Zpráva o stavu

kybernetické bezpečnosti České republiky za rok 2019

NÚKIB

Úvodní slovo ředitele NÚKIB

Je pro mne poctou i potěšením, že mohu za Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) představit v pořadí sedmou Zprávu o stavu kybernetické bezpečnosti České republiky. Naleznete v ní trendy v kybernetické bezpečnosti za hodnocený rok 2019, nejzávažnější kybernetické incidenty v tomto období i opatření, která byla realizována k zabezpečení českého kyberprostoru a našich občanů.

V roce 2019 došlo k dalšímu nárůstu počtu kybernetických útoků proti naší zemi, z nichž některé lze označit za velmi vážné. Řada veřejných i soukromých institucí se musela vyrovnávat s obranou před těmito útoky a odstraňováním jejich následků. NÚKIB v průběhu roku řešil 78 kybernetických incidentů. Jeho pracovníci pomáhali napadeným institucím státní správy, územní samosprávy, nemocnicím i firmám s obnovováním jejich systémů, a to jak formou doporučení a metodické pomoci, tak i fyzicky přímo na místech incidentů. Úřad byl této podpory schopen jen díky týmové práci, maximálnímu úsilí a pracovnímu nasazení všech jeho zaměstnanců.

Kybernetický prostor není vymezen geografickými hranicemi a tyto hranice neuznávají ani útočníci, kteří se v kyberprostoru pohybují. Pro naši kybernetickou bezpečnost je tak nezbytná i dobře fungující mezinárodní spolupráce. Česká republika je v mezinárodním prostředí v oblasti kybernetické bezpečnosti považována za důvěryhodného partnera a v mnoha směrech se dokonce stává inspirátorem a lídrem změn. Bezesporu nejdůležitější mezinárodní aktivitou České republiky na tomto poli v roce 2019 bylo uspořádání Pražské mezinárodní bezpečnostní konference o 5G sítích pod záštitou předsedy vlády České republiky a se širokou účastí vládních představitelů a expertů z více než 30 zemí a mezinárodních organizací. Prostřednictvím výstupů z konference Česká republika aktivně přispěla k dalšímu rozvoji kybernetické bezpečnosti v rámci EU i v globálním měřítku, na což můžeme být všichni právem hrdí.

S rostoucí mírou digitalizace naší společnosti se stále větší část našich aktivit odehrává na internetu. Narušování bezpečnosti kyberprostoru České republiky má proto dopad na životy nás všech. Riziko úspěšných kybernetických útoků bude v budoucnu nadále stoupat a je velmi pravděpodobné, že se s nimi každý z nás někdy setká. To se týká nejen správců či provozovatelů informačních a komunikačních systémů důležitých pro klíčové funkce státu a chod naší společnosti, ale i běžných občanů.

Kybernetická bezpečnost vyžaduje týmové úsilí, efektivní komunikaci a spolupráci veřejného i soukromého sektoru, všech orgánů státní správy i územní samosprávy, bezpečnostních složek, průmyslu, akademické obce, vzdělávacích institucí i širší veřejnosti – prostě nás všech. Česká republika je schopna kybernetickým hrozbám čelit jen díky široké spolupráci, podpoře a úsilí všech subjektů, které se NÚKIB snaží koordinovat ve prospěch bezpečného kyberprostoru pro všechny občany naší země.

Dovolte mi, abych Vám všem, kteří nás v našem společném úsilí podporujete, jménem zaměstnanců Národního úřadu pro kybernetickou a informační bezpečnost poděkoval. Velké díky patří také našim zahraničním partnerům, kteří jsou pro náš úspěch nepostradatelní.

Rád bych také poděkoval všem 125 institucím z oblasti státní správy, územní samosprávy, nemocnic, firem a dalších, které se podílely na tvorbě této výroční zprávy. Věřím, že i tato zpráva, která by bez jejich dat nikdy nemohla vzniknout, přispěje k bezpečnosti v kyberprostoru pro nás všechny.

Ing. Karel Řehka

ředitel NÚKIB

Shrnutí Zprávy o stavu kybernetické bezpečnosti České republiky za rok 2019

01 Rok 2019 se vyznačoval nárůstem počtu kybernetických útoků proti institucím, organizacím a firmám v České republice. V roce 2019 bylo NÚKIB nahlášeno 217 incidentů proti 164 incidentům v roce 2018. Rostla rovněž závažnost incidentů, jak ukazují útoky proti Nemocnici Rudolfa a Stefanie Benešov nebo těžební společnosti OKD. Nejčastějšími typy útoků byly v roce 2019 **spam, phishing a podvodné e-maily,** které mnohdy stojí na začátku sofistikovanějších a škodlivějších akcí útočníků.

02 V roce 2019 zaznamenal NÚKIB spolu s partnery **kybernetickou špionáž** proti strategické instituci státní správy, téměř jistě ze strany státního aktéra. Na základě zjištění NÚKIB za útokem velmi pravděpodobně stála skupina Sofacy, kterou odborná komunita, včetně partnerů NÚKIB, spojuje s vojenskou rozvědkou Ruské federace GU (též GRU).

03 Ve srovnání s rokem 2018 ubylo těžby kryptoměn prostřednictvím malwaru. Zároveň se změnil charakter kampaní **vyděračského malwaru (ransomware)**, kdy sice klesl počet primitivnějších plošných útoků, ale naopak přibylo útoků cílených a sofistikovaných. To se projevilo na konci roku, kdy ransomware Ryuk napadl systémy nemocnice v Benešově a těžební společnosti OKD.[i]

04 Zdravotnictví se ze sledovaných sektorů potýkalo s největším **nedostatkem odborníků na kybernetickou bezpečnost** a zároveň se stále častěji stává cílem kyberzločinců. V prosinci 2019 se obětí ransomwarového útoku stala nemocnice v Benešově. Následkem útoku bylo významné omezení provozu na téměř měsíc a způsobení škod pohybujících se v rozmezí 40 až 50 milionů korun.

05 V roce 2019 se v oblasti kybernetické bezpečnosti řada dotazovaných organizací potýkala s **nedostatkem financí ve vlastních rozpočtech a nedostatkem odborníků.** Téměř žádný z respondentů neměl obsazené všechny pozice v oblasti kybernetické bezpečnosti. Pro více než polovinu byly největším faktorem, který odrazoval případné uchazeče, mzdové podmínky.

06 NÚKIB společně s Ministerstvem zahraničních věcí v roce 2019 zorganizoval první ročník mezinárodní expertní konference **Prague 5G Security Conference** k bezpečnosti sítí páté generace (5G), konané pod záštitou a za účasti předsedy vlády Andreje Babiše. Konference se zúčastnilo přes 150 vládních představitelů a expertů na problematiku 5G sítí a kybernetickou bezpečnost z více než 32 států, včetně představitelů Evropské unie (dále „EU“) a NATO. Hlavním výstupem expertní konference bylo zveřejnění tzv. **Pražských návrhů**, série doporučení týkajících se bezpečnosti 5G sítí, které se promítly do výsledné podoby 5G Toolboxu Evropské unie a kterými se při tvorbě regulačních dokumentů inspirovaly i další státy.

07 V roce 2019 NÚKIB pokračoval ve vzdělávání zaměstnanců státní správy a v rámci e-learningového kurzu Dávej kyber! **proškolil více než pět tisíc úředníků**. Úřad dále pokračoval v osvětových a vzdělávacích projektech zaměřených na děti, mládež a seniory. Osvětové aktivity provozovala také celá řada dalších organizací, včetně univerzit nebo poskytovatelů telekomunikačních služeb.

08 V roce 2019 NÚKIB zaznamenal výrazné zvýšení poptávky po cvičeních v oblasti kybernetické bezpečnosti, přičemž jich 17 uskutečnil. Úřad připravil a provedl například společné **cvičení s Národní centrálou proti organizovanému zločinu** nebo sektorové cvičení **Electro Czech** pro zástupce energetického průmyslu.

Obsah

2019: Kybernetická bezpečnost ČR v datech

217 nahlášených kybernetických incidentů GovCERT.CZ

78 z nahlášených kybernetických incidentů řešeno GovCERT.CZ

8417 přednášek pro žáky středních škol

954 aktivit pro žáky mateřských či základních škol

483 nahlášených phishingových útoků CSIRT.CZ

17 cvičení kybernetické bezpečnosti provedených NÚKIB

90 zemí, které se cvičení účastnily

468 účastníků cvičení kybernetické bezpečnosti uspořádaných NÚKIB

5172 proškolených úředníků státní správy

109 informačních a komunikačních systémů kritické informační infrastruktury

47 subjektů kritické informační infrastruktury

38 provozovatelů základní služby

70 správců a provozovatelů významných informačních systémů

178 významných informačních systémů

42 informačních systémů základní služby

Kapitola A

Kybernetická bezpečnost v roce 2019 pohledem českých institucí, organizací a firem[1]

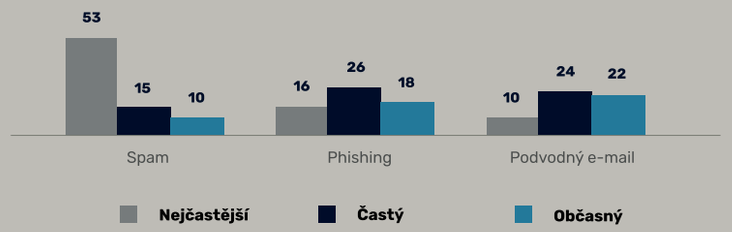
A | 01

Incidenty:

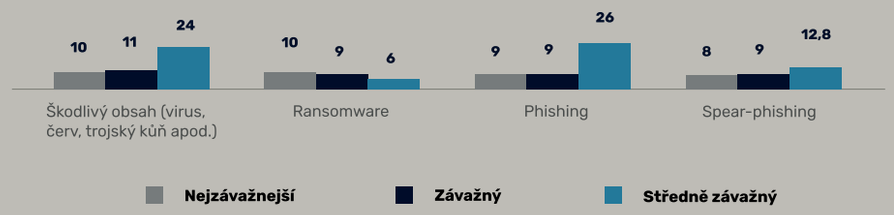
Malware a phishing jako nejzávažnější hrozby

V roce 2019 byly nejčastějšími typy útoků, se kterým se dotazované organizace setkaly, spam, phishing a podvodné e-maily (graf 1), tedy technicky nejméně náročné útoky. Za nejzávažnější typy útoků většina respondentů považovala škodlivý kód (virus, červ, trojan), ransomware a phishing (graf 2). Ne všechny pokusy o kybernetický útok pro útočníky skončily úspěchem. Pouze u třetiny respondentů došlo následkem útoku k narušení důvěrnosti, integrity nebo dostupnosti informací nebo služeb, přičemž u většiny z nich se počet incidentů pohyboval mezi jedním a pěti (graf 3). Největší výskyt byl zaznamenán u územních samosprávných celků a finančních institucí. Zhruba třetina incidentů měla za následek omezení dostupnosti služby. Téměř třetina respondentů se rovněž setkala s útoky DDoS (Distributed Denial of Service), nicméně ani respondentia ani Úřad nezaznamenali žádný rozsáhlejší útok tohoto typu. Stejně tak respondenti ani NÚKIB nezaznamenali rozsáhlejší útoky prostřednictvím techniky SQL Injection.[2]

Graf 1: **Nejčastější** typy útoků za rok 2019 (%)



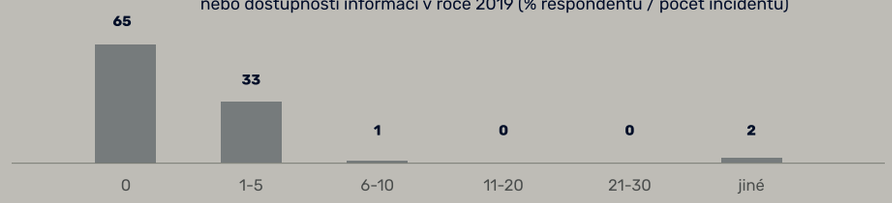
Graf 2: **Nejzávažnější** typy kybernetických útoků za rok 2019 (%)



[1] NÚKIB na začátku roku 2020 rozeslal dotazník se 49 otázkami, a to jak subjektům regulovaným zákonem č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (také zákon o kybernetické bezpečnosti, dále „ZKB"), tak i řadě dalších klíčových institucí a organizací, které ZKB regulovány nejsou. Otázky se týkaly širokého záběru témat, například kybernetických útoků, nákladů na kybernetickou bezpečnost, personálních kapacit v oblasti kybernetické bezpečnosti, uživatelů, technologií i zavedených procesů. Dotazníky vyplnilo 125 státních institucí, organizací a státních i soukromých firem. Z těchto dat NÚKIB čerpal data pro potřeby Zprávy o stavu kybernetické bezpečnosti České republiky za rok 2019 (dále „ZSKB 2019"). Veškeré údaje z dotazníků jsou anonymizované a uváděné v procentech. Na následujících řádcích budou shrnuty některé trendy.

[2] SQL Injection je technika, která zneužívá bezpečnostní chyby vyskytující se v databázové vrstvě aplikace. Tato chyba zabezpečení se projevuje infiltrací neoprávněných znaků do SQL příkazu oprávněného uživatele nebo převzetím uživatelova přístupu k vykonání SQL příkazu. Útočníci pak mohou nad kompromitovanou databází převzít kontrolu a téměř libovolně s ní nakládat (kopírovat, měnit nebo mazat data).

Graf 3: Počet incidentů, kdy došlo u respondentů k narušení důvěrnosti, integrity nebo dostupnosti informací v roce 2019 (% respondentů / počet incidentů)



A | 02

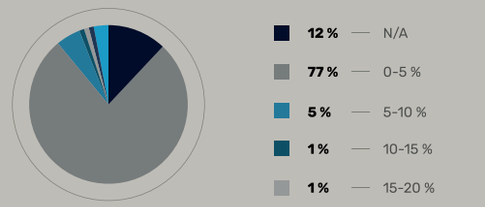
Finance:

Minimální pokles rozpočtů na kybernetickou bezpečnost

Jak ukázaly odpovědi dotazovaných organizací, jedním z nejslabších míst české kybernetické bezpečnosti byly v roce 2019 nedostatečné finanční prostředky. Organizace většiny respondentů alokují na kybernetickou bezpečnost 0–5 % svého celkového rozpočtu (graf 4), což 44 % hodnotí jako nedostatečné (graf 5). Pozitivní zprávou je, že v roce 2019 rozpočty na kybernetickou bezpečnost většinou neklesaly. U 44 % respondentů se zvýšily a u 45 % zůstaly stejné jako v roce 2018 (graf 6).

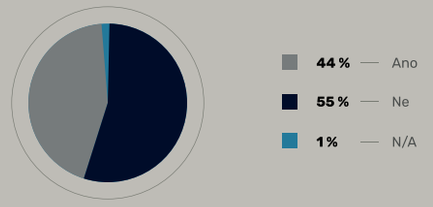
Graf 4:

Podíl rozpočtu alokovaného na kybernetickou bezpečnost na celkovém rozpočtu organizací respondentů v roce 2019 (%)

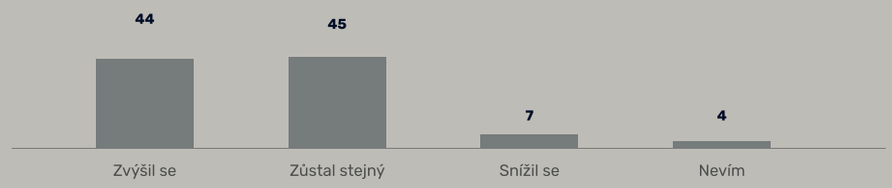


Graf 5:

Byly finance alokované na kybernetickou bezpečnost v organizacích respondentů v roce 2019 dostatečné? (%)



Graf 6: Vývoj rozpočtů respondentů na kybernetickou bezpečnost v roce 2019 (%)



A | 03

Lidé – odborníci:

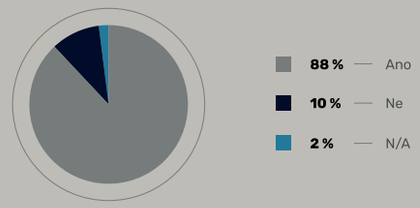
Nedostatek pracovníků v oblasti kybernetické bezpečnosti

Jedním z důsledků nedostatku financí byla v roce 2019 nouze o odborníky na kybernetickou bezpečnost. Na konci roku 2019 potřebovalo 88 % dotazovaných organizací obsadit místa v oblasti kybernetické bezpečnosti (graf 7). Podle 67 % respondentů byly zásadním důvodem, který odrazuje uchazeče, nevýhodné mzdové podmínky (graf 8). Situaci organizace řeší různě. Některé sází například na benefity, kterými by uchazeče přilákaly. Jiné kybernetickou bezpečnost částečně řeší outsourcingem, na který spoléhá polovina respondentů (graf 9).

Nízké rozpočty jsou jen jednou z příčin nezaplněných pozic. Nedostatek odborníků na kybernetickou bezpečnost je celosvětovým problémem a důsledkem vyšší poptávky jsou i vyšší mzdové náklady než u jiných IT profesí. To vede k tomu, že dostatek odborníků dokáže zaplatit pouze část zaměstnavatelů, většinou ze soukromého sektoru. Nedostatkem pak trpí zejména instituce státní správy, územní samosprávy a zdravotnické organizace.

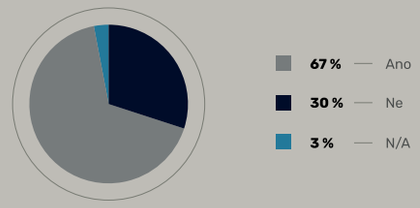
Graf 7:

Potřebovali respondenti v roce 2019
obsadit místa v oblasti kybernetické bezpečnosti?



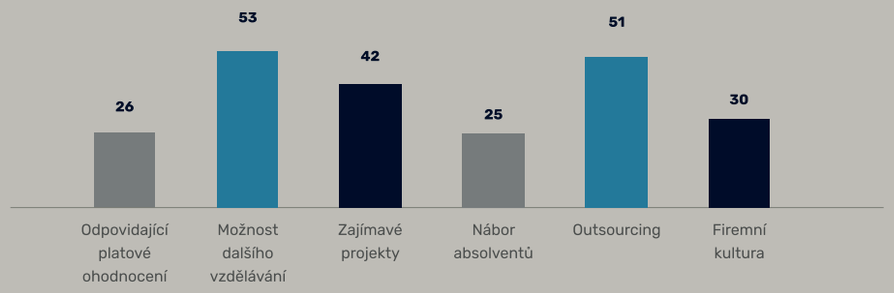
Graf 8:

Byly peníze v roce 2019 zásadním faktorem, který odrazoval uchazeče při náborech na místa v oblasti kybernetické bezpečnosti? (%)



Graf 9:

Jak se organizace snaží vypořádávat s nedostatkem odborníků v oblasti kybernetické bezpečnosti (%)



A | 04

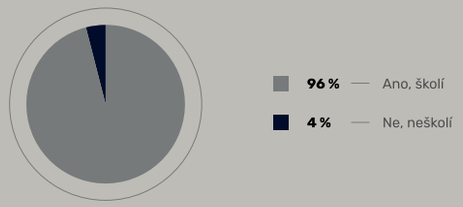
Lidé – uživatelé:

Školení jako nová norma

Za nejzranitelnější článek kybernetické bezpečnosti bývají považováni uživatelé, kteří mohou pouhým kliknutím a otevřením infikované přílohy způsobit vyřazení desítek až stovek počítačů v síti. Školení uživatelů ohledně existujících kybernetických hrozeb braly v roce 2019 organizace respondentů vážně a naprostá většina z nich své uživatele nějakým způsobem školila (graf 10). U většiny měla školení podobu e-learningu nebo byla prováděna vlastními zaměstnanci, přičemž třetina organizací v roce 2019 sáhla po službách třetích stran. Dvě třetiny dotazovaných organizací školí s frekvencí alespoň jednou za rok (graf 11). Více než polovina respondentů zvyšovala odolnost zaměstnanců proti kybernetickým hrozbám i formou aktivního testování, například simulovanými phishingovými kampaněmi (graf 12). Skutečnost, že uživatele školí téměř všechny organizace respondentů, je velmi pozitivní, nicméně forma školení je v tomto ohledu zásadní. Za nejefektivnější metody školení lze považovat kombinaci **častějších**, **interaktivních** a **kratších** školení.

Graf 10:

Stav školení uživatelů v oblasti kybernetické
bezpečnosti v organizacích respondentů v roce 2019 (%)



Graf 11:

Frekvence školení uživatelů v oblasti kybernetické bezpečnosti
v organizacích respondentů v roce 2019 (%)

Graf 12:

Forma testování odolnosti zaměstnanců proti kybernetickým
hrozbám v organizacích respondentů v roce 2019 (%)

Kapitola B

Aktéři hrozeb v kybernetickém prostoru

Podle informací dostupných NÚKIB Českou republiku v kybernetickém prostoru v roce 2019 nejvíce ohrožovali kyberzločinci. Další významnou kategorií byly útoky cizích mocností, které cílily na české státní instituce.

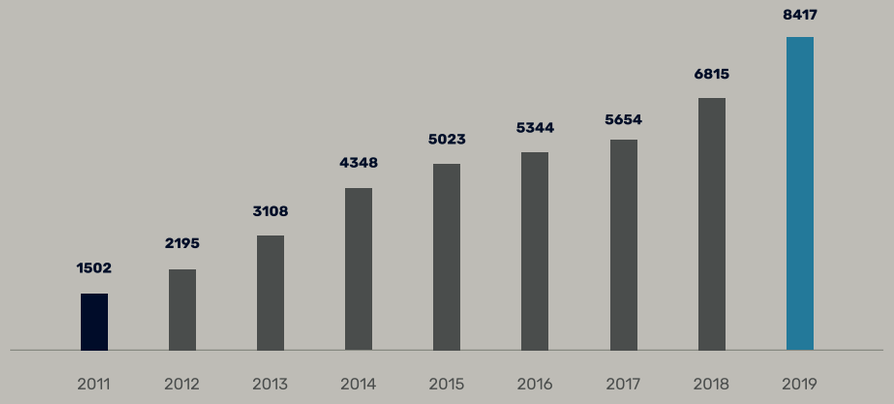
Aktivita kyberzločinců byla patrná například při kybernetických útocích na Nemocnici Rudolfa a Stefanie Benešov nebo proti společnosti OKD.

Jak ukazují statistiky Policie ČR (graf 13), je kybernetická kriminalita a kriminalita páchaná na internetu v České republice na vzestupu a jejich případů každoročně přibývá.[ii] Mezi rokem 2018 a 2019 došlo k 24% nárůstu vyšetřovaných případů. Trend nárůstu kyberkriminality je patrný dlouhodobě a velmi pravděpodobně (pravděpodobnost 75–85 %) poroste i v roce 2020 a 2021. Důvodem tohoto trendu je především relativně snadný zisk a nízké riziko odhalení při páchání této trestné činnosti.

Mezi další aktéry, kteří působí v kyberprostoru, patří kyberteroristé, politicky motivovaní hacktivisté[3] či málo sofistikovaní aktéři (tzv. skript kiddies[4]). Žádný z těchto aktérů v roce 2019 nepředstavoval pro českou kybernetickou bezpečnost významnější hrozbu.

Graf 13:

Vyšetřované kyberkriminální případy v ČR mezi roky 2011 a 2019



Zdroj: **Policie ČR**

[3] Politicti aktivisté, kteří s cílem politické, ideologické nebo sociální změny narušují dostupnost, důvěrnost nebo integritu informací.
[4] Slangové označení pro amatéry, kteří pro své útoky používají nástroje vyvinuté jinými útočníky.

Kapitola C

Kybernetické hrozby

C | 01

Kybernetická špionáž:

Medvědi v českých sítích

Stejně jako téměř každý rok byla kybernetická špionáž aktuálním tématem v České republice i v roce 2019. NÚKIB spolupracoval na řešení incidentu, při kterém byla narušena důvěrnost dat v sítích **strategické instituce státní správy**. Prvotním vektorem útoku byl spear-phishingový e-mail. Následná analýza indikátorů kompromitace ze strany NÚKIB ukázala, že útočníkem byl téměř jistě státní aktér (pravděpodobnost 90–100 %) a velmi pravděpodobně (pravděpodobnost 75–85 %) APT [5] **skupina známá jako Sofacy**, APT28 či Cozy Bear (přítulný medvěd). Odborná komunita, včetně partnerů NÚKIB, **spojuje Sofacy s vojenskou rozvědkou Ruské federace GU** (známá též jako GRU). [iii]

V roce 2019 byly jedněmi z nejaktivnějších aktérů v kyberprostoru skupiny spojované s backdoorem **Winnti**. Stopy Winnti byly k nalezení v případech průmyslové špionáže, kyberšpionážních útocích na státní instituce či nevládní neziskové organizace a média. Backdoor Winnti je odborníky od počátku své existence spojován s Čínskou lidovou republikou (dále „ČLR“) [iv] . V roce 2019 došlo k rozsáhlému útoku jedné z Winnti skupin na významné německé společnosti, včetně Bayer, Siemens, BASF a Henkel. [v] I když NÚKIB v roce 2019 v České republice neatribuoval žádný útok skupinám Winnti, vzhledem k charakteru jejich cílů v zahraničí, do budoucna tuto hrozbu **nelze vyloučit (pravděpodobnost 25–50 %) ani v České republice.** Winnti patří mezi aktéry, kteří využívají slabin v dodavatelském řetězci a jsou odbornou komunitou spojováni s útokem na službu CCleaner [vi] , kterou v roce 2017, během probíhajícího útoku, koupila česká bezpečnostní společnost Avast (více na straně 20).

C | 02

Ransomware:

Ústup primitivnějších plošných kampaní na úkor sofistikovaných útoků

Zatímco v roce 2018 NÚKIB v České republice pozoroval ústup ransomwaru a vzestup malwaru využívající výpočetní výkon infikovaného počítače k těžbě kryptoměn (tzv. kryptominer), v roce 2019 byla situace opačná. V lednu 2019 bylo podle bezpečnostních odborníků kryptominery nakaženo 30 % organizací, nicméně v říjnu 2019 šlo již pouze o 11 % organizací [vii] Důvodem ústupu kryptominerů je velmi pravděpodobně (pravděpodobnost 75–85 %) kombinace klesající lukrativnosti těžby kryptoměn a zvýšené pozornosti ze strany antivirových společností.

V roce 2019 ubylo plošných ransomwarových útoků typu WannaCry a naopak **narostl počet sofistikovaných cílených vyděračských kampaní**. Tento trend se týkal i České republiky.

Ransomware

je druhem škodlivého softwaru, který bere zasažený systém a data jako rukojmí („ransom“ – anglicky výkupné). Útočníci infikují systém oběti ransomwarem, který zašifruje veškerá data, a za jejich obnovení požadují finanční obnos.

I přes možné závažné dopady útoků NÚKIB napadeným subjektům nedoporučuje platit útočníkům za dešifrování dat, jelikož neexistuje záruka, že tak skutečně učiní.

32 % respondentů uvedlo, že v roce 2019 zaznamenali útok nebo pokus o útok typu ransomware

[5] Advanced Persistent Threat neboli pokročilá trvalá hrozba – označení pro obzvláště sofistikované skupiny útočníků.

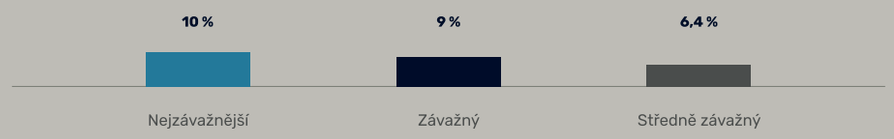
V České republice se v roce 2019 vyděračský malware nejvíce projevil v prosinci v podobě kampaně ransomwaru Ryuk. Ten napadl sítě Nemocnice Rudolfa a Stefanie Benešov a těžební společnosti OKD (více v kapitole Cíle kybernetických útoků).

Podle dat z dotazovaných organizací se s útokem ransomwaru nebo s pokusem o něj setkalo 32 % respondentů, přičemž čtvrtina (graf 14) hodnotí ransomware jako nejzávažnější, závažný nebo středně závažný typ útoku. Tato čísla jsou výrazně vyšší, než uvádí zprávy zaměřené na soukromé společnosti. [viii] Vzhledem ke složení dotazovaných organizací v šetření NÚKIB [subjekty dle zákona o kybernetické bezpečnosti (dále „ZKB“)] z toho lze vyvodit, že cílenost ransomwaru se pravděpodobně (pravděpodobnost 55–70 %) projevuje i v České republice. Subjekty ZKB lze zařadit mezi cíle, jejichž kompromitace by mohla mít vliv na hladké fungování státu a jeho suverenitu (státní instituce, telekomunikační a energetické společnosti, nemocnice) a předpokládáme proto, že útočníci mohou věřit ve vyšší šanci na zaplacení výkupného.

Vedle cílenějších útoků se v oblasti ransomwaru v roce 2019 objevil trend hrozby zveřejnění citlivých dat v případě nezaplacení výkupného. Tato hrozba vytváří další tlak na oběť, aby zaplatila výkupné a neriskovala, že se důvěrné informace o zaměstnancích nebo obchodní tajemství objeví volně na internetu. NÚKIB nemá informace o tom, že by se v roce 2019 obětí podobného útoku stala česká organizace či firma, ale existuje reálná možnost (pravděpodobnost 25–50 %), že tento trend v budoucnu zasáhne i Českou republiku.

Graf 14:

Závažnost ransomwarových útoků dle respondentů (%)



C | 03

Phishing, spear-phishing a podvodné e-maily:
Vyšší počet i lepší čeština

V roce 2019 se s phishingovými e-maily setkalo 90 % respondentů, se spear-phishingovými e-maily 44 % a s podvodnými e-maily 94 %. Zatímco phishingové a podvodné e-maily zasahovaly všechny sektory srovnatelným dílem (graf 15 a 16), spear-phishingové e-maily cílily především na finanční instituce, zdravotnictví a další subjekty kritické informační infrastruktury (graf 17). Útočníci se tedy zaměřují především na lukrativní cíle nebo na subjekty, které jsou zásadní pro fungování státu a které pro hackery mohou znamenat potenciálně vyšší zisk.

V České republice byl v roce 2019 patrný nárůst phishingových, spear-phishingových i podvodných e-mailů z hlediska počtu i sofistikovanosti. Tento trend zaznamenalo 36 % respondentů. Kvalitativní posun byl patrný zejména z používání dokonalejší češtiny, propracovanějších formátů e-mailů a různorodosti jejich motivů (exekutorská výzva, zápis z jednání apod.). Útočníci v e-mailech také často oslovovali oběti prostřednictvím jména skutečného člověka, ať už šlo o kolegu nebo nadřízeného.

Phishing, spear-phishing a podvodné e-maily

Phishing má podobu e-mailu, SMS nebo zprávy na sociální síti, ve které se útočník snaží přesvědčit oběť, aby mu prozradila citlivou informaci, otevřela odkaz vedoucí na škodlivou stránku nebo otevřela soubor obsahující škodlivý kód. **Spear-phishing** je personalizovanou formou phishingu, která cílí na konkrétní instituce a osoby. V **podvodných e-mailech** se útočníci zpravidla snaží svou oběť přesvědčit, aby jim zaslala peníze. Phishingové, spear-phishingové i podvodné zprávy se ve zvýšené míře objevují i na sociálních sítích.

44 % dotazovaných organizací uvedlo, že na ně byl v roce 2019 veden **spear-phishingový útok** nebo pokus o něj

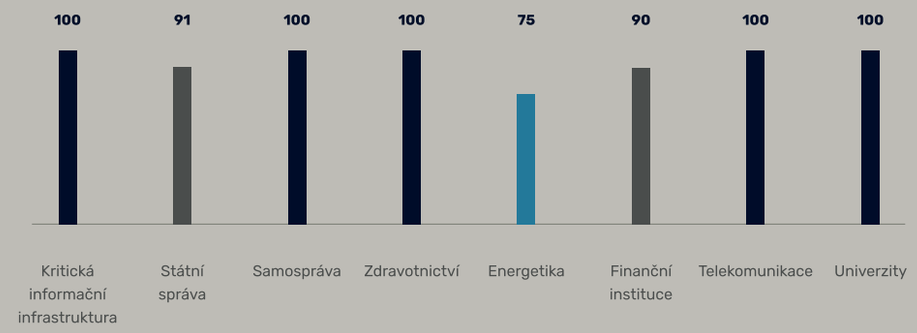
94 % dotazovaných organizací uvedlo, že na ně byl v roce 2019 veden útok formou **podvodného e-mailu** nebo pokus o něj

36 % dotazovaných organizací uvedlo, že v roce 2019 zaznamenaly nárůst kvality i kvantity **phishingových, spear-phishingových a podvodných e-mailů**

90 % dotazovaných organizací uvedlo, že na ně byl v roce 2019 veden **phishingový útok** nebo pokus o něj

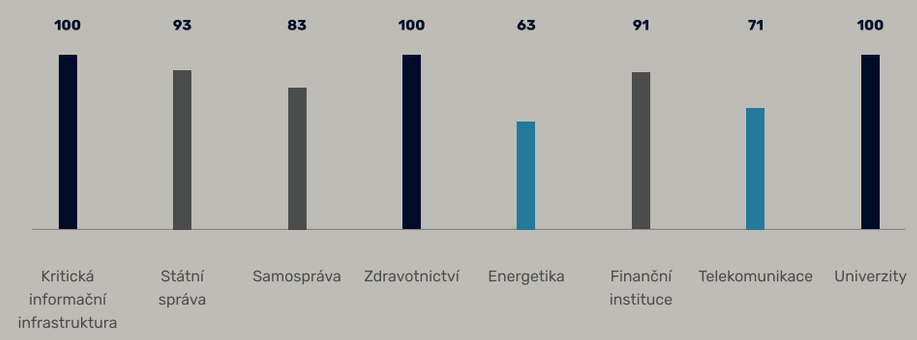
Graf 15:

Procento respondentů (dle sektoru), kteří v roce 2019 čelili podvodným e-mailům (%)



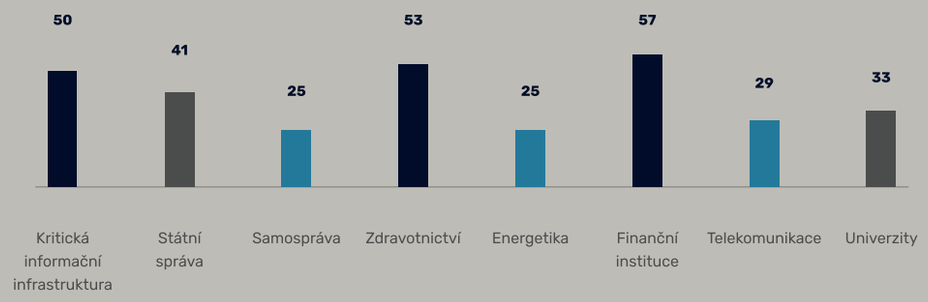
Graf 16:

Procento respondentů (dle sektoru), kteří v roce 2019 čelili phishingovým útokům (%)



Graf 17:

Procento respondentů (dle sektoru), kteří v roce 2019 čelili spear-phishingovým útokům (%)



Více o spear-phishingu (i phishingu) a jak se mu bránit naleznete na stránkách NÚKIB:

https://www.govcert.cz/cs/informacni-servis/doporuceni/2748-spear-phishing-a-jak-se-pred-nim-chranit/

Doporučení NÚKIB pro ochranu před spear-phishingem na stránkách NÚKIB:

https://www.govcert.cz/download/doporuceni/NUKIB_doporuceni-spear-phishing.pdf

Rozeznat phishing a spear-phishing není vzhledem k jejich rostoucí propracovanosti snadné, což demonstruje i tento test od společnosti Google:

https://phishingquiz.withgoogle.com/

C | 04

Útoky zneužívající slabá místa v dodavatelském řetězci:

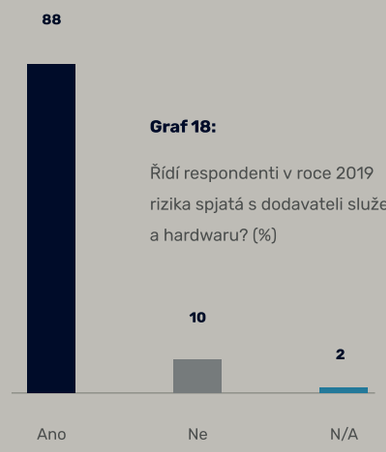
Výjimečné, ale s potenciálně rozsáhlými následky

Ačkoli v roce 2019 zaznamenala **útok na dodavatelský řetězec**, nebo pokus o něj, jen 2 % dotazovaných organizací, jsou si české instituce, organizace a firmy vědomy rizika, které tento způsob útoku přináší, a rizika spjatá s dodavateli proto řídí 88 % respondentů (graf 18).

Relativně sporadický výskyt tohoto typu útoku v České republice je pravděpodobně (pravděpodobnost 55–70 %) důvodem, proč 38 %, a tedy nejvíce, respondentů hodnotí hrozbu kybernetických útoků skrze dodavatele služeb jako nízkou. Pouze 18 % riziko hodnotí jako vysoké a 33 % jako střední (graf 19).

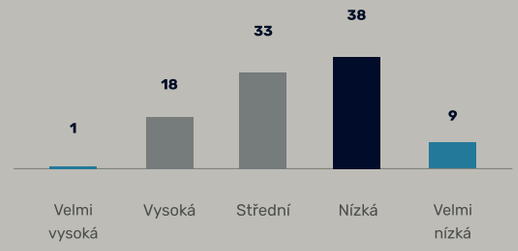
Graf 18:

Řídí respondenti v roce 2019 rizika spjatá s dodavateli služeb a hardwaru? (%)



Graf 19:

Hodnocení velikosti hrozby kybernetických útoků skrze dodavatele služeb a hardwaru respondenty v roce 2019 (%)



Kyberbezpečnostní problémy s dodavatelským řetězcem se v roce 2019 dotkly i České republiky. Česká antivirová společnost Avast se stala obětí kybernetického útoku ve druhé polovině roku 2019. Útočníci získali přístup do sítí společnosti, kde byli odhaleni. Cílem útočníků bylo pravděpodobně (pravděpodobnost 55–70 %) infikovat škodlivým softwarem široce rozšířený produkt firmy Avast na čistění počítače – CCleaner. Podle Bezpečnostní informační služby útok z roku 2019 přicházel z Číny. [ix] Jednalo se už o druhý pokus kompromitace populárního softwaru, přičemž první útok odhalený v září 2017 byl úspěšný. Z útoku byla na základě výzkumu izraelské kyberbezpečnostní společnosti podezřelá skupina Winnti. [x]

Jedním ze způsobů, jak taková rizika řídit, je nezohledňovat u veřejných zakázek pouze kvantitativní hlediska, jako je cena, ale i kvalitativní kritéria zaměřená na kybernetickou bezpečnost. Činí tak 77 % respondentů (graf 20). Podle poznatků NÚKIB zůstává v **České republice** potenciálně rizikovým faktorem, který souvisí s dodavatelským řetězcem, současný způsob aplikace zákona o zadávání veřejných zakázek (zákon č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů), kdy převládají zadávací řízení s cenou jako hlavním či jediným kritériem. [xi] Vysoký počet respondentů uvedl, že při zadávání veřejných zakázek využívá i kvalitativní kritéria (graf 20). Úřad také v roce 2019 zaznamenal zvýšený zájem povinných subjektů o konzultace k zadávání konkrétních veřejných zakázek.

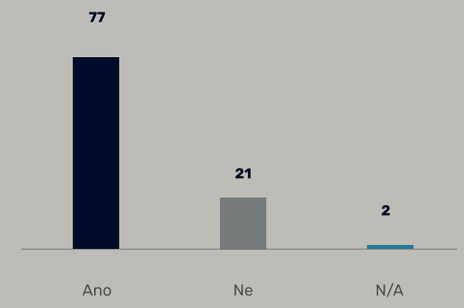
V roce 2019 bylo v souvislosti s varováním Úřadu proti technologiím Huawei a ZTE důležitou událostí rozhodnutí Úřadu pro ochranu hospodářské soutěže (ÚOHS) o zastavení řízení, které se týkalo stížnosti firmy Huawei na podmínky výběrového řízení na servery pro Ministerstvo životního prostředí ČR. Společnosti Huawei v podmínkách tendru vadila podmínka zohledňující varování NÚKIB, která byla dle firmy diskriminační. ÚOHS dospěl k závěru, že podmínku namítanou společností Huawei nepovažuje za diskriminační, neboť její zařazení představuje jediný způsob, jak mohl zadavatel dostát svým zákonným povinnostem v oblasti kybernetické bezpečnosti. [xii]

2 %

dotazovaných organizací v roce 2019 zaznamenala útok nebo pokus o útok skrze dodavatelský řetězec

Graf 20:

Využívají respondenti při zadávání veřejných zakázek i kvalitativní kritéria? (%)



Kapitola D

Cíle kybernetických útoků

D | 01

Státní správa a územní samospráva:

Cíl sofistikovaných phishingových útoků

Častým cílem kybernetických útoků byly i v roce 2019 instituce státní správy a územní samosprávy. Zejména instituce ústřední státní správy jsou pro útočníky spjatými se státními aktéry zdrojem zpravodajsky, vojensky, politicky i ekonomicky významných informací. V roce 2019 se zaměstnanci státní správy a samosprávy nejčastěji setkávali se spamem, phishingem a podvodnými e-maily (graf 21), přičemž za ty nejzávažnější jsou považovány škodlivý kód, phishing a spear-phishing (graf 22). Tyto hrozby byly v roce 2019 s drobnými odchylkami stejné ve všech sledovaných sektorech.

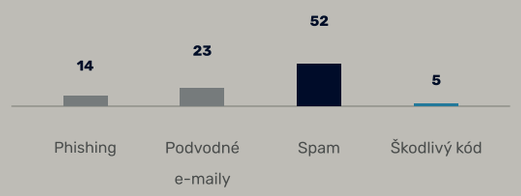
Více než polovina respondentů označila za největší trend v útocích na jejich organizaci **zdokonalení phishingových, spear-phishingových a podvodných e-mailů.** Útočníci projevili lepší znalost prostředí i češtiny, což ztížilo jejich detekci.

V institucích státní správy a územní samosprávy je dlouhodobě **problém získat a zaplatit odborníky na kybernetickou bezpečnost**. Na základě zjištění NÚKIB chybělo ministerstvům a Úřadu vlády v roce 2019 153 pracovníků se zaměřením na kybernetickou bezpečnost. Téměř všichni respondenti uvedli, že důvodem neobsazeností míst v oblasti kybernetické bezpečnosti v jejich organizaci jsou mzdové podmínky. Tuto situaci v roce 2019 řešily dvě třetiny institucí outsourcingem.

Zatímco nejzávažnější útoky na instituce státní správy zůstávaly v roce 2019 doménou státních aktérů, územní samospráva se v roce 2019 v České republice i ve světě stala obětí kyberzločinců. Úřadu byl nahlášen ransomwarový útok proti jednomu z krajů, přičemž měl za následek jednotky nakažených počítačů.

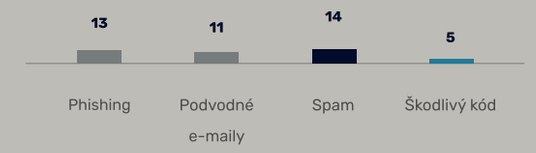
Graf 21:

Nejčastější útoky nebo pokusy útoků vedené proti respondentům ze státní správy a územní samosprávy v roce 2019 (%)



Graf 22:

Nejzávažnější útoky nebo pokusy útoků vedené proti respondentům ze státní správy a územní samosprávy v roce 2019 (%)



D | 02

Kritická infrastruktura:

Omezení dostupnosti služeb jako největší hrozba

Podle informací dostupných NÚKIB v **České republice** neproběhl v roce 2019 žádný sofistikovaný a soustředěný kybernetický útok, který by cílil na informační systémy kritické infrastruktury (KI) a měl závažné dopady na fungování státu. Přesto subjekty kritické informační infrastruktury (KII) čelily stovkám až tisícům pokusům o kybernetické útoky. Z odhalených kybernetických bezpečnostních incidentů vedla až polovina z nich k **omezení dostupnosti** služeb, což je u subjektů kritické infrastruktury nejzásadnější hledisko k zajištění hladkého fungování státu a společnosti. Třetina respondentů se s nejzávažnějšími útoky vypořádala během několika hodin, nicméně řešení následků některých zabralo 9 % respondentů až měsíce (graf 23).

Navzdory obecnému trendu nespokojenosti s rozpočtem alokovaným na kybernetickou bezpečnost napříč ostatními sektory považovala většina respondentů z oblasti KI rozpočet v roce 2019 za dostatečný a oproti roku 2018 se u 45 % z nich zvýšil a u stejného množství subjektů zůstal stejný (graf 24). To naznačuje, že subjekty KI berou kybernetickou bezpečnost vážně a investují do ní natolik potřebné zdroje.

Kritickou informační infrastrukturou (KII) jsou dle ZKB [xiii] komunikační a informační systémy prvků kritické infrastruktury (KI). KI samotná je dle zákona č. 240/2004 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon) [xiv], definována jako prvek nebo systém prvků, jejichž narušení by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu.

Mezi typické prvky KI patří elektrárny, přehrady, letiště nebo telekomunikační sítě, ale také strategické finanční instituce nebo státní úřady. Vyřazení některého z těchto prvků může ochromit poskytování kritických služeb (elektřina, teplo, voda, výplata důchodů) nebo v krajním případě způsobit fyzické škody (například kybernetickou sabotáží).

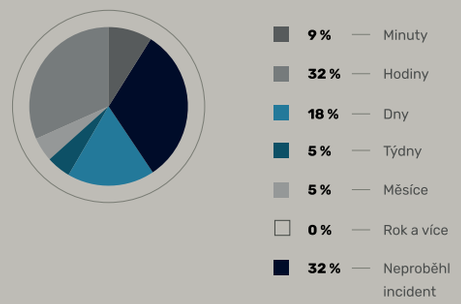
50 % odhalených incidentů v oblasti KII v roce 2019 vyústilo v omezení dostupnosti služeb

Kybernetická cvičení jako jeden z aspektů zabezpečení kritické infrastruktury

V roce 2019 NÚKIB zorganizoval první sektorové cvičení **Electro Czech** pro významné povinné subjekty v oblasti výroby, přenosu a distribuce elektrické energie. Simulovanou komplexní krizovou situací si prošlo na 40 účastníků celkem ze čtyř institucí.

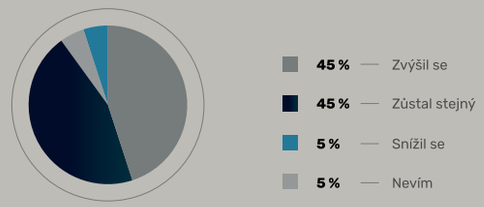
Graf 23:

Čas, jak dlouho respondentům trvalo vypořádání se s nejzávažnějším incidentem roku 2019 (%)



Graf 24:

Jak se v roce 2019 změnil rozpočet alokovaný na kybernetickou bezpečnost u respondentů z KII (%)



D | 03

Finanční sektor:

Zabezpečený, a přesto velmi lákavý cíl

Z absence vážnějších incidentů v roce 2019 lze vyvodit, že **český bankovní sektor je poměrně dobře zabezpečený**. Stále ale existují rozdíly ve vyspělosti jednotlivých finančních institucí, především ve smyslu ochrany proti pokročilým kybernetickým hrozbám. Obecně se ale banky snaží kybernetickou bezpečnost nepodceňovat, protože kompromitace jejich informačních systémů by mohla mít dalekosáhlé finanční i reputační následky. To se projevuje zejména investicemi do kybernetické bezpečnosti, mimo jiné v podobě vyšších platů pro odborníky. Finanční sektor byl jedinou oblastí, kde v naprosté většině neobsazenost míst v oblasti kybernetické bezpečnosti nesouvisela se mzdovými podmínkami. Ani jedna z dotazovaných finančních institucí svůj rozpočet na kybernetickou bezpečnost v roce 2019 nesnížila a 57 % ho naopak zvýšilo (graf 25). Kromě odborníků na kybernetickou bezpečnost finanční instituce investují také do vzdělávání uživatelů. Více než tři čtvrtiny dotazovaných finančních institucí aktivně testují odolnost svých zaměstnanců proti kybernetickým hrozbám. Ze všech dotazovaných organizací tak finanční instituce do kybernetické bezpečnosti investují nejvíce.

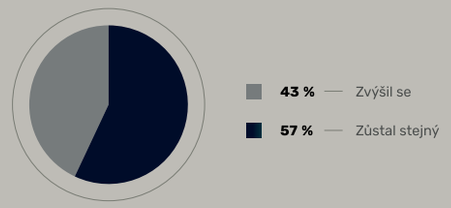
Stejně jako v roce 2018 **byli největší zranitelností v bankovním sektoru v roce 2019 uživatelé samotní.** Útočníci tohoto dlouhodobě slabého článku často využívali a bylo zaznamenáno množství phishingových kampaní na zákazníky tuzemských finančních institucí. Velmi často šlo o e-maily, které uživatele vyzývaly k přihlášení do internetového bankovnictví. Banky a další finanční instituce před těmito kampaněmi své klienty pravidelně varují.

Útoky na míru českým uživatelům

Pokračujícím trendem jsou **útoky na mobilní internetové bankovnictví, přičemž v roce 2019 se objevily škodlivé aplikace cílené přímo na klienty českých bank**. Škodlivé aplikace útočníkům umožňují ukrást přihlašovací data uživatelů. Šlo například o překladatelskou aplikaci **Word Translator** v obchodě Google Play pro operační systémy Android.[xv] Přes aplikaci se útočníci prostřednictvím snímání aktivit uživatele pokoušeli odcizit přihlašovací údaje pro přístup do internetového bankovnictví. Před svým zablokováním měl Word Translator přes deset tisíc stažení. Polovina detekcí malwaru byla zaznamenána v České republice a zhruba 40 procent v Polsku. Další podobnou aplikací v obchodě Google Play byla **Blockers Call 2019**, která rovněž cílila na internetové bankovnictví uživatelů.[xvi]

Graf 25:

Byly finance alokované na kybernetickou bezpečnost v organizacích respondentů v roce 2019 dostatečné? (%)



D | 04

Zdravotnictví:

Atraktivní a nedostatečně chráněný cíl

V prosinci 2019 došlo ke kybernetickému útoku proti systémům Nemocnice Rudolfa a Stefanie Benešov, spádové nemocnici až pro 400 000 lidí. Ransomware zašifroval data na serverech, nemocničních přístrojích a pracovních stanicích. V ordinacích nebylo možné provádět standardní ošetření, rušily se plánované operace a hospitalizovaní pacienti museli být převezeni do okolních nemocnic, včetně pacientů na jednotce intenzivní péče. Obnovení plného provozu trvalo téměř měsíc a následky útoku byly vyčísleny na 40–50 milionů korun.

Největší rizika v oblasti kybernetické bezpečnosti v českém zdravotnictví

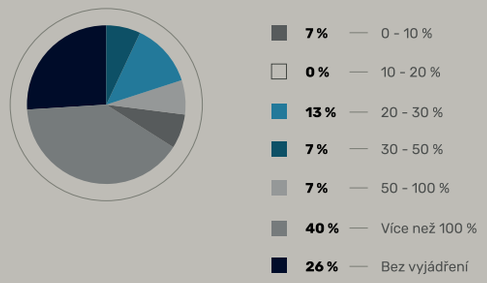
- Nedostatečná regulace standardů kybernetické bezpečnosti
- Nedostatečné plánování pro krizové situace
- Zastaralost softwaru
- Riziko odcizení dat

Finanční prostředky alokované na kybernetickou bezpečnost se v roce 2019 u dotazovaných organizací zpravidla pohybovaly mezi 0–5 % rozpočtu, přičemž většina respondentů takové finance považovala za nedostatečné. **Téměř polovina dotazovaných zdravotnických organizací by svůj rozpočet na kybernetickou bezpečnost navýšila o více než sto procent** (graf 26), což je nejvíce ze všech dotazovaných sektorů. Nejde však o novou ani překvapivou skutečnost, jelikož kybernetická bezpečnost byla v nemocnicích s jinými rozpočtovými prioritami dlouhodobě upozaďována. S ohledem na ransomwarové útoky proti českým nemocnicím v roce 2019 a na začátku roku 2020 je s ohledem na zachování provozuschopnosti nemocnic žádoucí, aby se tento stav změnil.

V návaznosti na nedostatek financí postrádají nemocnice pro zajištění kybernetické bezpečnosti i odborníky. Téměř polovina respondentů neměla obsazených 30–50 % pracovních míst (graf 27) a pro většinu jsou hlavním důvodem neobsazenosti míst mzdové podmínky, které uchazečům nabízejí.

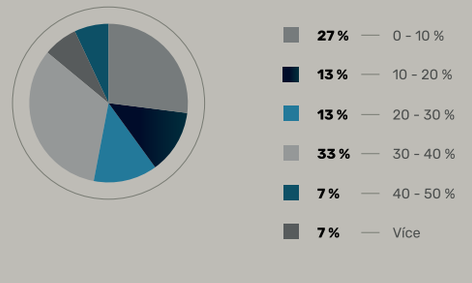
Graf 26:

O kolik procent by se rozpočet na kybernetickou bezpečnost nemocnic podle respondentů měl navýšit? (%)



Graf 27:

Procento neobsazených míst v oblasti kybernetické bezpečnosti v nemocnicích v roce 2019 (%)



D | 05

Akademický svět:
Nárůst zájmu kyberzločinců

Akademické instituce v České republice se v roce 2019 stávaly cílem zejména kyberzločinců **s finanční motivací**. Akademický svět byl v roce 2019 častým cílem spamu, phishingových kampaní a podvodných e-mailů, které cílily jak na studenty, tak na zaměstnance. E-maily měly různé podoby, od jednoduchých a plošně rozesílaných vyděračských až po sofistikované a specificky cílené podvodné e-maily, v nichž se útočníci vydávali za zaměstnance univerzity.

U phishingových útoků z roku 2019 byl patrný pokračující trend nárůstu sofistikovanosti, kdy útočníci namísto generického e-mailu psaného špatnou češtinou prokazovali detailní znalost prostředí tuzemských univerzit. Útočníci vystupovali jako reální zaměstnanci univerzit a podvodné stránky, na které phishingové a spear-phishingové e-maily odkazují, přesně kopírují vizuální styl jednotlivých pracovišť. V případě jednoho konkrétního phishingu se útočník vydával za rektora České zemědělské univerzity a v e-mailu vyzýval adresáta k podání cenové nabídky, jejíž vzor byl přiložen k e-mailu v podobě škodlivého souboru. [xvii]

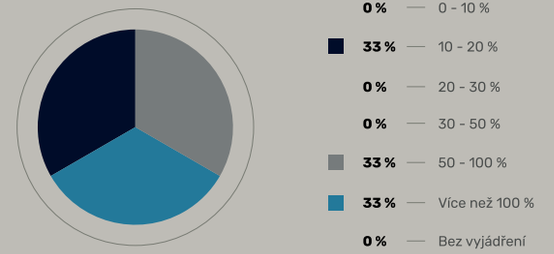
Univerzity jsou si zvýšené pozornosti kyberzločinců vědomy. Všichni respondenti uvedli, že se rozpočet jejich organizací na kybernetickou bezpečnost zvedl. Zároveň však žádný z respondentů nepovažuje finance za dostatečné a dvě třetiny z nich by byly pro jejich navýšení o více než 50 % (graf 28). Univerzity jsou z hlediska zajištění kybernetické bezpečnosti specifické tím, že musí brát v potaz nejen zaměstnance a četná pracoviště, ale také tisíce studentů, což vyžaduje i odpovídající náklady.

Kybernetické útoky na vzdělávací a výzkumné instituce nelze podceňovat. V případě kompromitace univerzitních sítí může dojít k úniku duševního vlastnictví a dosud nepublikovaných výsledků výzkumu. Pokud by útočníci v sítích českých univerzit působili nepozorovaně delší dobu, mohlo by to pro Českou republiku ve výsledku znamenat oslabení její konkurenceschopnosti a až miliardové finanční ztráty.

Ve Spojených státech se školy a univerzity staly jedním z nejčastějších cílů **ransomwaru** a v roce 2019 jich bylo zasaženo více než tisíc, čímž se po městech staly druhým nejčastějším cílem tohoto typu útoku v USA. Náznak tohoto trendu byl v roce 2019 patrný i v Evropě, kde byly na konci roku ransomwarem nakaženy sítě německé Universität Giessen a nizozemské Universität Maastricht. Existuje reálná možnost (pravděpodobnost 25–50 %), že se v roce 2020 a 2021 stanou cílem ransomwarových kampaní i české univerzity.

Graf 28:

O kolik procent by se rozpočet univerzit na kybernetickou bezpečnost podle respondentů měl navýšit? (%)



Kapitola E
Opatření

E | 01
Národní spolupráce v oblasti kybernetické bezpečnosti:
Implementace varování a spolupráce s dalšími dozorovými orgány

Implementace varování a spolupráce s dalšími dozorovými orgány

Za rok 2019 provedl NÚKIB **15 kontrol** podle ZKB, respektive vyhlášky 82/2018 Sb., o kybernetické bezpečnosti (dále „VKB"). Kontrola u povinných orgánů a osob dle ZKB ověřuje plnění povinností plynoucích ze ZKB a VKB. V rámci každé kontroly je ověřeno rámcově 150 kontrolních bodů.

Za rok 2019 proběhla také **metodická podpora**, která je prováděna na základě usnesení vlády a dopadá na všechna ministerstva a Úřad vlády ČR. Dobrovolně se k metodické podpoře každý rok navíc hlásí kancelář Poslanecké sněmovny a Senátu Parlamentu České republiky a také Kancelář prezidenta republiky. Metodická podpora je založena na individuální analýze kybernetické bezpečnosti každého ze subjektů a na ní založených konzultacích o vhodných řešeních identifikovaných kyberbezpečnostních nedostatků. Rozsahem pokrývá systémy spravované dotčenými subjekty, do kterých mohou pracovníci přistupovat z vnější sítě (internetu).

Stále platné varování proti technickým nebo programovým prostředkům společností Huawei a ZTE

NÚKIB na konci roku 2018 vydal varování, které se týká použití technických nebo programových prostředků společností Huawei Technologies a ZTE Corporation z Čínské lidové republiky. Varování bylo i v roce 2019 v platnosti a docházelo k jeho postupné implementaci.

V průběhu roku 2019 provedl NÚKIB průzkum mezi povinnými osobami dle ZKB, z něhož vyplynulo, že 27 povinných osob používalo v době průzkumu technologie Huawei a ZTE v systémech kritické informační infrastruktury (KII), významných informačních systémů (VIS) a poskytovatelů základních služeb (PZS). Po analýze rizik na základě varování 22 z nich vyřadilo technologie zmíněných společností z informačních systémů KII, VIS a PZS.

Spolupráce s dalšími dozorovými orgány v oblasti kontroly za rok 2019

NÚKIB v oblasti kontroly dlouhodobě usiluje o **spolupráci s dalšími dozorovými orgány** (regulátory) a o maximální společnou harmonizaci v oblastech s přesahem jimi dozorovaných (regulovaných) oblastí do oblasti kybernetické bezpečnosti. Kromě České národní banky a Úřadu pro civilní letectví, se kterými NÚKIB spolupracuje dlouhodobě, začala v roce 2019 spolupráce například se **Státním úřadem pro jadernou bezpečnost** a **Českým telekomunikačním úřadem**. Cílem spolupráce je především snaha minimalizovat zátěž regulovaných orgánů a osob. Vedle kontrol také stále probíhalo určování informačních systémů, které spadají do působnosti ZKB.

Počet určených subjektů ke konci roku 2019:

47 Správci a provozovatelé informačních a komunikačních systémů kritické informační infrastruktury	**109** Informační a komunikační systémy kritické informační infrastruktury
70 Správci a provozovatelé významných informačních systémů	**178** Významné informační systémy
38 Správci a provozovatelé informačních systémů základní služby	**42** Informační systémy základní služby

Podpůrné materiály NÚKIB na webu

NÚKIB na svých internetových stránkách pravidelně zveřejňuje podpůrné materiály a schémata týkající se výkladu zákona o kybernetické bezpečnosti, jejichž cílem je pro odbornou i širokou veřejnost zjednodušit problematiku spojenou s kybernetickou bezpečností. V roce 2019 NÚKIB například aktualizoval metodické materiály k zadávání veřejných zakázek v oblasti ICT a kybernetické bezpečnosti a další důležité materiály.

Tyto podpůrné materiály jsou k dispozici zde: **https://www.govcert.cz/cs/regulace-a-kontrola/podpurne-materialy/.**

E | 02
Cvičení kybernetické bezpečnosti:
Nárůst zájmu i provedených cvičení

V roce 2019 zaznamenal NÚKIB výrazné zvýšení poptávky po cvičeních ze strany organizací působících v České republice. Tento trend bylo možné v menší míře pozorovat již o rok dříve, nicméně až rok 2019 se stal poptávkou po cvičeních opravdu zlomovým. Na základě těchto změn lze usoudit, že cvičení se stávají respektovaným nástrojem pro zvyšování úrovně kybernetické bezpečnosti. **Cvičení podporovali a aktivně na nich participovali vedoucí pracovníci zúčastněných**

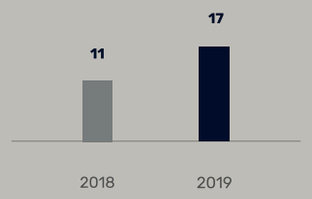
institucí ze sektorů státní správy či energetiky, stejně jako odborníci na danou problematiku. Nárůst zájmu o cvičení se projevil v jejich počtu. V roce 2019 uspořádal NÚKIB o 42 % více cvičení, kterých se zúčastnilo o 27 % více účastníků než v předchozím roce (graf 29 a 30). **V roce 2019 proběhla významná cvičení se zaměřením na orgány činné v trestním řízení, státní správu a energetický sektor.**

Proč jsou kybernetická cvičení užitečná

Cvičení jsou neocenitelným **zdrojem nových znalostí, zkušeností a technických schopností**. Dávají NÚKIB **možnost identifikovat a poukázat na slabá místa** v oblasti kybernetické bezpečnosti, stejně tak představují výborný **nástroj pro ověřování i revizi politik a procesů**. V neposlední řadě pak cvičení pomáhají **identifikovat, definovat či potvrzovat konkrétní trendy v oboru** a výstupy ze cvičení představují cenné poznatky, které jsou dále využívány pro **přípravu dalších osvětových či edukativních aktivit**. Žádanost a ohlas ze strany zahraničních partnerů, jakými jsou například Spojené státy americké, Izrael nebo Tchaj-wan, potvrzuje, že se cvičení stala **významným příspěvkem v české zahraniční politice**.

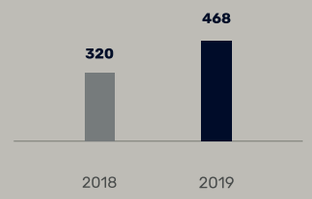
Graf 29:

Vývoj počtu cvičení pořádaných NÚKIB v roce 2018 a 2019



Graf 30:

Vývoj počtu účastníků cvičení pořádaných NÚKIB v roce 2018 a 2019



Cvičení kybernetické bezpečnosti v roce 2019

17
Počet cvičení pořádaných NÚKIB

12
Počet domácích cvičení

3
Počet cvičení pro zahraniční partnery

3
Počet multinárodních cvičení, do kterých se NÚKIB zapojil

468 (z 90 zemí)
Počet účastníků cvičení provedených NÚKIB

276
Počet účastníků v ČR

192
Počet účastníků v zahraničí

Významné poznatky ze cvičení v roce 2019:

01

Pro včasnou, efektivní a adekvátní reakci na závažné kybernetické incidenty by organizace měly disponovat předem připravenými krizovými plány v oblasti kybernetické bezpečnosti a příslušní pracovníci by tyto plány měli znát.

02

Jednou z největších výzev kybernetické bezpečnosti je sdílení informací mezi partnery (domácími i zahraničními), bez nichž je obtížné zasadit kybernetické útoky do širšího kontextu a odkrýt všechny aktivity útočníků, jejich motivace, cíle a přijmout adekvátní opatření.

Úspěchy NÚKIB na mezinárodních cvičeních v roce 2019

V dubnu 2019 se český tým tvořený NÚKIB a experty ze státní, soukromé i akademické sféry umístil na druhém místě (z 22 týmů) v mezinárodním cvičení Locked Shields, které je považováno za nejkomplexnější technické cvičení na světě.

V listopadu český tým, jehož součástí byli i pracovníci NÚKIB, zvítězil na mezinárodním cvičení CODE 2019, které se konalo na Tchaj-wanu.

E|03

Osvěta a vzdělání v ČR:

Vzdělávání uživatelů všech věkových kategorií

Velmi důležitou proměnou v kybernetické bezpečnosti České republiky je vzdělávání. Bezpečné využívání digitálních technologií je jednou ze základních kompetencí digitální gramotnosti a zaslouží si patřičnou pozornost. Osvětové aktivity v oblasti kybernetické bezpečnosti byly v České republice v roce 2019 poměrně pestré a kromě zaměstnanců veřejné správy se nejvíce zaměřovaly na zranitelné skupiny populace, jimiž jsou především děti a senioři.

Mezi celorepublikové osvětové a vzdělávací aktivity v oblasti kybernetické bezpečnosti, které probíhaly v roce 2019, patří například:

E-Bezpečí:

Projekt Univerzity Palackého v Olomouci, v oblasti internetové bezpečnosti zaměřený na různé cílové skupiny (senioři, pedagogové, rodiče, žáci a studenti).

Chytrá škola:

Portál poskytující informace především pedagogům a rodičům.

Internetem bezpečně:

Projekt spolku you connected, z.s., v rámci kterého vznikl informační web, osvětová videa, přednášky a vzdělávací učebnice.

Buď safe online:

Osvětový online projekt antivirové společnosti Avast, který poskytuje materiály a interaktivní hry pro učitele, rodiče i děti. S youtuberem Jirkou Králem byl připraven soubor vzdělávacích videí zaměřených na jednotlivé hrozby v kyberprostoru.

Kyberkompas:

Šestidílný online kurz Masarykovy univerzity, která jej poskytuje svým studentům i široké veřejnosti. Kurz zvyšuje uživatelské kompetence v oblasti zabezpečení zařízení, nastavení hesel nebo i hlášení incidentů.

Internetem bezpečně:

Osvětový projekt sdružení CZ.NIC, který připravuje především audiovizuální osvětový obsah. Projekt nabízí řadu vzdělávacích krátkometrážních filmů i osmidílný seriál #Martyisdead.

NÚKIB v průběhu roku 2019 aktualizoval svůj e-learningový portál a poskytované online kurzy. Pro rozsáhlou skupinu úředníků veřejné správy NÚKIB aktualizoval kurz **Dávej kyber!** zaměřený na základy kybernetické hygieny a informační bezpečnosti. Do kurzu bylo zapsáno celkem 6 953 uživatelů a certifikát o absolvování získalo **5 172 uživatelů**. Tento počet rozšířil již proškolené úředníky státní správy z roku 2018, kterých bylo **21 443**.

Druhý online kurz NÚKIB **Šéfuj kyber!** je naopak určen IT administrátorům a těm, kdo zastávají pozici manažerů kybernetické bezpečnosti nebo jinou z rolí podle ZKB. Do kurzu Šéfuj kyber! bylo zapsáno 422 uživatelů a certifikát o absolvování získalo celkem **287 uživatelů**.

NÚKIB se v osvětové činnosti a vzdělávacích aktivitách v oblasti kybernetické bezpečnosti dále zabýval následujícími projekty:

Městečko kybernetov

NÚKIB začal v roce 2019 připravovat inovativní **deskovou hru pro mateřské školy Městečko Kybernetov,** která dětem od 5 do 9 let věku nenásilnou formou představuje problémy závislosti na komunikačních technologiích, kyberšikany a kybergroomingu a zdraví.

Digitální stopa

V roce 2019 byla upravena a zdokonalena online vzdělávací aktivita **Digitální stopa**; zábavný interaktivní příběh pro žáky 5. a 6. třídy, který hravou formou představuje aktuální rizikové jevy a učí bezpečnému chování na internetu.

Senzační senioři

Ve spolupráci se sdružením **Senzační senioři (SenSen)** se NÚKIB zapojil do série sedmi přednášek pro seniory, které byly uspořádány napříč městy v České republice. Celá série byla zakončena konferencí v Praze.

Vanda a Eda v Onl@jn světě

Pro mateřské školy vytvořil NÚKIB knihu s názvem Vanda a Eda v Onl@jn světě, která je doplněna o metodické karty využitelné učitelem. Kniha obsahuje příběhy, které jednoduchou formou seznamují předškoláky s riziky při používání digitálních technologií. Knihu NÚKIB vydal v tištěné formě, rozeslal do více než 5300 mateřských škol v České republice a zároveň ji nabízí ke stažení na webu. [xviii]

Network Security Monitoring Cluster

NÚKIB v roce 2019 pokračoval v podpoře projektu **Network Security Monitoring Clusteru** na vybudování krajských středoškolských **juniorních center excelence kybernetické bezpečnosti**, které by poskytovaly odbornou i technickou pomoc při výuce kybernetické bezpečnosti celému regionu. Cílem je, aby v každém kraji byla minimálně jedna střední škola, která bude zastávat úlohu juniorního centra.

NÚKIB se v roce 2019 angažoval v pracovních skupinách rezortu školství, které připravují revize rámcových vzdělávacích programů. V roce 2019 NÚKIB rovněž začal spolupráci s komisí Ministerstva vnitra pro akreditaci vzdělávacích aktivit, kde vydává posudek k žádostem o akreditaci z oblasti kybernetické bezpečnosti. Během roku 2019 vydal NÚKIB celkem pět posudků.

Výzkum a vývoj: Kryptografie a ochrana před škodlivým zářením

V roce 2019 bylo v rámci NÚKIB řešeno několik výzkumných a vývojových projektů v oblastech aplikované kryptografie, vývoje speciálních měřicích metod a technologií při zajišťování ochrany před kompromitujícím vyzařováním a výzkum a vývoj kryptografických prostředků určených k ochraně utajovaných informací.

15 přednášek pro státní správu, knihovny, univerzity, soudy, nemocnice atp.

17 aktivit pro žáky mateřských či základních škol

8 přednášek pro žáky středních škol

8 přednášek pro seniory

6 přednášek pro rodiče

E | 04

Mezinárodní spolupráce:
Podíl na globální kybernetické bezpečnosti

Mnoho rozhodnutí podstatných pro vývoj kybernetické bezpečnosti v České republice je tvořeno nikoli pouze na vnitrostátní, ale také na mezinárodní úrovni. Zájmy České republiky v oblasti kybernetické bezpečnosti v klíčových mezinárodních organizacích, zejména pak v EU, OSN, NATO, ale i OECD a OBSE, zastupuje NÚKIB společně s Ministerstvem zahraničních věcí (dále „MZV"), Ministerstvem obrany a dalšími partnery. [6] V roce 2019 se NÚKIB soustředil zejména na jednání s členskými státy a institucemi EU, a to především pokud jde o agendu tzv. kybernetického balíčku (například ECCG – Evropská skupina pro kybernetickou certifikaci), 5G EU Toolboxu, závěrů Evropské rady i Rady EU (Cyber Diplomacy Toolbox, Blueprint), povinností vyplývajících ze směrnice NIS a nového legislativního návrhu o kompetenčním centru. V rámci OSN byla ustavena tzv. Otevřená pracovní skupina, na jejíž činnosti se NÚKIB a MZV také aktivně podílejí.

Prague 5G Security Conference a zveřejnění Pražských návrhů

NÚKIB společně s MZV v roce 2019 zorganizoval první ročník mezinárodní expertní konference k bezpečnosti 5G sítí. Prague 5G Security Conference se uskutečnila ve dnech druhého a třetího května 2019 pod záštitou a za osobní účasti

[6] Ministerstvo průmyslu a obchodu, Český telekomunikační úřad a další.

předsedy vlády ČR Andreje Babiše a ministra zahraničních věcí ČR Tomáše Petříčka. Dvoudenní uzavřené mezinárodní konference se zúčastnilo přes 150 vládních představitelů a expertů z více než 32 států, včetně představitelů EU a NATO.

Hlavním výstupem expertní konference bylo zveřejnění tzv. Pražských návrhů, série doporučení týkajících se bezpečnosti 5G sítí. Pražské návrhy mimo jiné zdůrazňují **důležitost netechnických aspektů** bezpečnosti komunikační infrastruktury a zásadní roli důvěry uživatelů (včetně státu) ve výrobce používaného hardwaru a softwaru.

Prague 5G Security Conference i samotné Pražské návrhy zaznamenaly značný mezinárodní ohlas a staly se vodítkem pro řadu bilaterálních dohod v oblasti kybernetické bezpečnosti, které byly během roku 2019 uzavřeny. Netechnické aspekty a otázka důvěry v dodavatele byly rovněž zařazeny mezi klíčové charakteristiky bezpečnosti 5G sítí a promítnuty do EU 5G Toolboxu. Pražské návrhy jsou tak významným příspěvkem České republiky ve formulaci principů bezpečnosti 5G na globální úrovni, na který naváže druhý ročník Prague 5G Security Conference plánovaný na září 2020.

Pražské návrhy:

Překlad Pražských návrhů naleznete zde:
https://nukib.cz/download/5G%20site/Prazske-navrhy-5G-Sec-190503-cz.pdf.

Originál je k přečtení zde:
https://nukib.cz/download/5G%20site/Prague-Proposals-5G-Sec-190503.pdf.

EU Toolbox: opatření k bezpečnosti 5G sítí v EU

Toolbox představuje sadu konkrétních opatření k tomu, jak by měla být bezpečnost sítí 5G v členských státech nastavena, regulována a realizována. Česká republika, spolu s Francií a dalšími členskými státy, zastávala při přípravě tohoto 5G EU Toolboxu vedoucí úlohu, což znamenalo i skutečnost, že se do výsledného dokumentu podařilo z velké části promítnout český přístup. Z nejdůležitějších aspektů lze zmínit požadavek na to, aby v případě analýzy rizik byly hodnoceny nejen technické hrozby, ale i ty netechnické. Příkladem je právní a politické prostředí země, ze které výrobce pochází, neboť to má zásadní dopady na důvěryhodnost produkovaných technologií.

E | 05
Síťové sondy v klíčových orgánech státu:
Noví partneři i nové projekty

Aby Česká republika měla lepší povědomí o škodlivých aktivitách napříč strategickými sítěmi státu, realizuje NÚKIB projekt s názvem **„Systém detekce kybernetických bezpečnostních událostí ve vybraných ISVS“[7].** Jeho cílem je pomocí rozmístění síťových sond usnadnit administrátorům těchto klíčových státních sítí nalezení případného útočníka a lépe tyto sítě chránit.[8]

V rámci tohoto systému došlo v roce 2019 ke **zlepšování schopností centrálního analytického nástroje**. Došlo k jeho napojení na interní databáze NÚKIB a v rámci následného provozu a zkušeností se připravují návrhy změn v tomto napojení, aby umožňovalo poskytovat další potřebné funkcionality a poskytovalo další typy dat. Také byla zpřesňována pravidla pro automatizované vyhledávání podezřelého datového provozu a událostí cílících na více zapojených organizací.

[7] Informační systémy veřejné správy.
[8] Projekt nesouvisí s plány rozmisťování sond v sítích elektronických komunikací ze strany Vojenského zpravodajství.

V průběhu roku bylo také zahájeno jednání s dalšími potenciálními partnery, kteří provozují vlastní síťovou sondu sledující provoz na perimetru sítě. S těmito partnery byly upřesněny dohody o jejich zapojení do projektu a na konci roku proběhlo vlastní technické připojení.

Na konci roku 2019 byly síťové sondy nasazeny u 23 partnerů z oblasti státní správy. Místní správci byli patřičně proškoleni a začali s GovCERT.CZ sdílet kybernetické bezpečnostní události a vybraná data o síťovém provozu procházejícím přes perimetr sítě.

Síťové sondy pomohou upozornit na podezřelá datová spojení, anomální objemy dat opouštějící konkrétní síť, rozpoznají „oťukávání“ sítě zvnějšku a budou sloužit i jako nástroj včasného varování před blížícími se útoky. Sondy mají také schopnost získávat a uchovávat popisná data o provozu a vytvořit tak auditní stopu pro pozdější zkoumání toho, k čemu na daném ministerstvu nebo úřadě došlo. Díky sdílení dat s partnery bude NÚKIB schopen dohledat i bezpečnostní incidenty, které by v rámci jednoho rezortu nebyly detekovány, případně by nebyly vyhodnoceny jako nebezpečné,
a informovat o nich další organizace ještě před jejich případným zasažením.

Kapitola F

Výhled trendů v kybernetické bezpečnosti na roky 2020 a 2021

Ransomware:

Kyberkriminální aktivity využívající malware, který zablokuje přístup k datům a žádá výkupné, bude v roce 2020 a 2021 téměř jistě (pravděpodobnost 90–100 %) jednou z nejvýznamnějších hrozeb. Přestože počet infikovaných uživatelů může průběžně klesat, u ransomwaru lze v současnosti sledovat trend zvýšené sofistikovanosti kampaní a jejich cílení, který bude velmi pravděpodobně pokračovat v letech 2020 a 2021. Stejně jako je tomu v případě phishingu, i zde útočníci využívají tématu pandemie covid-19, aby zvýšily úspěšnost svých útoků. S ohledem na zahraniční trendy a dosavadní vývoj v České republice je velmi pravděpodobné (pravděpodobnost 75–85 %), že se cílem ransomwaru budou stávat instituce územní samosprávy a zdravotnická a vzdělávací zařízení, zejména pak vysoké školy a univerzity.

Cloud:

Organizace ve stále větší míře využívají cloudovou infrastrukturu a platformy jako službu, která vedle řady pozitiv přináší také svá rizika. Jejich využívání znamená, že se citlivá data organizací nacházejí v prostředí, jehož údržbu a monitoring nemají plně pod kontrolou a které je dostupné z internetu. Cloudová infrastruktura navíc mnohdy bývá nevhodně nakonfigurována. Obchodní tajemství a další citlivá data umístěná na cloudu představují lákavý cíl jak pro státní cizí aktéry, tak pro kyberkriminální skupiny. Trend nebezpečí kompromitace cloudových služeb bude v letech 2020 a 2021 velmi pravděpodobně (pravděpodobnost 75–85 %) sílit a cílem se stanou zejména jejich poskytovatelé. Nelze vyloučit (s pravděpodobností 25–50 %), že mezi poškozenými budou i české instituce nebo firmy.

Mobilní malware:

V roce 2020 a 2021 se čeští uživatelé budou pravděpodobně (pravděpodobnost 55–70 %) více setkávat se škodlivými mobilními aplikacemi, které se budou vydávat za legitimní. Útočníkům půjde velmi pravděpodobně (pravděpodobnost 75-85 %) především o přístup do internetového bankovnictví svých obětí.

Phishing, spear-phishing a podvodné e-maily:

Rok 2019 se nesl v trendu sofistikovanějších a cílenějších škodlivých e-mailů, ve kterých útočníci dokazovali lepší znalost prostředí, jazyka a vysokou variabilitu témat. Zdokonalování technik sociálního inženýrství bude téměř jistě (pravděpodobnost 90–100 %) pokračovat i v roce 2020 a 2021. Již na začátku roku 2020 je ve světě a v České republice patrný trend zneužívání pandemie covid-19 v agresivních phishingových kampaních. Nelze rovněž vyloučit (pravděpodobnost 25–50 %), že se čeští uživatelé začnou častěji setkávat nikoli pouze s podvodnými e-maily, ale také s podvodnými telefonáty za využití deepfake technologií, díky kterým mohou útočníci imitovat hlas cizí osoby (například ředitele firmy). Této metody lze využít i pro velmi sofistikované spear-phishingové kampaně.

Nedostatek odborníků:

Některé sektory se v roce 2019 potýkaly s problémem obsadit pracovní místa v oblasti kybernetické bezpečnosti odborníky, zpravidla z důvodů nedostatečných financí. Tento stav bude v České republice velmi pravděpodobně (pravděpodobnost 75–85 %) pokračovat i v letech 2020 a 2021. Kybernetická bezpečnost vyžaduje nezanedbatelné investice a v řadě organizací bývá kvůli prioritizaci jiných oblastí upozaďována. V kombinaci s každoročně rostoucím počtem kybernetických útoků a jejich zdokonalováním tento stav ve vybraných sektorech (zdravotnictví, školství a instituce státní správy a územní samosprávy) v letech 2020 a 2021 pravděpodobně (pravděpodobnost 55–70 %) povede k vyššímu počtu úspěšných kybernetických útoků.

Kapitola G

Přílohy

G | 01

Příloha 1:

Údaje o incidentech řešených na GovCERT.CZ

V průběhu roku 2019 obdrželi pracovníci GovCERT.CZ od českých i zahraničních partnerů v souhrnu 217 relevantních hlášení o kybernetických bezpečnostních incidentech. Tato hlášení byla dále vyhodnocována ve vztahu k oblasti působnosti týmu GovCERT.CZ a následně zpracována buď vlastními prostředky, nebo předána příslušným subjektům. Za uplynulý rok tak bylo z přijatých hlášení a z informací získaných vlastními prostředky vyhodnoceno, zpracováno a řešeno 78 kybernetických bezpečnostních incidentů spadajících do oblasti působnosti vládního CERT.

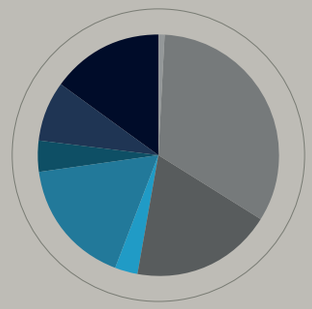
Proti roku 2018, kdy bylo GovCERT.CZ nahlášeno 164 incidentů a vyřešeno 54, jde o znatelný nárůst.

Mezi nejzávažnější incidenty, které GovCERT.CZ v roce 2019 řešil, byl bezesporu případ infikování systémů Nemocnice Rudolfa a Stefanie Benešov a těžební společnosti OKD ransomwarem Ryuk. Ačkoli benešovská nemocnice ani OKD nejsou povinnými osobami dle ZKB, vyslal NÚKIB po dohodě s poškozenými organizacemi na místo svůj tým. Jeho členové se podíleli na obnově informační sítě, forenzní a síťové analýze a pomoci s nastavením základních bezpečnostních prvků.

Dalším incidentem, který GovCERT.CZ v roce 2019 řešil, bylo infikování státní instituce malwarem Emotet. Instituce předala disky deseti napadených počítačů k analýze, na jejímž základě Úřad doporučil, jak se s nákazou vypořádat.

Graf 33:

Klasifikace řešených incidentů v roce 2019



Popis kategorií vychází z formuláře pro hlášení incidentů:

- **15 %** — Škodlivý obsah (například virus, červ, trojský kůň, dialer, spyware)
- **8 %** — Průnik (například úspěšná kompromitace aplikace nebo uživatelského účtu)
- **4 %** — Pokus o průnik do systému (například pokus zneužití zranitelnosti, kompromitace aktiva, "0-day" útok)
- **17 %** — Narušení informační bezpečnosti
- **3 %** — Sběr informací (například skenování, sniffing, sociální inženýrství)
- **19 %** — Podvod (Phishing)
- **33 %** — Dostupnost (například narušení dostupnosti způsobené DoS/DDoS útokem nebo sabotáží)
- **1 %** — Urážlivý obsah (například spam, kyberšikana, nevhodný obsah)
- **0 %** — Administrativní (například bezpečnostní incident způsobený administrativní chybou)

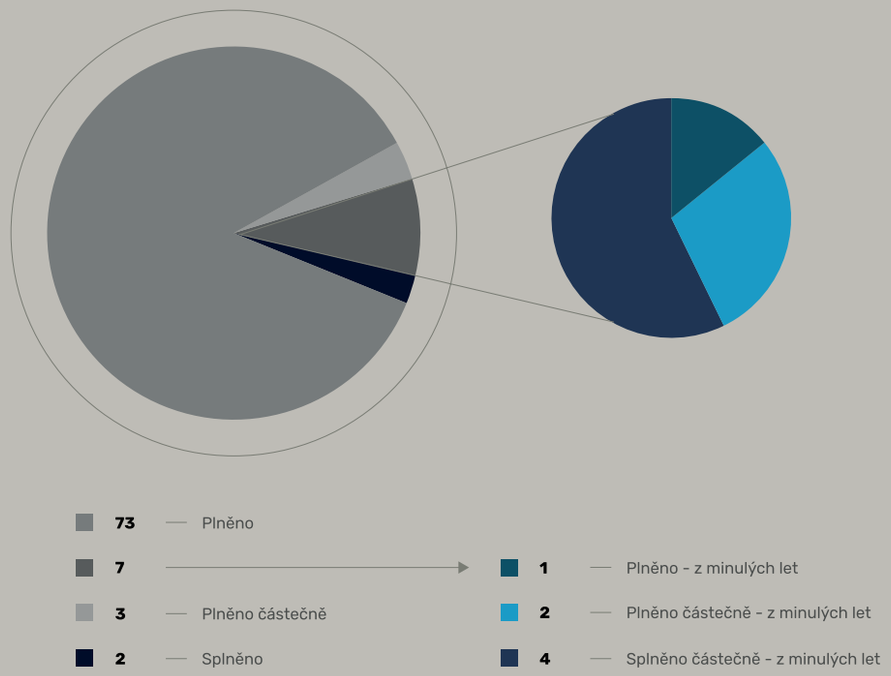
G | 02

Příloha 2:
Naplňování Akčního plánu

Rok 2019 byl předposledním rokem plnění současného Akčního plánu k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020. To se projevilo na klesajícím absolutním počtu zadaných úkolů v porovnání s předešlými roky. V roce 2019 došlo navíc k plnění nesplněných úkolů z minulých let. Lze konstatovat, že většina úkolů byla splněna či byla plněna průběžně a jen minimum úkolů bylo tzv. splněno částečně, tedy s nějakými nedostatky. Mezi **splněné úkoly** (ve spolupráci s dalšími subjekty) v roce 2019 patřilo například vypracování národní koncepce výzkumu a vývoje v oblasti kybernetické bezpečnosti a vytvoření databáze výzkumných projektů v rámci kybernetické bezpečnosti, z níž jsou informace podávány dalším subjektům.

Graf 34:

Plnění Akčního plánu v roce 2019



Příkladem **částečně plněného** úkolu bylo vytvoření a zavedení honeypot systému k detekci kybernetických hrozeb a anomálií v síťovém provozu s cílem identifikovat potenciální kybernetické hrozby. V roce 2019 došlo pouze k částečnému splnění. Honeypot detektory jsou aktuálně nasazeny v sítích NÚKIB a postupně je jejich počet dále navyšován. K detekci anomálií v síťovém provozu je nasazen centrální analytický software, do kterého jsou dále zapojeni vybraní partneři. V současné době dochází k zapojování nových partnerů v závislosti na dostupných kapacitách licencí analytického softwaru, optimalizaci systému a k jeho dalšímu rozšiřování.

G | 03

Pravděpodobnostní výrazy použité ve Zprávě o stavu kybernetické bezpečnosti za rok 2019

Pravděpodobnostní výrazy a vyjádření jejich procentuálních hodnot.

Výraz	Pravděpodobnost
Téměř jistě	90–100 %
Velmi pravděpodobně	75–85 %
Pravděpodobně	55–70 %
Nelze vyloučit / Reálná možnost	25–50 %
Nepravděpodobně	15–20 %
Velmi nepravděpodobně	0–10 %

G | 04

Zdroje:

i **Rozhlas. 2020. Na nemocnici v Benešově útočil ruský virus Ryuk. Jermanová odmítá, že by někdo požadoval výkupné.** https://www.irozhlas.cz/zpravy-domov/nemocnice-benesov-kyberneticky-utok-ransomware-vykupne-ochrana-osobnich-udaju_2001140615_cha

ii **Policie ČR. 2018. Kyberkriminalita.** https://www.policie.cz/clanek/kyberkriminalita.aspx

iii **BIS. 2018. Výroční zpráva Bezpečnostní informační služby za rok 2017.** https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2017-vz-cz.pdf

iv **401TRG. 2018. Burning Umbrella: An Intelligence Report on the Winnti Umbrella and Associated** State-Sponsored Attackers. https://401trg.com/burning-umbrella/

v **Reuters. 2019. BASF, Siemens, Henkel, Roche target of cyber attacks.** https://www.reuters.com/article/us-germany-cyber/basf-siemens-henkel-roche-target-of-cyber-attacks-idUSKCN1UJ147

vi **Cyberscoop. 2017. Research claims CCLeaner attack carried out by Chinese-linked group.** https://www.cyberscoop.com/ccleaner-attack-china-intezer-labs-piriform-apt17/

vii **Check Point. 2019. October 2019's Most Wanted Malware: the Decline of Cryptominers Continues, as Emotet Botnet Expands Rapidly.** https://blog.checkpoint.com/2019/11/12/october-2019s-most-

wanted-malware-the-decline-of-cryptominers-continues-as-emotet-botnet-expands-rapidly/

viii **Check Point. 2020. Helping you navigate the ever-changing security landscape: Check Point Research's 2020 Cyber Security Annual Report** https://blog.checkpoint.com/2020/01/15/the-2020-check-point-cyber-security-annual-report-is-available/

ix **BIS. 2019. BIS spolupracovala se společností Avast na odvrácení útoku na její produkty.** https://www.bis.cz/aktuality/bis-spolupracovala-se-spolecnosti-avast-na-odvraceni-utoku-na-jeji-produkty-6acda7bf.html

x **CyberScoop. 2017. Research claims CCLeaner attack carried out by Chinese-linked group.** https://www.cyberscoop.com/ccleaner-attack-china-intezer-labs-piriform-apt17/

xi **Econlab. 2019. Analýza: Necenová kritéria při zadávání veřejných zakázek v EU.** https://econlab.cz/files/2019/07/2019-07-22-MPSV%20-%20studie%20kriteria.pdf

xii **ÚOHS. 2019. Č. j.: ÚOHS-S0262/2019/VZ-30266/2019/523/Jma.** https://www.uohs.cz/cs/verejne-zakazky/sbirky-rozhodnuti/detail-16400.html

xiii **Národní centrum kybernetické bezpečnosti. 2018. Aktuální legislativa.** https://www.govcert.cz/cs/regulace-a-kontrola/legislativa/

xiv **Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), v aktuálním znění.** https://www.zakonyprolidi.cz/cs/2000-240

xv **Eset. 2019. ESET informuje o další nebezpečné aplikaci, nástroj pro překládání textů cílil na klienty bank v Česku.** https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/eset-informuje-o-dalsi-nebezpecne-aplikaci-nastroj-pro-prekladani-textu-cilil-na-klienty-bank-v-ces/

xvi **Česká spořitelna. 2019. Upozornění na podvodnou mobilní nebankovní aplikaci.** https://www.csas.cz/cs/zpravy-z-banky/2019/01/22/upozorneni-na-podvodnou-mobilni-aplikaci

xvii **Česká zemědělská univerzita. 2019. Cenová poptávka.** https://www.oikt.czu.cz/cs/r-13742-spam/r-13743-vzory/cenova-poptavka-ceska-zemedelska-univerzita-v-praze-uni-784-.html

xviii **NÚKIB. 2019. Vanda a Eda v Onl@jn světě.** https://nukib.cz/download/vzdelavani/rozcestniky/Vanda_a_Eda_v_Onljn_svete_kniha_s_kartami.pdf