Na záver sa podarilo získať aj vzorky škodlivého kódu, ktorý útočník použil na získavanie údajov obetí.

Elektronická komunikácia a digitálna infraštruktúra

Sektory elektronickej komunikácie a digitálnej infraštruktúry sa dajú z pohľadu kybernetickej bezpečnosti považovať za mimoriadne kritické sektory. Typické služby v týchto sektoroch sú

⁵ Tento model hovorí o prístupe organizácií k bezpečnosti na základe nulovej dôvery k subjektom vo vnútri a aj mimo organizácie, založenom na dôslednej aplikácii politík prístupov a monitoringu zariadení v sieti.

nevyhnutné pre samotnú existenciu siete internet, pre pripájanie užívateľov, pre výmenu informácií a pod. Zdieľanie dát prostredníctvom internetu spustilo 4. priemyselnú revolúciu a tieto informácie je možné využiť v prospech spoločnosti, ale aj na realizáciu kybernetických bezpečnostných útokov. Postupná smartifikácia štátov, miest a obcí, ale aj bežných súčastí ľudského života vedie k významnému zvýšeniu kvality života. Na druhej strane prináša aj nové výzvy, najmä postupné zavádzanie technológie 5G, centralizáciu informačných a riadiacich systémov verejnej a súkromnej správy a neustále zvyšujúcu sa závislosť spoločnosti od technického vybavenia.

Infraštruktúra

Podobne ako pri bankovníctve, elektronické komunikácie aj digitálna infraštruktúra patria z infraštruktúrneho hľadiska a z hľadiska detekčných schopností medzi sektory s vysokou úrovňou zabezpečenia. Najväčší telekomunikační operátori majú často vlastné jednotky CSIRT, ktoré medzi sebou komunikujú a zdieľajú informácie, čo podstatne urýchľuje proces identifikácie a riešenia kybernetických útokov. Aj sektor elektronických komunikácií postupne zavádza politiku nulovej dôvery, pomocou ktorého sa bránia aj tzv. supply chain útokom. Infraštruktúru, ktorú nemôžu oddeliť od internetu, dôsledne monitorujú prostredníctvom bezpečnostných a sieťových prvkov. Priemyselné systémy používané v predmetných sektoroch sú pravidelne kontrolované penetračným testovaním a ich výrobcovia sú tlačení do vydávania bezpečnostných aktualizácií. Schopnosť a ochota výrobcov rýchlo opravovať detegované zraniteľnosti vo svojich produktoch zároveň patrí k veľkému riziku v sektoroch elektronickej komunikácie a digitálnej infraštruktúry.

Používatelia

Pri kybernetickej bezpečnosti telekomunikačných služieb sú najkritickejším prvkom koncové zariadenia samotných používateľov. V roku 2019 vzrástol počet útokov na koncové zariadenia. Útoky boli dôsledkom nedostatočného povedomia o kybernetickej bezpečnosti a neochoty koncových používateľov aktualizovať svoje systémy aj v prípade, že sú opravy zraniteľností dostupné.

Takmer polovica kybernetických bezpečnostných zraniteľností má v roku 2019 na internete zverejnený návod na spôsob ich ošetrenia a viac než tretina nemá dostupné riešenie (oprava, patch, update).

Často využívaným útočným vektorom je zneužitie známych bezpečnostných zraniteľností v systémoch na manažovanie obsahu (CMS – Content Management System), medzi ktoré patrí napr. WordPress, Joomla alebo Drupal. V roku 2019 vývojári CMS systémov vydávali v priemere 2 až 3 aktualizácie mesačne, ktoré opravili nespočetné množstvo bezpečnostných zraniteľností. Počet objavených zraniteľností v systémoch CMS oproti roku 2018 stúpol o 68 % a špecificky zraniteľnosti v najpoužívanejšom systéme Wordpress stúpol medziročne o 143 %. Informácie a technické detaily o zraniteľnostiach CMS systémov sa predávali na čiernom trhu, iné boli zverejnené na internete a útočníci ich zneužívali na získanie čiastočnej alebo úplnej kontroly nad webstránkami, prístup k citlivým údajom a následné umiestnenie škodlivého alebo phishingového obsahu. Umiestnený obsah najčastejšie slúži na šírenie politickej propagandy, ťaženie kryptomien ale aj distribúciu malvéru.

Energetika

Sektor energetiky je spomedzi kritických sektorov najdôležitejším sektorom sociálno-ekonomickej stability. Je podmienkou na fungovanie všetkých kritických sektorov a prežitie spoločnosti.

Na rozdiel od ostatných kritických sektorov, v energetike je ohrozenie infraštruktúry zo strany koncových zariadení používateľov

strana

APT

Kvôli dôležitosti energií (elektrickej aj tepelnej) na zachovanie funkčnej ekonomiky je sektor energetiky najčastejším cieľom APT skupín.

Aj krátky výpadok energetiky/energie by mohol spôsobiť:

- straty na životoch pre pacientov nemocníc v kritickom zdravotnom stave,
- obmedzenie mobility občanov,
- straty zamestnania,
- pád ekonomiky,
- nedôveru občanov voči vláde.

najmenším rizikom, avšak strata energie by pre ne bola devastačná. Útok na energetiku sa dá kvôli počtu ovplyvnených súčastí ľudského života považovať za akt hybridnej vojny s euroatlantickými dôsledkami.

Infraštruktúra

Decentralizácia výroby elektrickej energie, ktorá spôsobuje nárast využívania obnoviteľných zdrojov zvyšuje počet OT systémov a vytvára nové výzvy v oblasti kybernetickej bezpečnosti. Tento jav zväčšuje počet cieľov pre potenciálnych útočníkov. Na druhej strane môže zvýšiť aj ich odolnosť a preto bude aj v roku 2020 najkritickejším podsektorom práve distribúcia a skladovanie energie.

V roku 2019 počet hlásených kybernetických bezpečnostných incidentov na energetický sektor Slovenskej republiky vzrástol o 600 %, čo poukazuje najmä na zlepšenie schopnosti detegovať incidenty u prevádzkovateľov. Na náraste počtu incidentov sa ale podpísal nárast počtu objavených zraniteľností na prevádzkovaných systémoch najmä počtu zraniteľností priemyselných (OT, SCADA) systémov. V roku 2019 celosvetovo dominovali rôzne formy útokov zneužívajúce bezpečnostné zraniteľnosti s následkom vzdialeného spustenia ľubovoľného kódu (28 % všetkých zraniteľností).

Incident 1

V roku 2019 bol detegovaný prípad rozsiahlej a po technickej stránke vysoko sofistikovanej phishingovej kampane slúžiacej na získavanie citlivých údajov obetí. Útočník zneužíval obchodné meno spoločnosti v energetickom sektore. V mene zasiahnutej spoločnosti rozposlal na viacero adries e-maily obsahujúce výzvu na úhradu nedoplatku a údajnú faktúru vo forme elektronickej prílohy. Po otvorení prílohy došlo k infekcii zariadenia obeť unikátnou rodinou malvéru, ktorá slúžila na získavanie citlivých údajov. Malvér mal v sebe implementované viaceré funkcionality na zachytávanie používateľských vstupov, ako napríklad keylogging a vytváranie screenshotov obrazovky. Z pohľadu technickej realizácie bola útočníkova infraštruktúra plne automatizovaná a umožňovala okamžité odoslanie phishingových správ po dokončení kompilácie škodlivého kódu. V rámci riešenia incidentu bolo podané trestné oznámenie.

Incident 2

V rámci vládnej siete GOVNET boli detegované viaceré pravidelne sa opakujúce spojenia, ktoré bezpečnostné prvky vyhodnotili ako podozrivé. Spojenia boli iniciované z IP adresného rozsahu pridelenému subjektu v oblasti energetiky. Riešenie incidentu odhalilo, že sa jednalo o IP adresy dynamicky pridelované v rámci vnútropodnikovej wifi siete určenej pre návštevníkov spoločnosti. V spolupráci s IT oddelením spoločnosti sa podarilo identifikovať koncové zariadenie návštevníka, ktoré bolo infikované malvérom. Malvér bol úspešne odstránený a na úrovni zasiahnutej spoločnosti došlo v rámci prevencie k nasadeniu proxy servera a IPS zariadenia. Nasadenie týchto prvkov viedlo k zvýšeniu detekčných schopností spoločnosti.

Verejná správa

Sektor verejnej správy a jeho podsektory sú pre kybernetických útočníkov typickým cieľom. Verejná správa disponuje informáciami o občanoch, rozvojových projektoch v procese prípravy, rozpracovanými stratégiami (aj ekonomického aj bezpečnostného charakteru), verejnými financiami a nespočetnými ďalšími prvkami záujmu pre potenciálnych útočníkov.

Zraniteľné webstránky a aplikácie samospráv sa môžu stať terčom útočníkov a môžu byť zneužívané na šírenie propagandy APT skupinami. V Slovenskej republike medziročne stúpol počet ľudí využívajúcich internet na komunikáciu s verejnými autoritami o 8 % (Eurostat, 2019). V roku 2019 v SR túto formu komunikácie využívalo 59 % ľudí. Užívatelia používajú aspoň jednu z nasledujúcich služieb: získavanie informácií z webstránok samospráv, sťahovanie oficiálnych formulárov a ich elektronické podávanie.

Kybernetický útok na verejnú správu by mohol spôsobiť sociálno-ekonomickú nestabilitu, dočasnú stratu alebo ochromenie základných funkcií miest a obcí (napr. prerozdeľovanie verejných financií,

poskytovanie sociálnych služieb, efektívnosť výučby na školách) a nedôveru občanov voči štátu. Na rozdiel od útoku na energetický sektor, útok na verejnú správu nemusí verejnosť považovať za osobný a jeho následky nebude vytykať útočníkovi, ale verejným inštitúciám.

Infraštruktúra

V roku 2019 bolo možné sledovať rapídny nárast hlásených aj automaticky detegovaných útokov na infraštruktúru verejnej správy.

Verejná správa na Slovensku bola aj v roku 2019 terčom sociálneho inžinierstva, najmä phishingových a spear-phishingových útokov.

Najnebezpečnejším fenoménom vo svete sa v roku 2019 stali ransomvérové útoky. Bolo možné konštatovať, že väčšina samospráv nemá dostatočne zabezpečené systémy, nemá implementovaný proces zálohovania údajov a preto ransomvérové útoky sú devastujúce. Najčastejším vstupným bodom do zraniteľných systémov sú neinformovaní zamestnanci.

Nedostatok povedomia o kybernetickej bezpečnosti, neznalosť zákona, jeho ignorovanie alebo laxný prístup riadiacich zamestnancov a štatutárov je kritickým faktorom nízkej úrovne odolnosti organizácii verejnej správy. Ďalším problémovým faktorom je nedostatočné finančné zabezpečenie potrebných investičných ale aj prevádzkových potrieb verejnej správy v oblasti kybernetickej bezpečnosti. Dôležitým faktorom je aj kritický nedostatok odborníkov na kybernetickú bezpečnosť v Slovenskej republike všeobecne. Verejná správa aj z dôvodu nedostatku finančných prostriedkov v oblasti IT prevádzkuje zastaraný hardvér alebo softvér. Vážnym problémom je aj skutočnosť, že zamestnanci nedodržiavajú zásady kybernetickej hygieny a bezpečnú politiku hesiel.

Ako už bolo spomenuté v časti Elektronická komunikácia a digitálna infraštruktúra, väčšina regiónov, miest a obcí volá po smartifikácii, zavádza alebo plánuje zaviesť napr. inteligentné merače spotreby, prepojenú dopravu, informačné tabule, zdieľanie informácií. Mestá ale aj inštitúcie chcú nasadzovať mobilné aplikácie hlásiace špeciálne situácie, napríklad žiadosti o pomoc, prehľady o doprave, kvalite ovzdušia, udalostiach, plánoch, hlasovaniach. Napriek zákonnej povinnosti (zákon o ITVS) pri plánovaní a následnej implementácii IT systémov vo verejnej správe veľmi často chýba ucelené riešenie kybernetickej bezpečnosti (technickej, prevádzkovej alebo procesnej). Problematika častokrát nie je riešená vôbec, alebo je riešená len formálne a nedostatočne (len papierovo).

Incident 1

Časť súborov na serveroch obecného úradu bola zašifrovaná prostredníctvom ransomvéru rodiny Wesker. Útočník požadoval výkupné vo výške 4 000 eur. Kritické dáta z databázy obyvateľov neboli negatívne zasiahnuté, pretože obecný úrad na pravidelnej báze vykonáva zálohovanie dát. Technická analýza odhalila, že útočník sa na server dostal prostredníctvom nezabezpečeného RDP protokolu, na napadnutom zariadení prostredníctvom anonymizačnej proxy stiahol a následne spustil ransomvér, ktorý vykonal šifrovanie súborov. Šifrovací algoritmus sa nepodarilo prelomiť, ale po odstránení malvéru a aktualizácii bezpečnostnej politiky architektúry ICT došlo k obnove dát zo zálohy. Incident poukázal na pokračujúci trend zneužívania nesprávne konfigurovaných služieb a protokolov, ktorých prevádzka by mala byť podrobne monitorovaná alebo úplne oddelená od internetu.

Incident 2

Webové sídlo jednej zo štátnych inštitúcií bolo terčom rozsiahlych DDoS útokov, ktoré spôsobili spomalenie a čiastočné prerušenie poskytovaných služieb. Po niekoľkých minútach sa podarilo obnoviť plnú dostupnosť portálu. Na základe technickej analýzy išlo o kombináciu viacerých útočných vektorov slúžiacich na amplifikáciu DDoS. Na základe logov boli identifikované ABUSE kontakty na prevádzkovateľov IP adries zneužitých na realizáciu útoku, ktoré boli následne kontaktované. Na základe spätnej väzby bola väčšina predmetných zariadení infikovaná malvérom, ktorý ich zapájal do rozsiahlej, bližšie neidentifikovanej botnet siete.

V roku 2019 sa viac ako 100 vládnych agentúr v USA stalo terčom ransomvérového útoku.

Mesto La Porte v štáte Indiana bolo pre obnovenie dát nútené zaplatiť útočníkovi 130 000 amerických dolárov.

Zdravotníctvo

Chyby v zabezpečení, systémy otvorené voči internetu, starý a neaktualizovaný softvér, úplná absencia kybernetickej hygieny (až ignorovanie bazálnych bezpečnostných povinností) zamestnancov alebo ďalšie nedostatky v kybernetickej bezpečnosti môžu mať v sektore zdravotníctva mimoriadne vážne následky (môžu viesť k závažným zdravotným následkom až k smrti). Rovnako ako v samospráve, aj v zdravotníctve prebieha smartifikácia, avšak pri zdravotníctve je možné s úplnou istotou konštatovať, že ich zavádzanie v drvivej väčšine nie je riešené v súlade s princípmi kybernetickej bezpečnosti. Príkladom týchto technológií môžu byť inteligentné monitory stavu pacienta z kancelárie lekára, automatizované dávkovače, centralizované dátové úložiská, alarmy stavu pacientov a iné systémy, ktorých napadnutie útočníkom, resp. pozmenenie údajov, priamo vedie k život ohrozujúcim situáciám.

Infraštruktúra

Aj v roku 2019 bolo možné sledovať kritické nedostatky v kybernetickej bezpečnosti zdravotníctva a to nielen v Slovenskej republike. Zdravotníctvo je vystavené kybernetickým bezpečnostným zraniteľnostiam, medzi ktoré v roku 2019 patrili zraniteľnosti typu jednoducho prístupná zdravotnícka technika z internetu, do siete pripojené pumpy na liečivá, zraniteľné bluetooth vstupy na dávkovače inzulínu, moderné prístroje napojené na zastarané počítače, absencia kontroly prístupu (dôslednej identifikácii a autorizácii užívateľov). Väčšina nemocníc a polikliník z pohľadu kybernetickej bezpečnosti funguje tak, ako keby žiadne bezpečnostné problémy neexistovali.

Zdravotné údaje patria na čiernom trhu k najhodnotnejším. Zvyšujú dôveryhodnosť phishingových útokov a v kombinácii s ostatnými informáciami môžu byť použité ako nástroj vydierania.

Postupy zavádzania nových technológií sú nekonceptné a systémy sú prepojené tak, že ak kybernetický útočník zistí nejakú zraniteľnosť v jednom prístroji, môže sa stať, že s ňou ovládne aj systémy, ktoré sú s ním prepojené. Zdravotníctvo v Slovenskej republike bolo v roku 2019 zasiahnuté viacerými ransomvérovými bezpečnostnými incidentmi (únik informácií, ťaženie kryptomien), avšak najčastejším druhom incidentov, tak ako aj v iných sektoroch, bol phishing.

Incident 1

Medzinárodná sieť jednotiek CSIRT identifikovala z internetu voľne prístupné zariadenie používajúce DICOM protokol slúžiaci na prácu s medicínskymi dátami. Na uvedenej IP adrese bola rovnako identifikovaná zastaraná a neaktualizovaná verzia OpenSSH protokolu. Obe tieto skutočnosti predstavovali potenciálne bezpečnostné riziko, ktoré by útočník mohol zneužiť na získanie neoprávneného prístupu k citlivým údajom uloženým na servery. V rámci riešenia incidentu bol upovedomený prevádzkovateľ predmetnej IP, ktorý situáciu vyriešil aktualizáciou predmetného protokolu a oddelením zariadenia od internetu. Preverovanie logov z bezpečnostných prvkov nepreukázalo žiadnu škodlivú aktivitu ani únik dát.

Incident 2

Jeden zo serverov nemocnice bol infikovaný ransomvérom, ktorý zašifroval všetky zdieľané zložky na serveroch. Databáza pacientov nebola činnosťou ransomvéru zasiahnutá, avšak kybernetický útok spôsobil obmedzenie funkcionality viac ako 50 % počítačov v rámci infraštruktúry nemocnice. V spolupráci s manažmentom nemocnice bol na účely forenznej analýzy zapožičaný server. Na základe výsledkov analýzy sa nepodarilo obnoviť šifrovaný obsah, boli však nájdené známky potenciálneho úniku citlivých údajov a časti zdravotnej dokumentácie pacientov a zamestnancov nemocnice ako súčasť iného, nedetegovaného staršieho incidentu. Útočník na prienik do systému zneužil nedostatočnú implementáciu bezpečnostných mechanizmov a nesprávny návrh topológie

nemocničnej siete. Uvedené nedostatky boli odstránené v spolupráci s IT oddelením nemocnice. V súvislosti s týmto incidentom bolo podané trestné oznámenie.

Ostatné sektory

Ústredný orgán pre sektor priemyslu začal v roku 2019 aktívne participovať a vyvíjať aktivity v oblasti kybernetickej bezpečnosti a budovania spôsobilostí.

V rámci aktivít ostatných sektorov podľa zákona o kybernetickej bezpečnosti neprišlo v roku 2019 k významnému posunu v oblasti kybernetickej bezpečnosti. Ústredné orgány týchto sektorov neboli v tejto oblasti veľmi aktívne a Národné centrum kybernetickej bezpečnosti SK-CERT aj napriek vyvíjanej snahe nedostávalo relevantné informácie o stave kybernetickej bezpečnosti v týchto sektorochoch.

Aktivity a opatrenia

Legislatíva

Transpozíciou Smernice 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 (smernica NIS) do slovenskej legislatívy vznikol ucelený rámec pre kybernetickú bezpečnosť v Slovenskej republike.

Cieľom smernice NIS je dosiahnutie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v rámci EÚ. Takúto úroveň by jednotlivé štáty svojimi čiastkovými úpravami neboli schopné dostatočne naplniť. Smernica NIS ponúka ucelený rámec riešenia kybernetickej bezpečnosti na strategickej i operatívnej úrovni. Takisto uvádza dôležité sektory, ktoré majú špeciálny význam v oblasti kybernetickej bezpečnosti. V tomto prípade však smernica NIS dovoľuje členským štátom pridávať sektory špecifické pre jednotlivé krajiny, ktoré sú taktiež kriticky dôležité pri zabezpečovaní kontinuálnej a efektívnej kybernetickej bezpečnosti v krajine.

POROVNANIE SEKTOROV V SMERNICI NIS A V ZÁKONE O KYBERNETICKEJ BEZPEČNOSTI				
Podsektor			NIS	Zákon
Bankovníctvo		MF SR	✓	✓
Doprava	Letecká doprava	MDaV SR	✓	✓
	Železničná doprava	MDaV SR	✓	✓
	Vodná doprava	MDaV SR	✓	✓
	Cestná doprava	MDaV SR	✓	✓
Digitálna infraštruktúra		NBÚ	✓	✓
Elektronické komunikácie	Satelitná komunikácia	MDaV SR		✓
	Siete a služby pevných a mobilných elektronických komunikácií	MDaV SR		✓
Infraštruktúra finančných trhov		MF SR	✓	✓
Pošta		MDaV SR		✓
Energetika	Baníctvo	MH SR		✓
	Elektroenergetika	MH SR	✓	✓
	Ropa a ropné produkty	MH SR	✓	✓
	Plynárenstvo	MH SR	✓	✓
	Tepelná energetika	MH SR		✓
Priemysel	Farmaceutický priemysel	MH SR		✓
	Hutnícky priemysel	MH SR		✓
	Chemický priemysel	MH SR		✓
	Inteligentný priemysel	MH SR		✓
Zdravotníctvo	Zdravotnícke zariadenia (vrátane nemocníc a súkromných kliník)	MZ SR	✓	✓
Voda a atmosféra	Meteorologická služba	MŽP SR		✓
	Vodné stavby	MŽP SR		✓
	Zabezpečovanie pitnej vody	MŽP SR	✓	✓
Verejná správa	Bezpečnosť	MV SR		✓
	Informačné systémy verejnej správy	ÚPVII		✓
	Obrana	MO SR		✓
	Spravodajské služby	SIS / VS		✓
	Utajované skutočnosti	NBÚ		✓

Členské štáty mali povinnosť transponovať smernicu NIS do 9. mája 2018, pričom Slovenská republika si túto povinnosť splnila v termíne (zákon bol účinný od 1. apríla 2018) ako jeden z veľmi mála členských štátov EÚ.

Kybernetická bezpečnosť je teda inštitucionálne a legislatívne definovaná zákonom o kybernetickej bezpečnosti a príslušnými vyhláškami. Momentálne sú platné a účinné tieto právne akty:

Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov
Vyhláška Národného bezpečnostného úradu č. 166/2018 Z. z. o podrobnostiach o technickom, technologickom a personálnom vybavení jednotky pre riešenie kybernetických bezpečnostných incidentov
Vyhláška Národného bezpečnostného úradu č. 165/2018 Z. z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov
Vyhláška Národného bezpečnostného úradu č. 164/2018 Z. z., ktorou sa určujú identifikačné kritériá prevádzkovej služby (kritériá základnej služby)
Vyhláška Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení
Vyhláška Národného bezpečnostného úradu č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora

Počas roka 2019 úrad intenzívne pracoval v legislatívnej oblasti, najmä na vyhláške o audite a znalostnom štandarde audítora. Takisto počas roka pripomienkoval viacero právnych aktov, ktoré súviseli s kybernetickou bezpečnosťou a dopĺňali tak legislatívny rámec v tejto oblasti.

Spolupráca s prevádzkovateľmi a poskytovateľmi

Prevádzkovateľ základnej služby Právnická osoba, ktorá prevádzkuje aspoň jednu základnú službu.	Poskytovateľ digitálnej služby Právnická osoba alebo fyzická osoba – podnikateľ, ktorá poskytuje digitálnu službu v niektorej z oblastí podľa zákona o kybernetickej bezpečnosti a zároveň zamestnáva aspoň 50 zamestnancov a má ročný obrat alebo celkovú ročnú bilanciáciu viac ako 10 000 000 eur.
Základná služba Služba v niektorom z určených sektorov alebo podsektorov, ktorej ohrozením alebo narušením jej spoľahlivosti a funkčnosti v dôsledku kybernetického bezpečnostného incidentu by mohol nastať závažný vplyv na dôležité alebo jednoduchým spôsobom nenahraditeľné služby občanom či podnikateľom a tým aj nepriaznivý vplyv na kvalitu života obyvateľov z hľadiska ochrany ich života, zdravia, bezpečnosti a majetku ale tiež podnikateľského prostredia.	Digitálna služba Služba online trhoviska, cloud computingu alebo internetového vyhľadávača.

V roku 2019 úrad pokračoval v úzkej spolupráci s prevádzkovateľmi základných služieb a poskytovateľmi digitálnych služieb. Úrad poskytoval jednotlivým subjektom najmä metodickú pomoc pri aplikácii zákona. Zástupcovia úradu sa takisto na pravidelnej báze stretávali so zástupcami prevádzkovateľov základných služieb a poskytovateľmi digitálnych služieb. Na týchto stretnutiach boli diskutované praktické problémy pri implementácii zákonných požiadaviek a úrad takýmto spôsobom získaval spätnú väzbu od subjektov, na základe ktorej môže v budúcnosti poskytovať kvalitnejšie služby.

Jednotliví prevádzkovatelia základných služieb a poskytovatelia digitálnych služieb sú zaradení v zozname. K 31. decembru 2019 bolo do zoznamu zaradených celkovo 243 prevádzkovateľov základných služieb a 12 poskytovateľov digitálnych služieb.

PREVÁDZKOVATELIA ZÁKLADNÝCH SLUŽIEB – ROZDELENIE NA SEKTORY		
Sektor	Podsektor	Počet prevádzkovateľov
Bankovníctvo		14
Infraštruktúra finančných trhov		1
Digitálna infraštruktúra		17
Doprava	Cestná doprava	1
	Letecká doprava	9
	Železničná doprava	3
Energetika	Elektroenergetika	9
	Plynárenstvo	6
	Ropa a ropné produkty	2
	Tepelná energetika	5
Pošta	Poskytovanie poštových služieb, poštový platobný styk a obstarávateľská činnosť	3
Priemysel	Chemický priemysel	1
	Farmaceutický priemysel	2
Verejná správa	Informačné systémy verejnej správy	80
Voda a atmosféra	Vodné stavby	1
Voda a atmosféra	Zabezpečovanie pitnej vody	15
Zdravotníctvo	Laboratórne služby, Poskytovanie zdravotnej starostlivosti	1
	Zdravotnícke zariadenia	73
Spolu		243

POSKYTOVATELIA DIGITÁLNYCH SLUŽIEB	
Digitálna služba	Počet poskytovateľov
Online trhovisko	7
Cloud computing	8
Internetový vyhľadávač	0
Spolu⁶	12

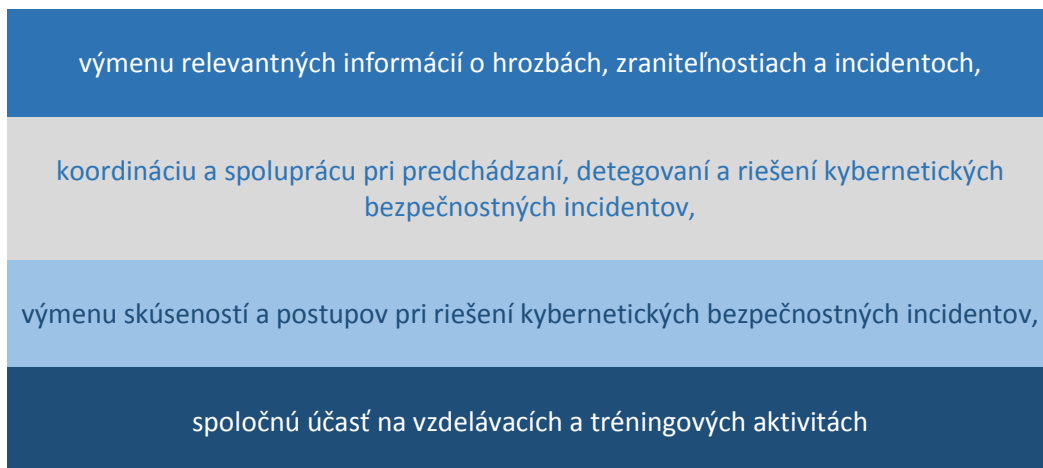
⁶ Niektorí z poskytovateľov sú poskytovateľmi dvoch digitálnych služieb.

Národné a medzinárodné aktivity a spolupráca

Kybernetická bezpečnosť je najmä o dobre fungujúcej spolupráci medzi partnermi a subjektami, ktoré zabezpečujú čiastkové úlohy v tejto oblasti.

Na národnej úrovni to bola najmä vzájomná spolupráca medzi Národným centrom kybernetickej bezpečnosti SK-CERT, Úradom podpredsedu vlády Slovenskej republiky pre investície a informatizáciu, Národnou agentúrou pre sieťové a elektronické služby, Slovenskou informačnou službou, Vojenským spravodajstvom a Ministerstvom zahraničných vecí a európskych záležitostí Slovenskej republiky. Intenzívna spolupráca takisto prebiehala s prevádzkovateľmi základných služieb, poskytovateľmi digitálnych služieb a súkromnými jednotkami CSIRT a profesijnými združeniami (najmä Asociáciou kybernetickej bezpečnosti a ISACA Slovensko).

Táto spolupráca sa zameriavala najmä na



Jednotlivé subjekty, najmä Národné centrum kybernetickej bezpečnosti SK-CERT, takisto zintenzívnilo spoluprácu so svojimi medzinárodnými partnermi – inými národnými a sektorovými jednotkami CSIRT v Európe a vo svete.

V rámci národnej spolupráce s jednotkami CSIRT Národné centrum kybernetickej bezpečnosti SK-CERT spolupracovalo najmä so sektorovými CSIRT jednotkami, CSIRT jednotkou pre podsektor „Informačné systémy verejnej správy“ CSIRT.SK a s Centrom kybernetickej obrany Slovenskej republiky, ale aj s ostatnými CSIRT jednotkami, napríklad s GOV CERT SK v agentúre NASES, VOID SOC a Binconf CDC.

Počas predsedníctva Slovenskej republiky v Organizácii pre bezpečnosť a spoluprácu v Európe (OBSE) bola jednou z hlavných priorít aj oblasť kybernetickej bezpečnosti. Počas predsedníctva zástupcovia Slovenskej republiky (Národný bezpečnostný úrad prostredníctvom Národného centra kybernetickej bezpečnosti SK-CERT, Ministerstvo zahraničných vecí a európskych záležitostí SR, Úrad podpredsedu vlády SR pre investície a informatizáciu, akademická obec a takisto aj súkromný sektor) reprezentovali Slovenskú republiku v expertných skupinách, zúčastňovali sa odborných konferencií a prispievali tak k celkovému zvýšeniu úrovne kybernetickej bezpečnosti v tomto regióne. Ako príklad možno uviesť konferenciu s názvom „Bezpečnejšia kybernetická/IKT budúcnosť: Úloha OBSE pri podpore regionálnej kybernetickej bezpečnosti“, ktorá sa uskutočnila v Bratislave 17. - 18. júna 2019. Konferencia bola zameraná na bezpečnosť informačno-komunikačných technológií (IKT) a kybernetického priestoru. Celkovo sa konferencie zúčastnilo 220 účastníkov z 36 krajín a množstvo medzinárodných organizácií. Obsahovo sa konferencia venovala zhodnoteniu súčasného stavu kybernetických aktivít na národnej a medzinárodnej úrovni, implementácii kybernetických CBMs v OBSE, ochrane kritickej infraštruktúry spojenej s cvičnou simuláciou kybernetického útoku,

bezpečnosti využívania umelej inteligencie, evolúcii a rozvoju spoločných stratégií v spolupráci s medzinárodnými organizáciami a identifikácii jestvujúcich medzier a výziev pri ich implementácii.

Slovenská republika sa prostredníctvom Národného centra kybernetickej bezpečnosti SK-CERT takisto zúčastňovala medzinárodných pracovných skupín Európskej komisie, NATO a OBSE, kde zástupcovia jednotlivých kompetentných orgánov hájili záujmy Slovenskej republiky v otázkach kybernetickej bezpečnosti.

Národné centrum kybernetickej bezpečnosti SK-CERT reprezentovalo Slovenskú republiku aj vo viacerých iných medzinárodných formátoch. Aktívne sa zúčastňovalo stretnutí vedenia agentúry ENISA, zástupca SK-CERT reprezentoval Slovenskú republiku aj v management board a executive board tejto agentúry. SK-CERT ďalej aktívne pôsobil aj v medzinárodných organizáciách, združujúcich CSIRT jednotky, a to hlavne v EU CSIRT Network, organizácii Trusted Introducer a svetovom združení CSIRT jednotiek FIRST (Forum of Incident Response and Security Teams).

V rámci hodnotenia spôsobilostí a vyspelosti Slovenskej republiky v oblasti kybernetickej bezpečnosti v roku 2019 Slovenská republika dosiahla niekoľko úspechov, z ktorých najdôležitejším bolo umiestnenie v ITU Global Cyber Security Index 2018. Slovenská republika sa v GCI indexe posunula o 36 miest oproti roku 2017 a obsadila 45. miesto. V ďalšom významnom indexe, National Cyber Security Index (NCSI), sa Slovenská republika v roku 2019 nachádzala v TOP 10 krajín sveta. Takisto bolo zverejnené aj hodnotenie Slovak Republic Cyber Readiness at a Glance, ktoré vypracovala nezisková organizácia Potomac Institute for Policy Studies v spolupráci s mimovládnu organizáciou Globsec a podporou Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu.

Národný bezpečnostný úrad prostredníctvom Národného centra kybernetickej bezpečnosti SK-CERT v roku 2019 zintenzívnil spoluprácu so všetkými svojimi partnermi, vrátane verejného a súkromného sektora a akademickej obce a v rámci jeho aktivít kontinuálne posilňoval úroveň kybernetickej bezpečnosti v rámci slovenského kybernetického priestoru.

Národné centrum kybernetickej bezpečnosti SK-CERT

Národný bezpečnostný úrad 1. septembra 2019 zriadil Národné centrum kybernetickej bezpečnosti SK-CERT (NCKB SK-CERT) transformáciou Národnej jednotky SK-CERT.

Zriadením Národného centra kybernetickej bezpečnosti SK-CERT úrad splnil úlohu Akčného plánu realizácie Koncepcie kybernetickej bezpečnosti SR 2015–2020.

NCKB SK-CERT zabezpečuje nielen služby spojené s riadením bezpečnostných incidentov, odstraňovaním ich následkov a následnou obnovou činnosti informačných systémov v spolupráci s vlastníkmi a prevádzkovateľmi týchto systémov, ale aj výkon analytických činností, výskumu, rozširovania bezpečnostného povedomia a vzdelávania v oblasti kybernetickej bezpečnosti.

NCKB SK-CERT následne získalo v mesiaci november 2019 najvyšší stupeň vyspelosti jednotky CSIRT, tzv. „Advanced Status“ v rámci siete EU CSIRT Network. Vyspelosť jednotky CSIRT podľa kritérií Európskej agentúry pre kybernetickú bezpečnosť (ENISA) je merateľný súbor parametrov z rôznych oblastí, ktoré sú v rámci jednotky riešené odporúčaným spôsobom. A práve spôsob a vyspelosť riešenia jednotlivých parametrov určuje, akú mieru vyspelosti jednotka CSIRT má. ENISA určila tri kategórie vyspelosti: Basic, Intermediate a Advanced. Pre každú úroveň sú nastavené požiadavky a jednotka, ktorá nespĺňa všetky vstupné požiadavky na určenej úrovni (podľa metodiky SIM3), nedosiahne ani jednu z troch úrovní.

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Úrad zriaďovacou listinou, vydanou 16. decembra 2019 rozhodnutím riaditeľa úradu podľa zákona č. 523/2004 Z. z. o rozpočtových pravidlách verejnej správy, zriadil Kompetenčné a certifikačné centrum kybernetickej bezpečnosti (KCKKB). Vznik kompetenčného centra vychádza aj z návrhu nariadenia EP a Rady, ktorým sa zriaďuje Európske centrum odvetvových, technologických a

výskumných kompetencií v oblasti kybernetickej bezpečnosti a sieť národných koordinačných centier. Tematicky ďalej vychádza z návrhu nariadenia o zriadení programu Digitálna Európa a zo slovenskej stratégie digitálnej transformácie schválenej vládou v roku 2019.

Kompetenčné centrum bolo vytvorené na plnenie úloh národného odvetvového, technologického a výskumného centra v oblasti kybernetickej bezpečnosti, konkrétne na:

plnenie úloh certifikačného orgánu podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti,
činnosti autorizovanej osoby podľa zákona č. 215/2004 Z. z. o ochrane utajovaných skutočností,
zabezpečenie služieb súvisiacich s organizáciou a technickým zabezpečením vzdelávacích aktivít pre zriaďovateľa,
zónové merania a merania nežiadúceho elektromagnetického vyžarovania,
vykonávanie znaleckej a expertíznej činnosti,
vykonávanie vedeckej, výskumnej činnosti a vývoja v oblasti kybernetickej bezpečnosti a informačno-komunikačných technológií,
konzultačnú činnosť v oblasti ochrany utajovaných skutočností, kybernetickej bezpečnosti a dôveryhodných služieb,
organizovanie vzdelávacích podujatí, kurzov, školení a seminárov

KCKKB začalo pôsobiť od 1. januára 2020 ako príspevková organizácia Národného bezpečnostného úradu. V súčasnosti prebieha zo strany SNAS akreditácia Kompetenčného a certifikačného centra na poskytovanie služieb certifikácie audítorov kybernetickej bezpečnosti.

Distribúcia bezpečnostných bulletinov a varovaní

NCKB SK-CERT v rámci preventívnych aktivít vytváralo a distribuovalo bezpečnostné varovania a týždenné bezpečnostné bulletiny, ktoré obsahovali upozornenia na bezpečnostné incidenty, hrozby, zraniteľnosti a iné kyberneticky relevantné informácie.

Pri vytváraní obsahu jednotlivých výstupov je využívaná metrika Common Vulnerability Scoring System 3.1 (CVSS 3.1)⁷. Touto metrikou sa hodnotia zraniteľnosti softvérových a hardvérových produktov. Zraniteľnosti sa hodnotia prostredníctvom vopred stanovených parametrov a výsledkom tohto hodnotenia je CVSS skóre, číselná hodnota, ktorá reprezentuje závažnosť zraniteľnosti. Ak nie

⁷ Viac informácií o tejto metrike: <https://www.first.org/cvss/>

je možné informáciu ohodnotiť metrikou CVSS v 3.0, využívajú sa iné metriky hodnotenia informácií (napríklad metrika NCCIC Cyber Incident Scoring System – skratka NCISS), ktoré sú medzinárodne uznávané a používané pri vyhodnocovaní kyberneticky relevantných informácií.

Skóre	Závažnosť
0.1 – 3.9	Nízka (Low)
4.0 – 6.9	Stredná (Medium)
7.0 – 8.9	Vysoká (High)
9.0 – 10.0	Kritická (Critical)

Týždňový bezpečnostný bulletin obsahuje súbor varovaní a upozornení, ktoré môžu mať dopad na stav kybernetickej bezpečnosti. Bulletin je vydávaný raz týždenne a obsahuje súbor informácií so strednou a vysokou dôležitosťou za predchádzajúci týždeň. V týždňovom bezpečnostnom bulletine sa nachádzajú údaje o zraniteľnostiach a informácie s relevanciou od nízkej po vysokú.

Bezpečnostné varovanie obsahuje konkrétne varovanie s kritickou dôležitosťou, ktoré môže mať významný dopad na stav kybernetickej bezpečnosti na národnej aj medzinárodnej úrovni. Vydáva sa podľa potreby tak, aby bolo zabezpečené včasné varovanie partnerov NCKB SK-CERT, ako aj iných potencionálne zasiahnutých subjektov. V bezpečnostnom varovaní sa nachádzajú údaje o zraniteľnostiach a informácie s kritickou relevanciou.

Všetky výstupy sú zasielané ihneď po ich vytvorení prostredníctvom e-mailu. Ich adresáti sú dôležité orgány a inštitúcie štátnej správy, inštitúcie finančného a bankového sektora, zdravotníctva a kritickej infraštruktúry. Prihlásenie na odber bulletinov a varovaní je bez obmedzení. Jednotlivé výstupy systému varovania sú uverejňované aj na webovom sídle NCKB SK-CERT.

Nasledujúce tabuľky obsahujú prehľad počtu vydaných týždenných bezpečnostných bulletinov a bezpečnostných varovaní v roku 2019.

TÝŽDŇOVÉ BEZPEČNOSTNÉ BULLETINY						
	Celkový	počet	z toho relevancia			
			Nízka	Stredná	Vysoká	Kritická
Január 2019	5	0	14	46	0	60
Február 2019	4	0	3	47	0	50
Marec 2019	4	0	8	53	0	61
Apríl 2019	5	0	3	41	0	44
Máj 2019	4	0	6	33	0	39
Jún 2019	4	0	8	27	0	35
Júl 2019	5	0	10	31	0	41
August 2019	4	0	5	35	0	40
September 2019	4	0	1	30	0	31
Október 2019	5	0	0	45	0	45
November 2019	4	0	2	29	0	31
December 2019	4	0	0	25	0	25
Spolu	52	0	60	442	0	502

BEZPEČNOSTNÉ VAROVANIA					
	Celkový počet varovaní za mesiac	z toho relevancia			
		Nízka	Stredná	Vysoká	Kritická
Január 2019	28	0	0	1	27
Február 2019	23	0	0	0	23
Marec 2019	28	0	0	1	27
Apríl 2019	23	0	0	0	23
Máj 2019	24	0	0	0	24
Jún 2019	24	0	0	0	24
Júl 2019	13	0	0	1	12
August 2019	12	0	0	0	12
September 2019	17	0	0	0	17
Október 2019	24	0	0	1	23
November 2019	12	0	0	1	11
December 2019	16	0	0	0	16
Spolu	244	0	0	5	239

Cvičenia

Tréning a vzdelávanie v oblasti kybernetickej bezpečnosti patria medzi najdôležitejšie preventívne aktivity. Budovanie bezpečnostného povedomia je kontinuálny a nekončiaci proces, kde majú svoje miesto aj cvičenia v oblasti kybernetickej bezpečnosti, či už z technického alebo netechnického hľadiska.

Národné Table-top cvičenia

SK-CERT v roku 2019 začal organizovať Národné Table-top cvičenia. Table-top cvičenia sú druhom netechnických cvičení, ktoré sa zameriavajú na tréning manažérskeho rozhodovania, ako aj na precvičenie, otestovanie vlastných postupov a procesov, tréning úloh a zodpovedností jednotlivých rolí a to všetko v súvislosti s riešením vzorových kybernetických bezpečnostných incidentov. Scenár cvičenia prenesie účastníkov do fiktívneho prostredia s hypotetickými udalosťami, na ktoré musia reagovať tak, ako by sa naozaj stali.

V rámci série Národných Table-top cvičení rozoznávame niekoľko úrovní, v rámci ktorých sú cvičenia organizované:

Vládna úroveň

Vysokoúrovňové cvičenie za účasti politických a manažérskych špičiek ministerstiev a významných štátnych úradov. Scenár je zameraný na riešenie kybernetickej bezpečnostnej krízy celoštátneho rozsahu.

Úroveň prevádzkovateľov základných služieb

Cvičenia určené pre zástupcov manažmentu prevádzkovateľov základných služieb (cvičenia so zmiešanými sektormi). Scenár je všeobecný a nastavený tak, aby v realite mohol postihnúť akúkoľvek organizáciu na úrovni prevádzkovateľov základných služieb pre vybranú skupinu sektorov.

Úroveň sektorov

Cvičenie, kde je scenár cielený na konkrétne situácie v určitom sektore, určené pre zástupcov prevádzkovateľov základných služieb tohto sektora. Scenár sa snaží simulovať prostredie vybraného sektora čo najvernejšie, aby sa zvýšila miera akceptácie vedomostí účastníkov.

V priebehu roka boli zorganizované štyri Table-top cvičenia pre rôzne cieľové skupiny. Dve boli usporiadané pre cross-sektor prevádzkovateľov základných služieb, jedno pre prevádzkovateľov informačných systémov verejnej správy a jedno bolo organizované v rámci špecializovanej IT konferencie pre odbornú.

Účasť na cvičeniach

Slovenská republika sa počas roka 2019 zúčastnila viacerých kybernetických cvičení, či už prostredníctvom zástupcov SK-CERT alebo zástupcov iných rezortov.

Cvičenie EU ELEX 2019

5. apríla 2019 sa na pôde Európskeho parlamentu uskutočnilo cvičenie EU ELEX 2019, zamerané na operatívne riešenie kybernetických bezpečnostných incidentov počas volieb do Európskeho parlamentu. Cvičenie bolo organizované agentúrou ENISA v spolupráci s Európskym parlamentom a Európskou komisiou. Slovenskú republiku na cvičení reprezentovali zástupca SK-CERT, zástupca oddelenia Strategickej komunikácie Ministerstva zahraničných vecí európskych záležitostí Slovenskej republiky a zástupca odboru volieb, referenda a politických strán Ministerstva vnútra Slovenskej republiky.

Cvičenie CyberSOPEX 2019

15. mája 2019 sa SK-CERT zúčastnil na medzinárodnom cvičení CyberSOPEX. Cvičenie organizovala agentúra ENISA a jej cieľom bolo zlepšenie koordinácie a spolupráce členských štátov EÚ pri riešení kybernetických bezpečnostných incidentov veľkého rozsahu, ako jednej z hlavných požiadaviek smernice NIS. Národná jednotka SK-CERT systematicky spolupracovala so sektorovou CSIRT jednotkou zodpovednou za ochranu informačných systémov verejnej správy, na riešení kybernetických incidentov vo forme aktívnej výmeny informácií a zdieľania analytických kapacít, čo viedlo k úspešnému zvládnutiu cvičenia.

Cvičenie BlueOLEX 2019

2. a 3. júla 2019 sa v Paríži uskutočnilo vysokoúrovňové Table-Top cvičenie BlueOLEX 2019, založené na Odporúčaní komisie o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu. Celkovo sa na cvičení zúčastnilo 23 členských štátov, pričom jednotlivé štáty primárne zastupovali riaditelia kyberneticko-bezpečnostných autorít alebo riaditelia národných CSIRT tímov. Slovenskú republiku na cvičení reprezentoval riaditeľ SK-CERT.

Cvičenie Cyber Coalition 2019

Slovenská republika sa už tradične zúčastnila NATO cvičenia kybernetickej obrany Cyber Coalition. Ide o cvičenie spôsobilostí jednotlivých členských štátov v oblasti kybernetickej bezpečnosti a kybernetickej obrany s presahom na legislatívne a strategické oblasti. Cvičenia sa za Slovenskú republiku zúčastnili v jednom tíme SK-CERT, sektorový CSIRT pre ISVS CSIRT.sk, vojenský CSIRT.MIL.SK a zástupcovia Policajného zboru Slovenskej republiky.

Kybernetická bezpečnosť 5G sietí

Zavedenie sieťových technológií 5G považuje Európska komisia za hlavný faktor umožňujúci prevádzku budúcich digitálnych služieb. Preto 26. marca 2019 vydala Odporúčanie Komisie (EÚ) 2019/534 o kybernetickej bezpečnosti sietí 5G. Podľa tohto odporúčania mali jednotlivé členské štáty vypracovať národné posúdenie rizík v oblasti kybernetickej bezpečnosti 5G sietí, ktoré boli podkladom pre neskoršie spoločné európske posúdenie rizík 5G sietí.

Za Slovenskú republiku vypracoval Národné posúdenie rizík implementácie 5G technológií Národný bezpečnostný úrad, ktorý pri tejto aktivite spolupracoval s vybranými orgánmi verejnej moci, telekomunikačným regulátorom a telekomunikačnými operátormi.

V októbri 2019 vydala Európska komisia v spolupráci s členskými štátmi a agentúrou ENISA Spoločné posúdenie rizík 5G sietí, na základe ktorého bude vypracovaný tzv. Toolbox, ktorý bude obsahovať konkrétne opatrenia pre bezpečnú implementáciu 5G technológií v rámci členských štátov. Očakávané vydanie Toolboxu je naplánované na január 2020.

Zástupcovia Národného centra kybernetickej bezpečnosti SK-CERT aktívne participovali aj na všetkých aktivitách spojených s prípravou spoločného posúdenia rizík 5G sietí, ako aj v príprave a pripomienkovaní návrhov Toolboxu, zastupovali tiež Slovenskú republiku v pracovnej skupine pre kybernetickú bezpečnosť 5G sietí a na ďalších stretnutiach a aktivitách v tejto oblasti.

Návod na oznamovanie zraniteľností

SK-CERT v roku 2019 zverejnil Návod na oznamovanie zraniteľností, ktorý slúži ako pomôcka pre bezpečnostných výskumníkov, vývojárov softvéru, výrobcov hardvéru a zariadení, ale aj pre verejnosť. V návode sa uvádza podrobný postup a odporúčané kroky pri oznamovaní novoobjavených zraniteľností, ale aj postup pri oznamovaní už existujúcich zraniteľností nájdených na prevádzkovaných systémoch a službách. Návod je dostupný na webovom sídle NCKB SK-CERT.

Predikcia vývoja kybernetickej bezpečnosti na rok 2020

Pre rok 2020 môžeme predpokladať kontinuálny nárast počtu kybernetických incidentov s národným aj medzinárodným dopadom. Už v roku 2019 sme mohli zaznamenať nárast počtu a sofistikovanosti phishingových a spearphishingových útokov. Tieto útočné vektory budú naďalej používané nielen na zber informácií, ale aj ako prvý krok pre získanie prístupu do chránených systémov.

V škandinávskych krajinách je možné sledovať fenomén tzv. SMS phishingu, ktorý spočíva v obfuskácii (zakódovaní) odosielateľa a obsahu SMS. Táto SMS potom vyzerá ako dôveryhodný, ľuďom známy formát na finančné transakcie. V minulosti bolo možné sledovať, že otestované útočné vektory z konkrétnych krajín postupne prešli do iných krajín a preto môžeme predpokladať, že SMS phishing sa čoskoro stane novým fenoménom v Európe a teda aj v Slovenskej republike. Podobne to môže byť pri tzv. data leak phishingu (phishing zameraný na únik dát), ktorý je v súčasnosti populárny v USA. Útočníci po identifikovaní (alebo spôsobení) úniku dát oslovia e-mailom obeť úniku a presvedčia ich, aby sa za poplatok pridali k spoločnej žalobe alebo si kúpili službu na ochranu dát, ktorá nefunguje.

Ďalším potenciálne rastúcim phishingovým vektorom je telefonický phishing. Rast jeho popularity sa veľmi ťažko sleduje (je ťažko detegovateľný a obeť ho väčšinou nehlásia). Využívanie nástrojov tzv. deep fake na obfuskáciu hlasu sa však v blízkej dobe nepredpokladá, ide totiž o technicky a investične stále náročný postup vyžadujúci dôslednú predprípravu a prístup k týmto technológiám. Vzhľadom na rýchly progres deep fake technológií však nie je možné nasadenie tohto vektora v roku 2020 s istotou vylúčiť.

Úspešnosť včasnej detekcie stúpa, avšak trh so zraniteľnosťami tiež. V roku 2020 môžeme predpokladať pokračovanie celosvetového ransomvéru trendu a aj výrazný nárast útokov pochádzajúcich z vonkajšieho perimetra (útoky zamerané na hardvér, ktorý zamestnanci používajú v práci a aj na súkromné účely). Tento fakt umocňuje aj rastúca popularita práce z domu, čo znižuje korporáciám náklady ale pri často neriešenej bezpečnosti zvyšuje riziko.

Menej očakávaný spôsob, ktorý môže popri konštantnom zvyšovaní úspešnosti detekcie útoku spôsobiť nárast úspešných vniknutí do priemyselných systémov a kritickej infraštruktúry, je však získanie fyzického prístupu k vybraným prvkom IT systémov. Aj vzhľadom na zvyšujúcu sa komplexnosť IT aj OT systémov a tlaku na znižovanie nákladov sa čoraz častejšie využíva spôsob zabezpečovania prevádzkovej podpory vzdialeným prístupom dodávateľa do infraštruktúry zákazníka. Tieto spôsoby mimoriadne zvyšujú riziko neoprávnených prienikov do systémov zabezpečujúcich výrobu a služby poskytovateľov. Zároveň s rastúcou globalizáciou a zvyšujúcim sa objemom dodávok z krajín mimo EÚ, resp. z nízkonákladových ale bezpečnostne rizikových krajín, sa nekontrolovaný prístup do systémov stáva jedným z najväčších rizík. Aj z týchto dôvodov je v roku 2020 nutné, aby sa prevádzkovatelia základných služieb, ale aj organizácie všetkých veľkostí pripravili aj na túto možnosť, zavedením politiky nulovej dôvery v rámci prístupov do ich systémov. Nutné je zabezpečiť oddelenie infraštruktúry od internetu, zavedenie dvojfaktorovej autentifikácie, limitovanie prístupu ku kritickej infraštruktúre a uplatňovanie dôslednej politiky hesiel. Tieto opatrenia budú pri kritickej infraštruktúre najlepším spôsobom mitigácie potenciálu rastúcich supply chain útokov. Napríklad môže ísť o útoky, ktorých cieľom je získať prístup na server, z ktorého sú distribuované aktualizácie softvéru. Takto kompromitovaný server môže útočník zneužiť na distribúciu malvéru z navonok dôveryhodného zdroja.

V rámci činnosti APT skupín môžeme predpokladať zvýšenú aktivitu najmä čínskych, ruských, ale aj iránskych a severokórejských skupín. Rastúce napätie vyvrcholené atentátom na iránskeho generálmajora Quasema Soleimaniho, popri konvenčnej odvete (bombardovaní amerických základní a celkového nárastu aktivít Hizballáhu v regióne), môže spustiť aj výraznú internetovú aktivitu zo strany iránskych hackerov. Je možné domnievať sa, že predmetnou aktivitou bude skenovanie zraniteľností a príprava na kybernetický útok. Vzhľadom na geopolitický vývoj je možné vylúčiť, že by Slovenská republika bola primárnym cieľom útoku Iránskych APT skupín, avšak môže sa stať, že útoky (napr. ransomvér, supply chain útoky a hacking) zasiahnu Slovenskú republiku ako sekundárny cieľ.

Objem útokov ruských a čínskych APT skupín tiež v rámci celej Európy rastie a pravdepodobne bude rásť ďalej. Môžeme predpokladať nárast sofistikovaných útokov nielen v rámci Európskej únie, ale aj špecifických regionálnych celkov, napríklad krajín V4. Veľkou hrozbou je tiež plán na zavedenie 5G technológií a s tým súvisiace napätie medzi USA a Čínou. V roku 2020 môžeme predpokladať pokračovanie v špiónážnych aktivitách a situáciu je nutné dôsledne monitorovať.

Priame útoky APT skupín štátnych aktérov, najmä ruských, čínskych, ale aj severokórejských a iránskych sa budú zvyšovať. Medzi najdôležitejšie budú patriť ciele v štátnej správe a samospráve, kritická infraštruktúra, ale aj Ozbrojené sily Slovenskej republiky.

Útoky môžu byť vedené aj prostredníctvom dezinformácií. Dezinformačné kampane sú v Slovenskej republike už dnes bežnou formou aktivít a slúžia na ovplyvňovanie verejnej mienky alebo ako súčasť pokusov ovplyvniť výsledky parlamentných volieb, najmä prostredníctvom podsúvania dezinformácií.