ZPRÁVA O STAVU KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY ZA ROK 2020

Národní úřad
pro kybernetickou
a informační bezpečnost

ÚVODNÍ SLOVO ŘEDITELE ÚŘADU

Vážené čtenářky, vážení čtenáři,

do rukou se Vám dostává Zpráva o stavu kybernetické bezpečnosti za rok 2020. Nemá smysl připomínat, kolik zvratů v tomto roce prodělala nejen Česká republika, ale prakticky celý svět. Rád bych však alespoň krátce zmínil, co globální pandemie znamenala pro oblast kybernetické bezpečnosti.

Uplynulý rok nám všem ukázal, že hranice toho, co všechno lze přesunout do kyberprostoru, leží daleko dál, než jsme si dokázali představit. Tento přechod však také ukázal, jak moc jsme závislí na informačních a komunikačních technologiích.

Experti z oblasti IT a kybernetické bezpečnosti na tuto závislost poukazují již léta. Ale teprve loňský rok, kdy se internet stal pro nespočet lidí jediným místem, kde šlo pracovat, uzavírat obchody, vést jednání i udržovat kontakt se svými blízkými, nám ukázal, jak obrovská tato závislost ve skutečnosti je.

Ale vnímejme to jako příležitost. Virus nám pomohl v tom, co jsme doposud sami nedokázali – přesvědčit většinu společnosti o tom, že kybernetickou bezpečnost a obecně náležitosti správného chování v kyberprostoru musí řešit každý z nás.

Následující texty a statistiky ukazují, že kyberprostor není bezpečným místem. Nikdo nemohl přehlédnout útoky ransomwarem, které v době nastupující pandemie ochromily mimo jiné Fakultní nemocnici Brno a způsobily škody za stovky milionů korun. Naše statistiky dále ukazují, že počet útoků kontinuálně narůstá a že jejich obětí se stávají další a další instituce, například samosprávy.

Jako Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) jsme se snažili zasaženým subjektům maximálně pomoci a zároveň ochránit ty, které by útoky mohly postihnout také. Připomenu vydání reaktivního opatření pro vybrané subjekty ve zdravotnictví a následně vydání varování pro stejný okruh příjemců. Mimo to jsme také vypracovali řadu podpůrných materiálů, které může kdokoliv zdarma použít k zabezpečení svých systémů.

Speciálně pro oblast zdravotnictví jsme vypracovali změnu legislativy, která je účinná od ledna letošního roku. Díky ní musí výrazně více nemocnic plnit podstatně přísnější nároky na bezpečnost a zároveň mohou šířeji využívat služby, které regulovaným subjektům zdarma nabízíme. Ať už jsou to skeny zranitelností, penetrační testování nebo další aktivity.

Mimo to jsme spustili řadu vzdělávacích kurzů pro veřejnost i pro zaměstnance důležitých institucí. Právě lidé bývají tím nejslabším článkem kybernetické bezpečnosti a je nezbytné, aby měli povědomí o rizicích, která na ně v kyberprostoru mohou číhat.

Mezi jednoznačné úspěchy bych zařadil schválení dvou dokumentů, které jsou zásadní pro rozvoj kybernetické bezpečnosti ČR i samotného NÚKIB. Jedná se o Národní strategii kybernetické bezpečnosti, která pro příštích pět let udává směr činnosti nejen našemu úřadu, ale všem subjektům, které se na zajišťování kybernetické bezpečnosti ČR podílejí. Bez nich a bez vzájemné spolupráce by nevznikla nejen tato Zpráva o stavu kybernetické bezpečnosti, ale především by vůbec nebylo možné kybernetickou bezpečnost ČR zajišťovat.

Druhým zásadním dokumentem je Koncepce rozvoje NÚKIB, která ukazuje, jakým způsobem se bude úřad dále rozvíjet, jaké kapacity chceme do budoucna mít a v neposlední řadě, kolik to bude stát. Jsem rád, že se práci na tomto dokumentu podařilo dotáhnout do konce. NÚKIB je stále ještě nový úřad a je nezbytné, aby bylo jasné, kam chceme jeho další rozvoj směřovat.

Z mezinárodního dění bych rád připomněl druhý ročník Prague 5G Security Conference, který se stejně jako ročník předešlý odehrál pod záštitou premiéra ČR a s účastí řady významných zahraničních hostů.

Loňský rok nám tedy všem ukázal nejen to, jak umí být kyberprostor nebezpečný, ale i to, jak nesmírně důležitý pro nás všechny je. Rád bych proto poděkoval všem 222 subjektům z nejrůznějších oblastí, které se formou vypracování našich dotazníků podílely na přípravě této Zprávy o stavu kybernetické bezpečnosti za rok 2020. Pevně doufám, že tato zpráva přispěje k šíření povědomí o kybernetické bezpečnosti a pomůže tak zvyšovat bezpečí nás všech.

Ing. Karel Řehka

SHRNUTÍ ZPRÁVY O STAVU KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY ZA ROK 2020

Rok 2020 se vyznačoval nárůstem počtu kybernetických útoků proti českým institucím, organizacím a firmám ve všech sektorech. V roce 2020 bylo NÚKIB nahlášeno 468 incidentů oproti 217 incidentům v roce 2019. Téměř třetinu z řešených incidentů nahlásily neregulované subjekty. Za tímto nárůstem stojí velmi pravděpodobně vyšší počet kybernetických útoků i větší povědomí o existenci a aktivitách NÚKIB. Vzrostla také závažnost incidentů, jak ukazují útoky proti Fakultní nemocnici Brno nebo Psychiatrické nemocnici Kosmonosy. Nejčastějšími typy útoků byly v roce 2020 **spam, phishing a scanning**.

Mezi nejvážnější hrozby pro kybernetickou bezpečnost ČR dlouhodobě patří kybernetická kriminalita. V roce 2020 byla nejvíce vidět u **ransomwarových útoků, které zasáhly český zdravotnický sektor**. Nárůst útoků proti nemocnicím lze do velké míry přisoudit probíhající pandemii i zacílení kyberkriminálních skupin na konkrétní instituce s vyšší pravděpodobností zaplacení výkupného. I přesto považují tři čtvrtiny zdravotnických zařízení finance k zajištění kybernetické bezpečnosti za nedostatečné.

NÚKIB ve spolupráci s Úřadem vlády a Ministerstvem zahraničních věcí uspořádal v září 2020 druhý ročník dvoudenní Prague 5G Security Conference, předního světového fóra pro diskusi o rizicích spojených s budováním 5G infrastruktury. Stejně jako minulý rok proběhla pod záštitou předsedy vlády ČR Andreje Babiše. Přestože se konference s ohledem na situaci spojenou s covid-19 poprvé konala virtuálně, vystoupilo na ní přes 50 řečníků z Evropy, USA, Jižní Koreje, Izraele, Austrálie, Indie a dalších zemí. Hlavním výstupem druhého ročníku bylo představení a spuštění tzv. **Prague 5G Security Repository**, virtuální knihovny určené ke sdílení legislativních, strategických a dalších nástrojů, které státy v uplynulém roce v oblasti bezpečnosti 5G sítí přijaly.

V roce 2020 NÚKIB pokračoval ve vzdělávání zaměstnanců státní správy a v rámci e-learningového kurzu Dávej kyber! **proškolil více než 18 209 zaměstnanců státní správy, 214 pracovníků Armády ČR a 2 000 pracovníků Fakultní nemocnice Na Bulovce**. Odborný kurz Bezpečně v kyber, který zaměstnance seznamuje se situacemi ze školního prostředí, absolvovalo **1 690 pracovníků prevence**.

V roce 2020 se řada dotazovaných organizací potýkala s nedostatkem odborníků a nedostatečnými rozpočty v oblasti kybernetické bezpečnosti. Tato situace byla citelnější v sektoru státní správy než u soukromých společností. Téměř žádný z respondentů neměl obsazené všechny pozice v oblasti kybernetické bezpečnosti. Více než polovina organizací za hlavní faktor uvedla nedostatečné mzdové podmínky.

NÚKIB vydal v reakci na dění v průběhu pandemie několik doporučení, upozornění, varování i reaktivních opatření. Patří mezi ně například upozornění na rizika online konferenčních služeb, doporučení **Bezpečná práce na dálku**, příručka **Videokonference bezpečně** nebo dokument **Minimální bezpečnostní standard** pro zabezpečení menších organizací, které vznikly ve spolupráci s NAKIT.

Navzdory pandemickým opatřením proběhlo i v roce 2020 mezinárodní cvičení kybernetické bezpečnosti Cyber Coalition, pořádané Severoatlantickou aliancí, poprvé ve virtuální formě. Česká republika tak opět maximálně přispěla do jednoho z největších mezinárodních cvičení kybernetické bezpečnosti.

OBSAH

SEZNAM POUŽITÝCH ZKRATEK

AFCEA – Armed Forces Communications & Electronics Association
CERT – Computer Emergency Response Team
CyCLONe – Cyber Crisis Liaison Organisation Network
ČLR – Čínská lidová republika
ČR – Česká republika
DoS/DDoS – Denial of Service/Distributed Denial of Service
EU – Evropská unie
ISVS – Informační systém veřejné správy
MTU – Mezinárodní telekomunikační unie
KI – Kritická infrastruktura
KII – Kritická informační infrastruktura
KLDR – Korejská lidově demokratická republika
MŠMT – Ministerstvo školství, mládeže a tělovýchovy
MV – Ministerstvo vnitra
MZV – Ministerstvo zahraničních věcí
NAKIT – Národní agentura pro komunikační a informační technologie
NATO – North Atlantic Treaty Organization
NCKB – Národní centrum kybernetické bezpečnosti
NCKO – Národní centrum kybernetických operací
NIS – Network and Information Security
NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost
OBSE – Organizace pro bezpečnost a spolupráci v Evropě
OECD – Organisation for Economic Co-operation and Development
OSN – Organizace spojených národů
PZS – Provozovatel základní služby
SIEM – Security Information and Event Management
TAČR – Technologická agentura České republiky
VeKySIO – Velitelství kybernetických sil a informačních operací
VIS – Významný informační systém
VKB – Vyhláška kybernetické bezpečnosti
ZKB – Zákon o kybernetické bezpečnosti

2020: KYBERNETICKÁ BEZPEČNOST ČR V DATECH

468 ^
nahlášených kybernetických incidentů NÚKIB

99 ^
z nahlášených kybernetických incidentů řešeno NÚKIB

9 ^
velmi významných kybernetických incidentů řešených NÚKIB

1 267 ^
bezpečnostních incidentů řešených CSIRT.CZ – národním bezpečnostním týmem ČR

738 ^
řešených phishingových útoků CSIRT.CZ

8 073 v
trestných činů v oblasti kybernetické kriminality a kriminality páchané na internetu

100 v
účastníků cvičení kybernetické bezpečnosti uspořádaných NÚKIB

8 v
cvičení kybernetické bezpečnosti provedených NÚKIB

18 209 ^
proškolených zaměstnanců státní správy

120 ^
informačních a komunikačních systémů kritické informační infrastruktury

52 ^
subjektů kritické informační infrastruktury

85 ^
správců a provozovatelů významných informačních systémů

177 v
významných informačních systémů

56 ^
provozovatelů základní služby

61 ^
informačních systémů základní služby

O DOKUMENTU

NÚKIB na začátku roku 2021 rozeslal dotazník se 79 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. Dotazník vyplnilo celkem 222 subjektů, z toho 63 institucí z veřejného sektoru, 24 finančních institucí, 77 zdravotnických zařízení, 14 organizací poskytujících digitální služby, 12 subjektů z energetického sektoru, 12 subjektů z průmyslu a 20 vzdělávacích institucí. Z těchto dat NÚKIB čerpal informace pro potřeby Zprávy o stavu kybernetické bezpečnosti České republiky za rok 2020 (dále „ZSKB 2020"). Veškeré údaje z dotazníků jsou anonymizovány.

PROCES HODNOCENÍ

Hodnocení stavu kybernetické bezpečnosti v ČR je založeno na analytickém procesu, který zahrnuje vyhodnocení dat z vyplněných dotazníků, poznatky NÚKIB, informace poskytnuté od partnerů a další dostupné informace z otevřených zdrojů. NÚKIB neměl možnost data poskytnutá respondenty kontrolovat, ani hlouběji ověřovat uvedená tvrzení. Analytické závěry obsažené ve zprávě jsou založeny na premise, že odpovědi v dotaznících nejsou zkresleny. K vyjádření analytického hodnocení jsou použity pravděpodobnostní výrazy.

Zpráva o stavu kybernetické bezpečnosti ČR neposkytuje vyčerpávající seznam všech aktivit v oblasti kybernetické bezpečnosti. Účelem dokumentu je popsat a vyhodnotit hrozby v kybernetickém prostoru, se kterými se Česká republika v roce 2020 potýkala, stejně jako aktivity, které napomáhají jejich zmírnění.

PRAVDĚPODOBNOSTNÍ VÝRAZY POUŽITÉ VE ZPRÁVĚ O STAVU KYBERNETICKÉ BEZPEČNOSTI ZA ROK 2020

PRAVDĚPODOBNOSTNÍ VÝRAZY A VYJÁDŘENÍ JEJICH PROCENTUÁLNÍCH HODNOT:

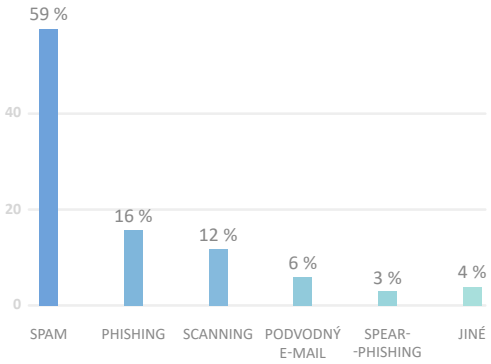
VÝRAZ	PRAVDĚPODOBNOST
Téměř jistě	90–100 %
Velmi pravděpodobně	75–85 %
Pravděpodobně	55–70 %
Nelze vyloučit/ Reálná možnost	25–50 %
Nepravděpodobně	15–20 %
Velmi nepravděpodobně	0–10 %

KYBERNETICKÁ BEZPEČNOST V ROCE 2020 POHLEDEM ČESKÝCH INSTITUCÍ, ORGANIZACÍ A FIREM[1]

INCIDENTY: NÁRŮST ZÁVAŽNOSTI CÍLENÉHO PHISHINGU A RANSOMWARU

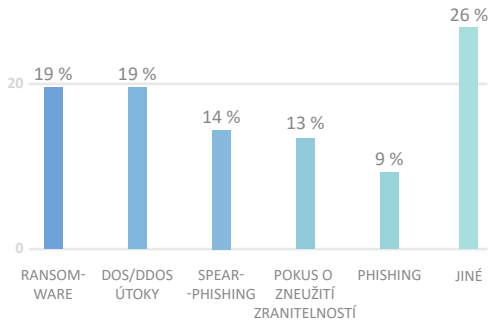
Mezi nejčastější typy útoků patřily v roce 2020 podle respondentů dotazníků spam, phishing a skenování vnějších sítí organizací[2] (Graf 1). Oproti tomu čelily dotazované instituce pouze v řádu jednotek např. sniffingu (skenování vnitřní sítě) nebo nelegální těžbě kryptoměn. Jako nejzávažnější útoky respondenti hodnotili ransomware, DoS/DDoS útoky, spear-phishingové e-maily a pokusy o zneužití zranitelností (Graf 2). Ačkoliv více než polovina respondentů uvedla, že detekovala alespoň jeden pokus o kybernetický útok, u téměř tří čtvrtin tento útok nevyústil v kybernetický bezpečnostní incident, tzn. nedošlo k narušení důvěrnosti, integrity nebo dostupnosti informací nebo služeb (Graf 3).[3] Největší počet incidentů detekovaly instituce veřejné správy a zdravotnická zařízení.

Graf 1: **Nejčastější** typy kybernetických útoků v roce 2020 (% respondentů)

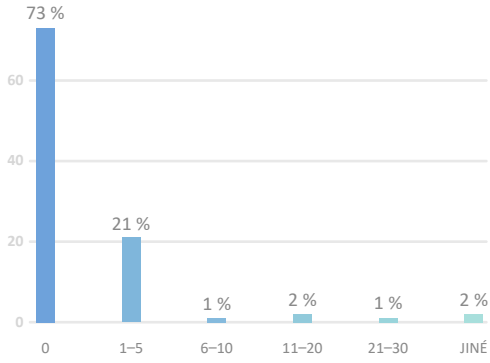


Skutečnost, že tak významný počet institucí nedetekoval kybernetický bezpečnostní incident nebo pokus o něj, ještě neznamená, že v jejich sítích ke kybernetickým incidentům nedochází. Zejména schopnost odhalit útoky mířící na integritu a důvěrnost dat vyžadují kapacity založené na pokročilých detekčních technologiích a dostatečně vyškoleném personálu, který je obsluhuje. Oproti tomu detekce útoků jako je spam, phishing nebo podvodný e-mail je výrazně snazší.

Graf 2: Kategorie **nejzávažnějších** typů kybernetických útoků v roce 2020 (% respondentů)



Graf 3: **Podíl incidentů, u kterých došlo k narušení důvěrnosti, integrity nebo dostupnosti informací** v roce 2020 (% respondentů)



1 Data plynou z vyhodnocení 222 dotazníků, viz část O dokumentu výše.

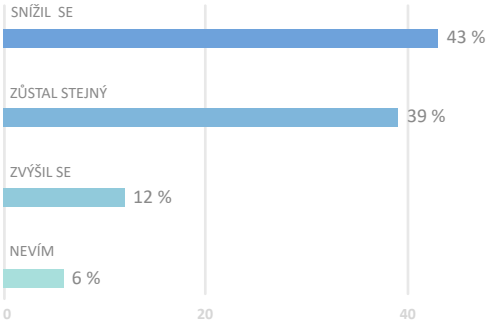
2 Skrze skenování vnějších sítí útočníci hledají zranitelnosti nebo chyby v zabezpečení, aby je mohli využít k infiltraci dané organizace.

3 Střední doba prodlevy od kompromitace k detekci kybernetického bezpečnostního incidentu je v Evropě 54 dnů, což ukazuje na velkou pravděpodobnost, že v řadě případů útočník odejde ze systému své oběti dříve, než jej oběť detekuje.[i]

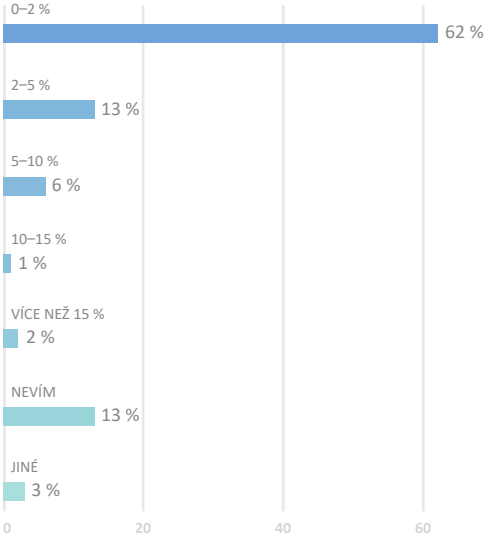
FINANCE: ZNAČNÝ PROPAD FINANČNÍCH PROSTŘEDKŮ NA KYBERNETICKOU BEZPEČNOST

Zatímco v roce 2019 většina respondentů uvedla, že se jejich rozpočet nezměnil nebo zvýšil, ve 43 % případů se za rok 2020 finance alokované pro oblast kybernetické bezpečnosti snížily (Graf 4). Oproti tomu zůstává podíl vynaložených nákladů na kybernetickou bezpečnost s rokem 2019 srovnatelný a u většiny respondentů se opět pohybuje v rozmezí 0–5 % na celkovém rozpočtu organizací (Graf 5). Tuto částku hodnotí stále více než polovina organizací jako nedostatečnou (Graf 6).

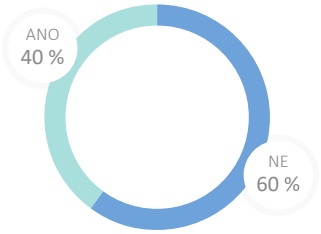
Graf 4: **Vývoj rozpočtů respondentů na kybernetickou bezpečnost** oproti roku 2019 (%)



Graf 5: **Podíl rozpočtu alokovaného na kybernetickou bezpečnost na celkovém rozpočtu organizací** v roce 2020 (% respondentů)



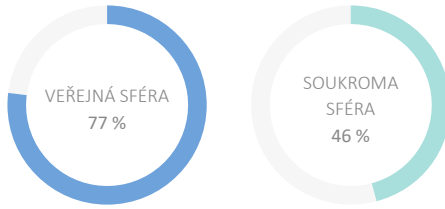
Graf 6: **Byly finance alokované na kybernetickou bezpečnost v roce 2020 podle respondentů dostatečné?** (%)



LIDÉ – ODBORNÍCI: ZKUŠENÍ PRACOVNÍCI ZŮSTÁVAJÍ, NOVÉ ODRAZUJÍ FINANČNÍ PODMÍNKY

V dotazníkovém šetření 68 % organizací uvedlo, že nízké finanční ohodnocení odradilo nové pracovníky v oblasti kybernetické bezpečnosti již při jejich náboru, a to zejména ve veřejném sektoru a v oblasti zdravotnictví. Nedostatek odborníků na kybernetickou bezpečnost představuje celosvětový problém. V důsledku vyšší poptávky jsou schopny vyšší mzdové náklady těchto odborníků zaplatit spíše organizace ze soukromého sektoru (Graf 7). U více než poloviny organizací zajišťují kybernetickou bezpečnost pracovníci s relevantní praxí v délce od 5 do 15 a více let (Graf 8). Za nejhůře obsaditelné role či služby v oblasti kybernetické bezpečnosti považují respondenti architekta kybernetické bezpečnosti a bezpečnostní dohled SIEM.[4] Pozitivním faktorem je, že jakmile pracovníci v oblasti kybernetické bezpečnosti místo získají, organizace se potýkají s jejich nízkou fluktuací. Odchod jednoho nebo dvou zaměstnanců zaznamenalo 10 % respondentů s tím, že v 74 % nebyla jeho hlavním důvodem výše finančního ohodnocení.

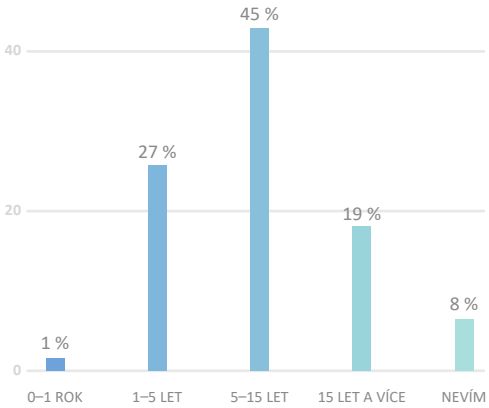
Graf 7: **Procentuální podíl organizací ze státního a soukromého sektoru, pro které byla v roce 2020 úroveň finančního ohodnocení zásadním faktorem odrazujícím uchazeče při náborech na místa v oblasti kybernetické bezpečnosti** (%)



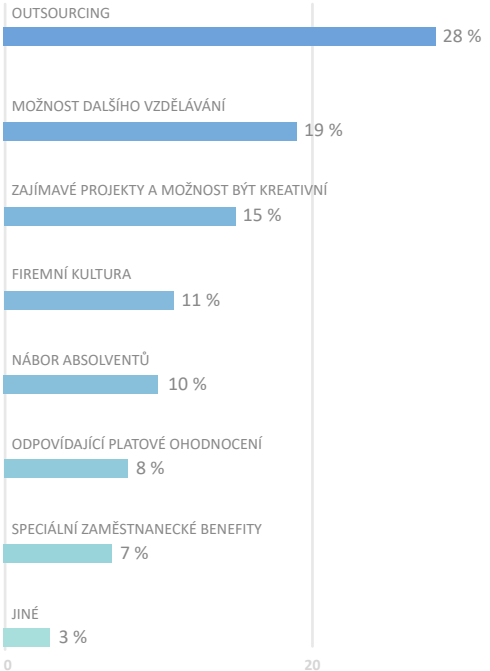
4 Role kybernetické bezpečnosti a jejich popis vychází z vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti.

Celých 38 % respondentů uvedlo, že v oblasti kybernetické bezpečnosti disponují dostatečnou právní expertizou. S nedostatkem pracovníků se organizace snaží vyrovnat nejčastěji skrze jejich outsourcing a k přilákání nových nabízejí benefity ve formě dalšího vzdělávání nebo účasti na zajímavých projektech (Graf 9).

Graf 8: **Jakou průměrnou relevantní praxi mají zaměstnanci zajišťující kybernetickou bezpečnost v organizacích respondentů?** (%)



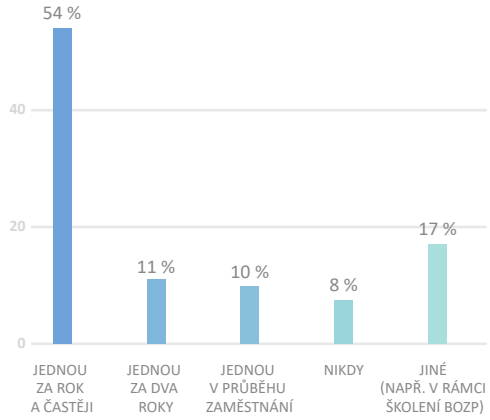
Graf 9: **Jak se organizace v roce 2020 snažily vypořádat s nedostatkem odborníků v oblasti kybernetické bezpečnosti?** (%)



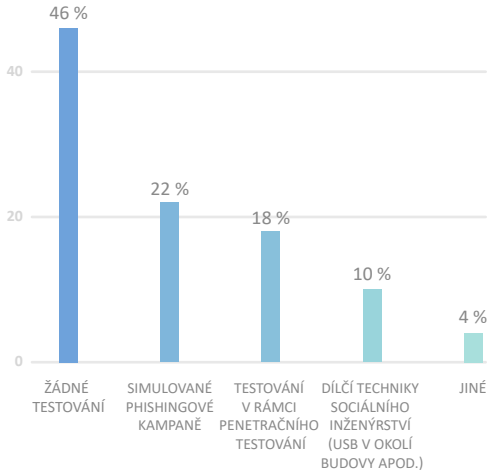
LIDÉ – UŽIVATELÉ: ZVYŠOVÁNÍ ODOLNOSTI ZAMĚSTNANCŮ, ALE ŠPATNÉ ZABEZPEČENÍ SOCIÁLNÍCH SÍTÍ

Kybernetickým útokům se 86 % organizací snažilo předcházet školením svých uživatelů. Ačkoliv celá polovina respondentů nealokuje finanční prostředky specificky na školení, u více než poloviny z nich proběhlo jednou za rok nebo častěji (Graf 10), a to ze tří čtvrtin v podobě e-learningu, nebo formou interních školení s pomocí vlastních zaměstnanců. Polovina organizací se zaměřila i na jiné formy zvyšování odolnosti svých zaměstnanců proti kybernetickým hrozbám. V téměř čtvrtině případů prováděla simulované phishingové kampaně nebo uživatele testovala v rámci penetračního testování (Graf 11).

Graf 10: **Frekvence školení uživatelů v oblasti kybernetické bezpečnosti v organizacích v roce 2020** (% respondentů)

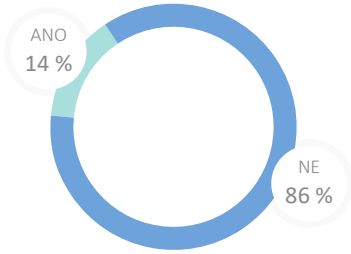


Graf 11: **Formy testování odolnosti zaměstnanců proti kybernetickým hrozbám v organizacích v roce 2020** (%)



Organizace se nezaměřují na ochranu svých sociálních sítí. Z dotazníkového šetření vyplynulo, že 68 % respondentů nepoužívá k jejich zabezpečení vícefaktorové ověření, přestože výrazně zvyšuje zabezpečení přístupu k digitálním platformám a při zneužití odcizeného účtu může dojít například k poškození reputace napadené instituce. Celých 86 % respondentů pak nemá zpracované postupy pro řešení případného zcizení účtů na sociálních sítích (Graf 12).

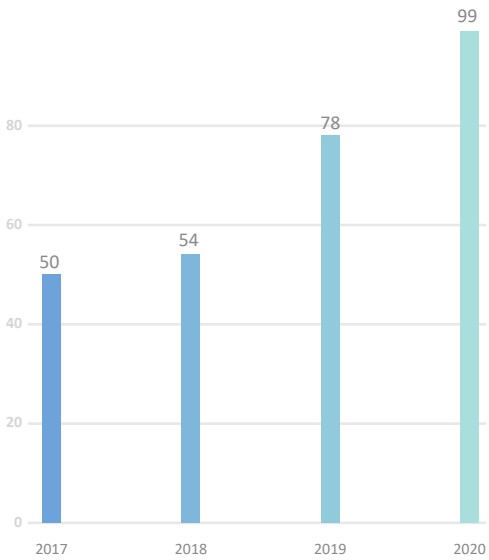
Graf 12: **V případě, že organizace používá ke komunikaci sociální sítě, disponuje zpracovanými postupy pro řešení případného zcizení účtů na těchto sociálních sítích?** (%)



KYBERNETICKÉ INCIDENTY POHLEDEM NÚKIB

NÚKIB v roce 2020 obdržel **468 hlášení o kybernetických bezpečnostních incidentech**, z nichž přímo řešil 99 incidentů (Graf 13). U zbývajících incidentů buď nebyl zásah NÚKIB potřebný, nebo jej řešila jiná příslušná instituce. Téměř třetinu z řešených incidentů nahlásily neregulované subjekty, což oproti roku 2019 představuje téměř desetinásobný nárůst, za kterým stojí velmi pravděpodobně (pravděpodobnost 75–85 %) vyšší počet kybernetických útoků i větší povědomí o existenci a aktivitách NÚKIB.

Graf 13: **Vývoj počtu kybernetických bezpečnostních incidentů řešených NÚKIB v letech 2017 – 2020: V roce 2020 NÚKIB řešil nejvíce incidentů za poslední čtyři roky a nárůst lze očekávat i v dalším roce**

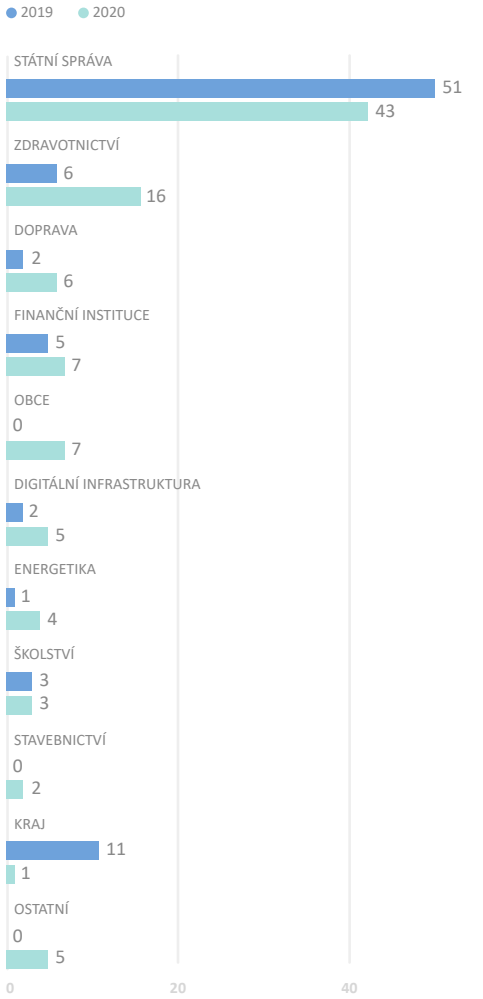


Během roku 2020 řešil NÚKIB nejvíce kybernetických incidentů v oblasti státní správy (Graf 14). Druhou nejčastěji řešenou oblastí byl sektor zdravotnictví, ve kterém počet meziročně stoupl o 267 %. Ve srovnání s rokem 2019 výrazně vzrostl i počet řešených incidentů hlášených jednotlivými obcemi. Tyto nárůsty jsou v souladu s globálními trendy.[ii]

267 %

meziroční nárůst incidentů v sektoru zdravotnictví

Graf 14: **Vývoj počtu kybernetických incidentů v letech 2019 a 2020 dle odvětví**



Nejvýznamnějším a nejzávažnějším incidentem řešeným NÚKIB bylo zašifrování systémů Fakultní nemocnice Brno ransomwarem, k němuž došlo v březnu 2020.[iii] Incident vyústil ve významné omezení provozu nemocnice na třech lokalitách a způsobil škody v řádu stovek milionů korun.[iv] Ve stejném měsíci se obětí ransomwaru stala Psychiatrická nemocnice Kosmonosy.[v] V tomto případě došlo k ochromení zejména její administrativní infrastruktury, ale nebyla ohrožena schopnost poskytování péče pacientům, ani nedošlo k zasažení systémů, na kterých závisejí lidské životy.[vi]

Třetím velmi významným incidentem[5] se v roce 2020 stala kompromitace několika desítek e-mailových účtů strategické státní instituce, ke které došlo v důsledku úspěšné spear-phishingové kampaně. Kromě narušení důvěrnosti obsahu schránek kompromitace vyústila v nedostupnost e-mailových služeb na jeden až dva dny.

Za více než třetinou všech řešených incidentů NÚKIB stály škodlivé kódy, z nichž téměř polovinu případů tvořil ransomware. Další téměř třetina incidentů vyústila v omezení dostupnosti služeb, systémů nebo webových portálů, ke kterému v polovině případů došlo v důsledku DDoS útoků.

KYBERNETICKÉ INCIDENTY V ROCE 2020 PODLE TYPU INCIDENTU

Popis kategorií vychází z formuláře pro hlášení incidentů:

37 **ŠKODLIVÝ KÓD (například virus, červ, trojský kůň, dialer, spyware)**

26 **DOSTUPNOST (například narušení dostupnosti způsobené DoS/DDoS útokem nebo sabotáží)**

16 **PRŮNIK (například úspěšná kompromitace aplikace nebo uživatelského účtu)**

7 **PODVOD/PHISHING (například e-mail se škodlivou přílohou nebo odkazem)**

7 **POKUS O PRŮNIK (například pokus o zneužití zranitelnosti, kompromitace aktiva, „zero day“ útok)**

3 **SBĚR INFORMACÍ (například skenování, sniffing, sociální inženýrství)**

1 **URÁŽLIVÝ OBSAH (například spam, kyberšikana, nevhodný obsah)**

2 **ADMINISTRATIVNÍ/TECHNICKÝ (bezpečnostní incident způsobený administrativní či technickou chybou)**

5 Hodnocení závažnosti incidentů vychází z vyhlášky č. 82/2018 Sb.

AKTÉŘI HROZEB V KYBERNETICKÉM PROSTORU

Aktivity státem podporovaných aktérů v kybernetickém prostoru a kybernetická kriminalita dlouhodobě patří mezi nejvážnější hrozby pro kybernetickou bezpečnost ČR. Vývoj v posledních letech naznačuje, že dochází k postupnému překryvu mezi aktivitou státních a vyspělých kyberkriminálních aktérů.[vii]

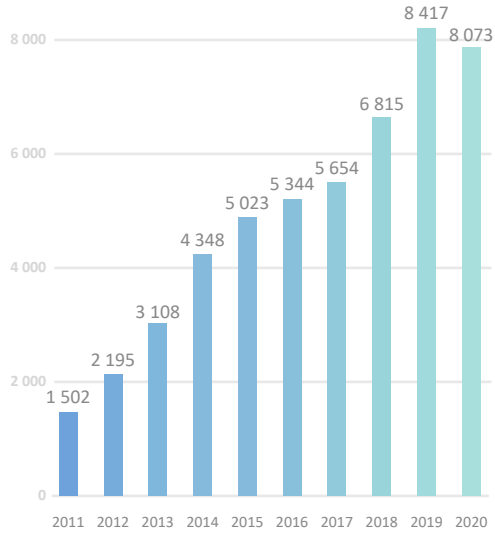
Evoluce kyberkriminální aktivity je nejlépe vidět na **vývoji ransomwarových útoků**. Ty v roce 2020 nejvíce zasáhly sektor zdravotnictví.[viii] V ČR byla aktivita kyberkriminálních skupin viditelná například při ransomwarových útocích na Fakultní nemocnici Brno nebo Psychiatrickou nemocnici Kosmonosy. Zatímco dříve byly vyděračské útoky nezacílenou činností s nízkými náklady zaměřenou na rychlý zisk, trend ransomwarové aktivity se v posledních letech nese ve znamení **zacílení na konkrétní instituce** spíše než na náhodnou masu individuálních uživatelů.[ix] Ransomwaroví operátoři si předem vyberou instituce, u nichž předpokládají největší pravděpodobnost zaplacení výkupného, a pokud se útočníkům podaří proniknout do jejich systémů, nepřistoupí ihned k zašifrování souborů. Místo toho se věnují průzkumu napadeného systému a k šifrování konkrétních dat dojde na základě zhodnocení jejich potenciální ceny pro napadenou oběť.[x] **Některé kyberkriminální skupiny tak podobně jako státní aktéři usilují o dlouhodobější nepozorovanou přítomnost (perzistenci).** Na tento vývoj má dopad i rozmach poskytování ransomwaru jako služby (tzv. Ransomware as a Service[6]).

Aktivita státních aktérů je široce zaměřená od získávání velkého množství osobních údajů až po průmyslovou a strategickou špionáž, ke které dochází i v ČR. NÚKIB v roce 2020 spolupracoval na řešení incidentu, při kterém byla narušena důvěrnost dat v sítích **strategické instituce státní správy**. Analýza indikátorů kompromitace ze strany NÚKIB ukázala, že útočníkem byl téměř jistě (pravděpodobnost 90–100 %) státní aktér.

Trendy ve špionáži naznačují, že některé státy velmi pravděpodobně (pravděpodobnost 75–85 %) stále častěji využívají kyberkriminální skupiny pro špionáž a jinou státem vyžadovanou činnost výměnou za toleranci jejich kriminální aktivity.

Ze statistik Policie ČR (Graf 15) vyplývá, že se kybernetická kriminalita a kriminalita páchaná na internetu oproti dřívějšímu rostoucímu trendu drží v posledních dvou letech na stejné úrovni. Mezi lety 2019 a 2020 došlo k 4,1% poklesu vyšetřovaných případů. Důvodem je legislativní změna trestního zákoníku,[7] která zvýšila hranice výše škody pro kvalifikaci trestného činu. Vzhledem k dlouhodobému trendu lze považovat nárůst kyberkriminality v ČR v dalších letech za pravděpodobný (pravděpodobnost 55–70 %).

Graf 15: **Počet vyšetřovaných kyberkriminálních případů v ČR v letech 2011 až 2020** (zdroj: Policie ČR)



6 Ransomware as a Service (RaaS) označuje službu, kterou poskytují vývojáři ransomwaru dalším hackerům, většinou za podíl z výkupného, a nestarají se o samotný průnik do systémů organizací.

7 Zákon č. 333/2020 Sb., který mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, a některé další zákony.

KYBERNETICKÉ HROZBY

RANSOMWARE: POKRAČUJÍCÍ TREND NÁRŮSTU SOFISTIKOVANÝCH VYDĚRAČSKÝCH ÚTOKŮ

V roce 2020 významně vzrostl celosvětový trend cílených vyděračských útoků na úkor plošných ransomwarových kampaní. V ČR získal v roce 2020 vyděračský malware největší pozornost v březnu, kdy došlo k zašifrování sítí Fakultní nemocnice Brno a Psychiatrické nemocnice Kosmonosy (více v kapitole Kybernetické incidenty pohledem NÚKIB). Hned následující měsíc proběhly útoky na Povodí Vltavy a na radnici městské části Prahy 3. Ačkoliv oba tyto incidenty proběhly ve stejný den, nebyla zjištěna jejich vzájemná souvislost.

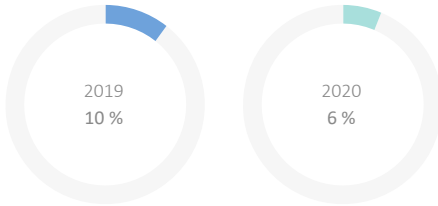
Při útoku na státní podnik Povodí Vltavy, který spadá pod Ministerstvo zemědělství, nedošlo k narušení prvků kritické informační infrastruktury a nebyl tak narušen provoz přehrad nebo dodávek pitné vody.[xi] Útok na radnici městské části Prahy 3 dočasně vyřadil provoz služeb systému CzechPoint na jejím území a způsobil nefunkčnost webu a několika dalších systémů.[xii] Mimo tyto incidenty se NÚKIB podílel na řešení dopadů ransomwarových útoků s největší četností ve veřejném sektoru, obzvláště na úrovni územních samospráv, v sektoru zdravotnictví, průmyslu, digitálních služeb a v oblasti vzdělávání. **Z počtu vyděračských útoků řešených NÚKIB i z dalších otevřených zdrojů vyplývá, že globální trend nárůstu ransomwarových útoků zasáhl v roce 2020 i ČR.**

V roce 2020 se s útokem ransomwaru nebo s pokusem o něj setkalo 28 % respondentů. Necelá pětina organizací, která se s ransomwarovým útokem nebo pokusem o něj setkala, jej hodnotí jako nejzávažnější, závažný nebo středně závažný typ útoku (Graf 16). Jde o relativně nízký počet respondentů, který může být dán tím, že ransomwarové útoky dvě třetiny organizací nedetekovaly a namísto nich se ve vyšších frekvencích potýkaly s jinými útoky, jež následně vyhodnotily jako více závažné. Ve srovnání s globálním rozmachem vyděračských útoků může být nižší četnost jejich záchytu v ČR zaviněná vyšší orientací operátorů ransomwaru na západní Evropu, Blízký východ a USA. V těchto oblastech existuje vyšší šance zaplacení výkupného mimo jiné z toho důvodu, že ve většině zemí mohou organizace využít finančních náhrad z pojištění proti vyděračským útokům. V ČR řada pojišťoven z pojistných podmínek vylučuje náhrady škod po ransomwarových útocích a platbu výkupného odmítá i z etických důvodů.

28 %

respondentů uvedlo, že v roce 2020 zaznamenali útok nebo pokus o útok ransomwarem

Graf 16: **Procentuální podíl respondentů, kteří hodnotili ransomwarové útoky jako nejzávažnější, v letech 2019 a 2020** (%)



I přesto lze mezi cíle útočníků zařadit instituce významné pro hladké fungování státu, jako jsou státní instituce, nemocnice nebo energetické, průmyslové a telekomunikační společnosti. Na ty budou útočníci velmi pravděpodobně (pravděpodobnost 75–85 %) i nadále zaměřovat svou pozornost kvůli vyšší šanci na zaplacení výkupného.

V oblasti ransomwaru pokračoval v roce 2020 kromě cílenějších útoků i globální trend hrozby odcizení citlivých dat a opětovného vydírání skrze jejich zveřejnění (tzv. dvojité vydírání). Podle informací, které má NÚKIB

k dispozici, se za rok 2020 obětí podobného útoku nestala žádná česká instituce, ale s ohledem na celosvětový vývoj existuje reálná možnost (pravděpodobnost 25–50 %), že tento trend v budoucnu zasáhne i ČR.

Ačkoliv při ransomwarovém útoku hrozí závažné dopady na chod instituce, NÚKIB napadeným subjektům doporučuje neplatit za dešifrování dat. Neexistuje záruka, že tak útočník skutečně učiní, a navíc může být získáním požadované částky povzbuzen k dalším útokům. Aby se napadené organizace vyhnuly nutnosti tuto variantu zvažovat, je velmi žádoucí udržovat segmentaci sítě, aktuální operační systém i aplikace nebo vytvářet offline zálohy alespoň kritických systémů nezbytných pro chod institucí. Z odpovědí respondentů vyplývá, že 56 % tyto offline zálohy vytváří a má zavedené procesy testování, 33 % disponuje offline zálohami, ale netestuje jejich obnovitelnost, a 7 % respondentů offline zálohy nevytváří vůbec.

Vzhledem k závažnosti a aktuálnosti problematiky ransomwaru vydal NÚKIB v roce 2020 analýzu shrnující základní fakta o tomto typu útoku, která popisuje základní zranitelnosti a dává doporučení, jak se proti podobným útokům chránit.

Analýza je dostupná na webu NÚKIB:
www.nukib.cz/cs/infoservis/aktuality

Podpůrný materiál Doporučení pro mitigaci, prevenci a reakci, na kterém NÚKIB spolupracoval se sdružením AFCEA a NAKIT, je dostupný na webových stránkách pod odkazem www.nukib.cz/download/publikace/podpurne_materialy

RANSOMWARE, DDOS ÚTOKY A SPEAR-PHISHING: TŘI NEJZÁVAŽNĚJŠÍ HROZBY ROKU 2020

Organizace jako nejzávažnější hrozby roku 2020 hodnotily ransomware a DDoS útoky (Graf 17). Ransomware za nejzávažnější útok označila téměř třetina respondentů ze sektoru zdravotnictví a 25 % respondentů z finančního i veřejného sektoru. Třetí nejzávažnější hrozbu představoval podle respondentů spear-phishing. V minulosti bylo možné phishingové útoky odhalit poměrně jednoduše skrze špatnou češtinu a odlišné domény v e-mailech. V posledních letech se však potvrzuje trend jejich vyšší propracovanosti v používání lepších formátů e-mailů i obsáhlého portfolia motivů útočníků od žádosti o zaplacení faktury po obnovení přihlašovacích údajů k účtu.

28 %

organizací ze sektoru zdravotnictví označilo ransomware za nejzávažnější hrozbu roku 2020

NÚKIB se v roce 2020 podílel na řešení dopadů phishingových a cílenějších spear-phishingových kampaní, které v rámci povinných osob nejčastěji mířily na veřejný sektor a v menší míře na sektor zdravotnictví. Útočníkům se nejčastěji podařilo své oběti přesvědčit k otevření souboru v příloze e-mailu s výzvou k zaplacení faktury. Po otevření souboru uživatel povolil makra a tím došlo k nákaze dalším malwarem.

53 %

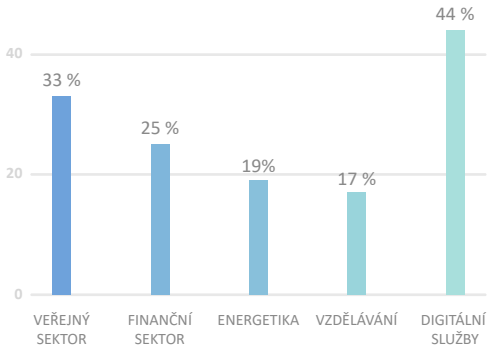
organizací uvedlo, že na ně byl v roce 2020 veden spear-phishingový útok nebo pokus o něj

DOPORUČENÍ NÚKIB PRO UŽIVATELE K OCHRANĚ PŘED ÚSPĚŠNÝMI SPEAR-PHISHINGOVÝMI ÚTOKY ZAHRNUJE:

- Nepovolovat makra v dokumentech MS Office
- Slepě neotevírat přílohy a odkazy v e-mailech
- Kontrolovat e-mailovou adresu v případě urgentních nebo neobvyklých požadavků
- V případě nejistoty nebo podezření kontaktovat odesílatele jinou cestou, následně kontaktovat IT oddělení
- Omezit sdílení informací o zaměstnání na sociálních sítích

Více o spear-phishingu a jak se před ním chránit naleznete na webových stránkách NÚKIB:
www.nukib.cz/cs/infoservis/doporuceni

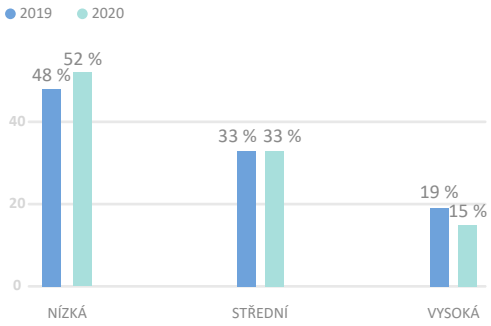
Graf 17: **Podíl DoS/DDoS útoků na útocích, které respondenti v jednotlivých sektorech označili za rok 2020 jako nejzávažnější** (% respondentů)



ÚTOKY NA DODAVATELSKÝ ŘETĚZEC: V ČR TÉMĚŘ NEZAZNAMENANÁ HROZBA S GLOBÁLNÍMI NÁSLEDKY

V roce 2020 zaznamenala útok nebo pokus o **útok na dodavatelský řetězec necelá 3 % organizací**, které jej zároveň z poloviny hodnotily jako hrozbu nejméně častou a nejméně závažnou. To je velmi pravděpodobně (pravděpodobnost 75–85 %) způsobeno nízkým výskytem tohoto typu útoku v ČR nebo nízkou schopností detekce ze strany organizací. **Hrozbu kybernetických útoků skrze dodavatele služeb vnímá více než polovina respondentů jako nízkou a meziročně navíc můžeme sledovat pokles závažnosti této hrozby ve vnímání respondentů** (Graf 18).

Graf 18: **Jak velká byla dle organizací hrozba kybernetických útoků ze strany dodavatele služeb, softwaru a hardwaru v letech 2019 a 2020?** (% respondentů)



V rozporu se stále slabším vnímáním hrozby útoku na dodavatelský řetězec v ČR bylo odhalení masivního útoku na americkou softwarovou společnost SolarWinds ke konci roku 2020. Ačkoliv doposud není celkový rozsah škod známý, odhady počítají s nízkými desítkami tisíc kompromitovaných[8] klientů po celém světě.[xiii] Dodavatelský řetězec útočníkům v kybernetickém prostoru umožňuje rozšířit jejich pole působnosti (tzv. attack surface) a získat tak přístup k násobně vyššímu množství citlivých dat organizací i jednotlivců najednou.

Útok na dodavatelský řetězec softwarové společnosti SolarWinds proběhl skrze infikování společností poskytované platformy Orion backdoorem[9] Sunburst, který útočníkům pomohl proniknout do systémů cílových společností. Mezi nimi se objevily např. kyberbezpečnostní firma FireEye, americká ministerstva financí, obrany nebo zahraničních věcí a společnosti Microsoft, Fujitsu nebo Lukoil.[xiv] **NÚKIB vzhledem k závažnosti situace vydal reaktivní opatření, přestože mu nebyl od osob regulovaných dle ZKB nahlášen žádný případ kompromitace.**

REAKTIVNÍ OPATŘENÍ VE VZTAHU K APLIKACÍM PLATFORMY ORION SPOLEČNOSTI SOLARWINDS

Poslední reaktivní opatření roku 2020 směřovalo k rizikům spojeným se softwarem americké společnosti SolarWinds. Správci systémů kritické informační infrastruktury, významných informačních systémů a systémů základní služby museli neprodleně provést bezpečnostní aktualizace, zkontrolovat, zda byl jejich systém kompromitován, a provést bezpečnostní audit.

Celý text reaktivního opatření naleznete webu NÚKIB: www.nukib.cz/cs/uredni-deska

Až 72 % respondentů řídí rizika spjatá s dodavateli nejčastěji na úrovni smluvních vztahů, což představuje jen jedno ze základních opatření.[10] Téměř tři čtvrtiny z nich udělují dodavatelům omezený vzdálený přístup pouze po souhlasu odpovědné osoby v organizaci a 8 % jim žádný vzdálený přístup neuděluje (Graf 19). Tyto výsledky dotazníkového šetření stojí proti nejčastějším zjištěním kontrolní činnosti NÚKIB, mezi které patří nedostatečné řízení rizik spojených s dodavateli. U organizací, které jsou zadavateli veřejných zakázek, je patrný trend využívání nejen kvantitativního

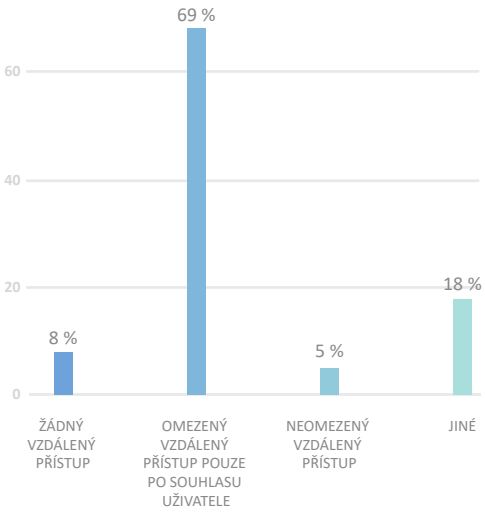
8 Klienti se staženou škodlivou aktualizací softwaru bez žádných dalších následků.

9 Backdoor (v českém překladu zadní vrátka) označuje název metody, kterou útočníci zneužívají pro vstup do systému bez vědomí uživatele.

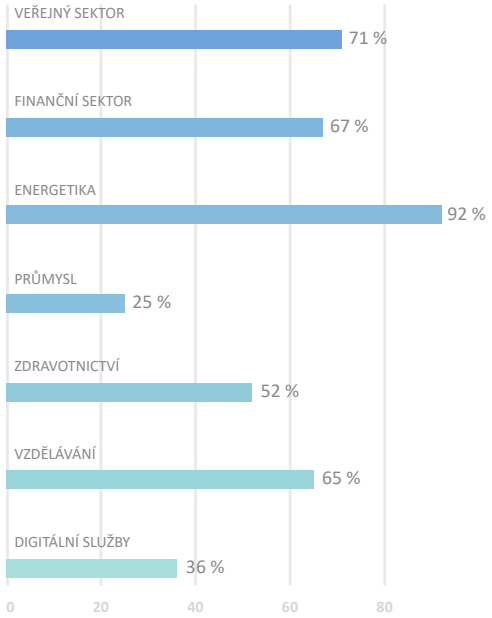
10 Globálně se stále více institucí obrací na bezpečnostní koncept nulové důvěry, tzv. **Zero Trust Security**, ve kterém mají organizace považovat za nedůvěryhodnou nejen vnější, ale i svou vnitřní síť, a před udělením přístupu musejí ověřit vždy všechna zařízení, která se pokoušejí připojit k jejich sítím či systémům. Uživatelé mají zároveň povolen přístup jen ke službám, které jim jsou explicitně přiděleny, a všechno ostatní mají blokováno. Koncept nulové důvěry lze využít nejen u mitigace rizik spojených s dodavateli, ale i k zabezpečení připojení a sítí při práci na dálku.

hlediska jako je cena, ale i kvalitativních kritérií. Ta v roce 2020 do hodnocení veřejné zakázky zahrnulo celkem 61 % respondentů, nejvíce z oblasti energetiky a veřejného sektoru (Graf 20).

Graf 19: **Jak rozsáhlý přístup do svých sítí udělují organizace svým dodavatelům?** (%)



Graf 20: **Rozdělení respondentů (dle sektoru), kteří pro hodnocení veřejné zakázky využívají i kvalitativní kritéria** (%)



CÍLE KYBERNETICKÝCH ÚTOKŮ

KRITICKÁ INFRASTRUKTURA: LEPŠÍ ÚROVEŇ ZABEZPEČENÍ A ŽÁDNÝ ZÁVAŽNÝ INCIDENT

Podle informací dostupných NÚKIB neproběhl v ČR v roce 2020 žádný sofistikovaný a cílený kybernetický útok, který by narušil informační systémy kritické infrastruktury (KI). Přesto byly subjekty kritické informační infrastruktury (KII) vystaveny až tisícům pokusů o kybernetický útok. K útokům na KII, na jejichž řešení se podílel NÚKIB, docházelo nejvíce skrze využití DDoS nebo pokusu o DDoS útok. Druhým nejčastějším typem útoku byly phishingové či spear-phishingové e-maily (Graf 21). Skutečnost, že sofistikovanější útoky nebyly v rámci KII zaznamenány, ani v tomto případě nepotvrzuje, že se takové útoky nedějí. Jejich detekce je totiž významně závislá na technických, procesních a personálních kapacitách zodpovědných subjektů. Stejně jako minulý rok vedla téměř polovina z odhalených kybernetických bezpečnostních incidentů k **omezení dostupnosti služeb**, které u subjektů KII představuje jedno z nejzásadnějších hledisek k zajištění hladkého fungování státu a společnosti. S bezpečnostními incidenty se z oblasti KII potýkaly zejména instituce státní správy.

47 %

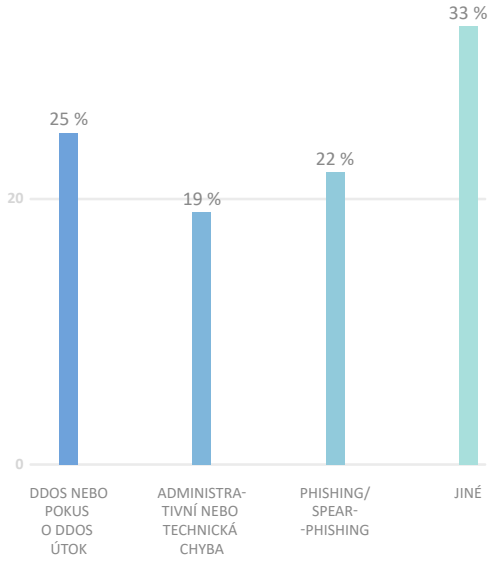
incidentů hlášených NÚKIB v oblasti KII v roce 2020 vyústilo v omezení dostupnosti služeb

Stejně jako v roce 2019 se třetina respondentů spadajících do KII vypořádala s nejzávažnějším útokem roku 2020 během několika hodin. V 5 % případů řešili respondenti jeho následky až rok. Z oblasti kritické infrastruktury se až 96 % organizací domnívá, že se oproti předchozím rokům jejich zabezpečení v oblasti kybernetické bezpečnosti zvýšilo (Graf 22). NÚKIB tento trend na základě informací, které má k dispozici, potvrdit nemůže. Nelze navíc vyloučit (pravděpodobnost 25–50 %), že významnou roli v odpovědích respondentů představuje pozitivní percepce dílčích kroků, ke kterým u mnohých organizací skutečně došlo, což ale nemusí znamenat, že se kybernetická bezpečnost subjektů KII objektivně zlepšila.

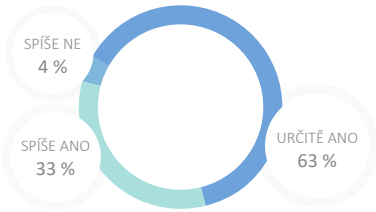
Kritickou informační infrastrukturou (KII) jsou dle ZKB komunikační a informační systémy prvků kritické infrastruktury (KI). KI samotná je dle zákona č. 240/2004 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů, definována jako prvek nebo systém prvků, jejichž 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 (dodávky elektřiny, tepla, vody nebo výplaty důchodů) nebo v krajním případě způsobit fyzické škody (například kybernetickou sabotáží).

Graf 21: **Které útoky na KII v roce 2020 vedly nejčastěji k vyústění v kybernetický bezpečnostní incident?** (% respondentů z KII)



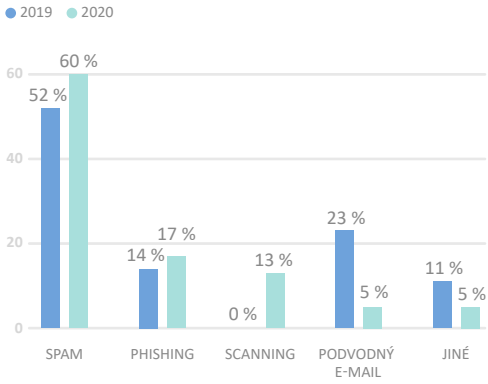
Graf 22: **Zlepšila se dle respondentů v oblasti KII úroveň kybernetické bezpečnosti v jejich organizaci oproti roku 2019?** (%)



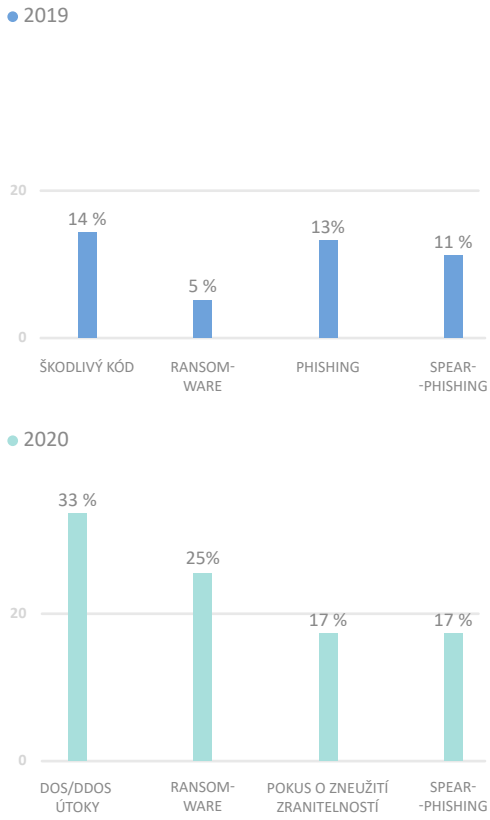
VEŘEJNÝ SEKTOR: CÍL DDOS ÚTOKŮ A PERSONALIZOVANÉHO PHISHINGU

V roce 2020 došlo k nárůstu četnosti útoků vedených proti institucím veřejného sektoru a k výrazné změně portfolia typů útoků z hlediska jejich závažnosti. Zvýšení počtu útoků zaměřených na státní správu a územní samosprávu, které vyplývá z odpovědí respondentů, koresponduje s daty dostupnými NÚKIB (více v kapitole Kybernetické incidenty pohledem NÚKIB). Zatímco se v roce 2019 zaměstnanci veřejného sektoru setkávali nejčastěji se spamem, phishingem a podvodnými e-maily, v roce 2020 tyto instituce zachytily nárůst útoků v podobě skenování jejich vnější sítě (Graf 23). Z hlediska závažnosti se u třetiny respondentů z veřejného sektoru dostaly na první místo DoS/DDoS útoky (Graf 24), stejně jako u čtyř dalších odvětví. To je dáno pravděpodobně (pravděpodobnost 55–70 %) vyšší četností zachycení tohoto typu útoků oproti jiným kybernetickým hrozbám. Na druhém místě se v hodnocení závažnosti hrozeb ve veřejném sektoru umístil ransomware, který jako nejzávažnější hrozbu roku 2020 hodnotila třetina respondentů ze sektoru zdravotnictví.

Graf 23: **Nejčastější útoky nebo pokusy o útoky vedené proti respondentům z veřejného sektoru** v letech 2019 a 2020 (%)



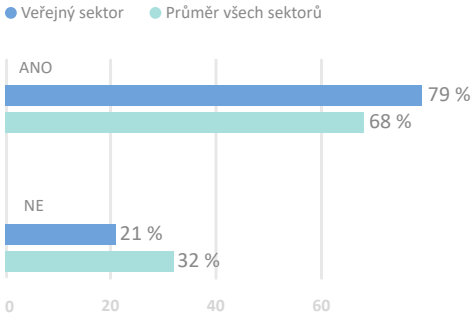
Graf 24: **Nejzávažnější útoky nebo pokusy o útoky vedené proti respondentům z veřejného sektoru** v letech 2019 a 2020 (%)



Stejně jako minulý rok organizace zaznamenaly **rostoucí trend sofistikovanějších útoků skrze phishingové, spear-phishingové a podvodné e-maily**, které jako návnadu kromě tématu pandemie využívaly podvodné informace o doručování zásilek nebo nedodržení splatnosti faktur. Útočníci nadále projevují lepší znalost prostředí i češtiny, což ztěžuje jejich detekci.

U institucí veřejného sektoru i v roce 2020 přetrvával **znatelný problém získat a zaplatit odborníky na kybernetickou bezpečnost**. Mimo to, že u téměř poloviny respondentů z veřejného sektoru došlo ke snížení rozpočtu na zajištění kybernetické bezpečnosti, téměř 80 % z nich uvedlo, že výše finančního ohodnocení je hlavním důvodem neobsazenosti míst v oblasti kybernetické bezpečnosti (Graf 25). Navzdory této situaci se k navýšení rozpočtu pro příští rok nechystá více než polovina respondentů. Kombinace těchto faktorů může mít v dalších letech velmi negativní dopad na úroveň kybernetické bezpečnosti v ČR.

Graf 25: **Byla v roce 2020 úroveň finančního ohodnocení zásadním faktorem, který uchazeče při náborech na místa v oblasti kybernetické bezpečnosti ve veřejném sektoru odrazoval?** (%)



ÚPRAVA VYUŽÍVÁNÍ CLOUD COMPUTINGU

Významným posunem při zajišťování kybernetické bezpečnosti veřejného sektoru se stala od srpna 2020 účinná novela zákona o informačních systémech veřejné správy, zavádějící pravidla pro ověření poskytovatelů cloud computingu a služeb cloud computingu, které využívají orgány veřejné správy. Během roku 2021 bude novela dále upravena a skrze prováděcí právní předpisy doplněna o bezpečnostní pravidla, která NÚKIB zpracovává formou vyhlášek.

FINANČNÍ SEKTOR: NEJVYŠŠÍ ROZPOČTY A ABSENCE VÁŽNĚJŠÍCH ÚTOKŮ

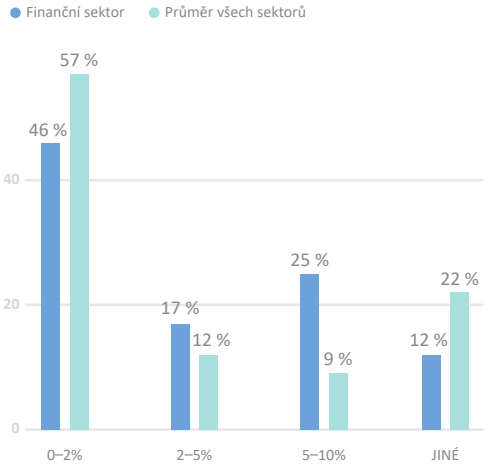
Tři čtvrtiny respondentů z finančního sektoru čelily v roce 2020 pokusům o kybernetický útok. V necelé třetině případů útoky vyústily v kybernetický incident pouze v řádu jednotek. Ačkoliv za nejzávažnější kybernetické incidenty označily finanční instituce cílený phishing, útoky DDoS a ransomware, stejně jako minulý rok přetrvává absence vážnějších incidentů a **český finanční sektor tak lze označit za zabezpečený na poměrně dobré úrovni**. Banky i pojišťovny se snaží kybernetickou bezpečnost nepodceňovat, protože kompromitace jejich informačních systémů by mohla mít dalekosáhlé finanční i reputační následky.

Finanční instituce investují do oblasti kybernetické bezpečnosti ve srovnání s ostatními sektory nejvyšší procento ze svého rozpočtu (Graf 26) a oproti jiným sektorům jako jediné uvedly, že při náborech na místa v oblasti kybernetické bezpečnosti nebyla úroveň finančního ohodnocení zásadním důvodem, který by uchazeče odrazoval. U více než poloviny dotazovaných finančních institucí nedošlo oproti roku 2019 ke snížení rozpočtu na kybernetickou bezpečnost a více než čtvrtina z nich jej naopak ještě zvýšila. Kromě odborníků na kybernetickou bezpečnost také všechny finanční instituce investují do vzdělávání svých zaměstnanců. Kromě využívání klasických metod testování některé organizace uvedly, že plánují zavedení interního Red Teamu.[11]

Klienti finančních institucí čelili v roce 2020 vishingovým útokům (spojení slov voice a phishing), kterými se z nich útočníci snažili vylákat finanční prostředky. Některé ze zasažených bankovních institucí vydaly na vishingovou kampaň upozornění, ve kterém uvedly průběh útoku.[xv] Útočníci klienty nejčastěji oslovili skrze telefonický hovor s tím, že došlo k napadení jejich účtu a pro ochranu prostředků jim doporučují, aby je převedli na jiné konkrétní číslo účtu. V některých případech se dožadovali přímo přístupových údajů k bankovnictví i přístupových kódů z SMS.

Trend vishingových kampaní narůstá i v zahraničí. Americké bezpečnostní služby vydaly v roce 2020 varování, ve kterém upozornily na vyšší četnost používání této metody v souvislosti s pandemií covid-19.[xvi]

Graf 26: **Jaké procento financí z celkového rozpočtu organizací ve finančním sektoru směřovalo v roce 2020 do nákladů na kybernetickou bezpečnost?** (%)



11 Red Team označuje tým etických hackerů, který provádí simulovaný útok s využitím stejně sofistikovaných prostředků jako reální útočníci.

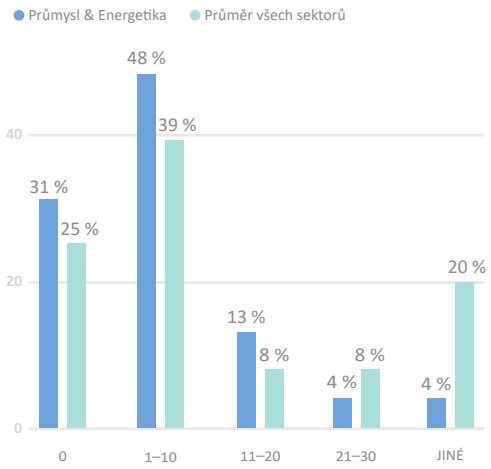
Celkem tři čtvrtiny institucí z finančního sektoru mají zavedeny procesy BCM (tzv. business continuity management), díky kterým organizace disponují systémem prevence a obnovy za účelem posouzení míry svého ohrožení a potažmo i svých klientů. Stejně jako minulý rok tak ze všech dotazovaných organizací investují finanční instituce do zajištění kybernetické bezpečnosti nejvíce.

PRŮMYSL & ENERGETIKA: CÍLE VYŠŠÍHO POČTU ÚTOKŮ S NÍZKÝMI DOPADY

Sektory průmyslu a energetiky se během roku 2020 setkaly s větším množstvím kybernetických útoků nebo pokusů o ně, než je průměr v ostatních sektorech (Graf 27). Pouhá 4 % z nich vyústila v kybernetický incident, s jehož dopady se instituce vypořádaly v téměř polovině případů buď ihned, nebo v řádu hodin. Téměř 90 % respondentů hodnotí zajištění kybernetické bezpečnosti svých organizací jako naprosto či spíše dostatečné oproti 70% průměru všech sektorů.

Až 92 % organizací z energetického sektoru i 58 % institucí z průmyslu mají v krizové komunikační směrnici uvedený kybernetický incident. Všechny ostatní sledované sektory jej mají obsažený průměrně pouze v polovině případů. Ačkoliv čtvrtina organizací hodnotí závažnost útoku skrze dodavatelský řetězec jako závažný, polovina respondentů jej zaznamenala jako nejméně častý. I přesto vnímají hrozbu kybernetických útoků na svou instituci skrze dodavatelský řetězec dvě třetiny respondentů jako střední či vysokou.

Graf 27: **Kolik pokusů o kybernetický útok detekovaly organizace ze sektorů průmyslu a energetiky v roce 2020?** (% respondentů)



Více než polovina organizací plánuje v následujícím roce zvýšit rozpočet na kybernetickou bezpečnost, ačkoliv 54 % respondentů považuje finance na zajištění kybernetické bezpečnosti svých organizací za dostatečné. Respondenti z energetického sektoru zároveň v 67 % uvedli, že disponují dostatečnou právní expertizou v oblasti kybernetické bezpečnosti, což představuje výrazně nadprůměrný výsledek v porovnání s ostatními sektory.

V nastavení procesů vytvářejí oba sektory shodně v 92 % offline zálohy kritických systémů včetně jejich testování a v necelé polovině mají respondenti z obou odvětví opět shodně zavedeny procesy BCM oproti 23% průměru ze všech sektorů.

ZDRAVOTNICTVÍ: LÁKAVÝ CÍL RANSOMWAROVÝCH ÚTOKŮ

České nemocnice a další zdravotnická zařízení byly v roce 2020 velmi atraktivním terčem ransomwarových útoků. Zaměření na tyto instituce lze do velké míry přisoudit probíhající pandemii spojené s nemocí covid-19. V důsledku pandemie je na zdravotnická zařízení vytvářen vysoký tlak na poskytování lékařské péče, a proto existuje vyšší šance, že útočníkům zaplatí požadované výkupné. NÚKIB se v roce 2020 v sektoru zdravotnictví podílel na řešení téměř dvaceti bezpečnostních incidentů, které byly nejčastěji spojeny s phishingovým nebo ransomwarovým útokem nebo zneužitím zranitelností v systémech. **Nejvýznamnější řešené případy se týkaly Fakultní nemocnice Brno a Psychiatrické nemocnice Kosmonosy** (více v kapitole Kybernetické incidenty pohledem NÚKIB).

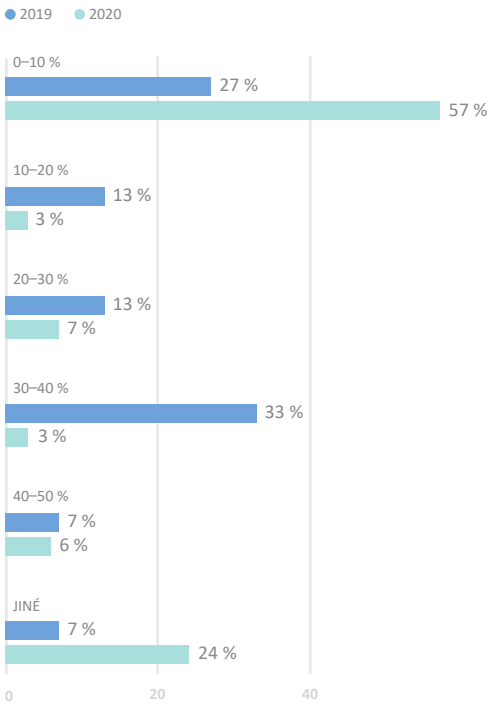
SPOJENÉ STÁTY AMERICKÉ VYJÁDŘILY ZNEPOKOJENÍ NAD ÚTOKY NA ZDRAVOTNICKÝ SEKTOR V ČR

V první polovině roku byly české nemocnice vystaveny vysoké hrozbě kybernetických útoků. České republice vyjádřil podporu při boji s pandemií i při zajišťování kybernetické bezpečnosti mj. tehdejší americký ministr zahraničí Michael Pompeo. Ten prohlásil, že USA jsou touto situací znepokojeny a kdokoliv, kdo se této činnosti účastní, musí být připraven, že ponese následky svých činů. Zároveň vyzval „ty, jichž se to týká, aby přestali s rušivou škodlivou aktivitou v kyberprostoru proti zdravotnímu systému v ČR a kdekoliv jinde.“ [xvii]

Téměř 90 % respondentů ze sektoru zdravotnictví se domnívá, že se úroveň kybernetické bezpečnosti v jejich organizaci zlepšila. Činnost NÚKIB v několika zdravotnických zařízeních v roce 2020 nicméně naznačuje, že je celková úroveň kybernetické bezpečnosti stále nedostatečná. **Tři čtvrtiny zařízení považují finance k zajištění kybernetické bezpečnosti za nedostatečné** stejně jako tomu bylo v předchozích letech. V roce 2019 by téměř polovina dotazovaných zdravotnických organizací rozpočet na kybernetickou bezpečnost navýšila o více než sto procent. V roce 2020 se pro vyšší než 50% nárůst vyslovila už jen třetina.

Úroveň finančního ohodnocení stejně jako v předchozích letech zůstává pro téměř tři čtvrtiny respondentů zásadním faktorem, který odrazuje uchazeče při náborech na místa v oblasti kybernetické bezpečnosti. **Ve srovnání s minulým rokem lze sledovat určitý pozitivní vývoj, kdy se procento neobsazených míst snížilo v téměř všech kategoriích** (Graf 28). Z odpovědí respondentů by tak bylo možné usuzovat, že se kybernetická bezpečnost pozvolně dostává do popředí rozpočtových priorit, ale ve většině případů mohli respondenti své rozpočty zvýšit jen díky 10. programové výzvě Integrovaného regionálního operačního programu EU Kybernetická bezpečnost.

Graf 28: **Neobsazená místa v oblasti kybernetické bezpečnosti v nemocnicích v letech 2019 a 2020** (%)



NOVELA VYHLÁŠKY O PROVOZOVATELÍCH ZÁKLADNÍCH SLUŽEB V OBLASTI ZDRAVOTNICTVÍ

V reakci na probíhající pandemii covid-19 a kybernetické útoky na nemocnice v ČR došlo v minulém roce k úpravě znění vyhlášky o provozovatelích základních služeb ve vztahu k sektoru zdravotnictví. Účelem této úpravy bylo zařazení většího počtu nemocnic mezi provozovatele základní služby a zajištění jejich lepšího regionálního rozložení k celorepublikovému pokrytí. Novela vyhlášky zohledňuje i specifičnost některých poskytovaných zdravotních služeb či kapacitu poskytovatelů zdravotních služeb, jejichž nahraditelnost by byla v případě výpadku z důvodu kybernetického incidentu obtížná, a zajišťuje návaznost na integrovaný systém záchranné služby. Novela nabyla účinnosti od 1. ledna 2021 a předpokládá, že by na základě nových kritérií mělo být v roce 2021 oproti původnímu počtu 16 nejvýznamnějších nemocnic regulováno přibližně 30 dalších nemocnic.

Celé znění novelizované vyhlášky můžete najít pod odkazem aplikace.mvcr.cz/sbirka-zakonu

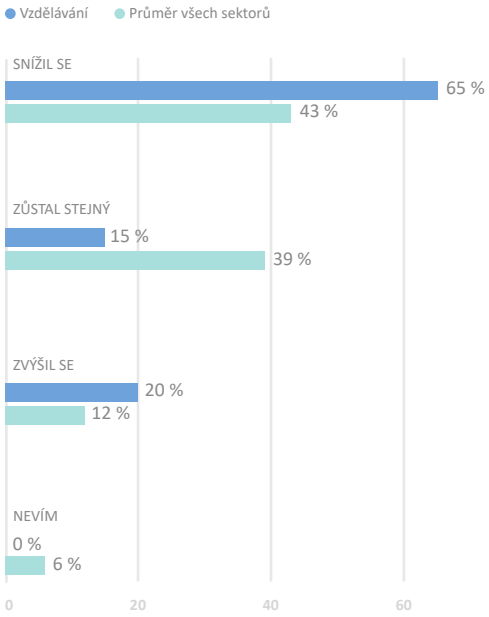
VZDĚLÁVÁNÍ: ROSTOUCÍ POČET KYBERNETICKÝCH ÚTOKŮ

Akademické instituce se v ČR stávají v posledních letech stále častějším cílem zejména ransomwarových útoků. Vysoké školy i univerzity v průběhu roku 2020 opakovaně varovaly před škodlivým jednáním v kybernetickém prostoru zaměřeným na své instituce. Vysoká škola ekonomická v Praze se potýkala s ransomwarovým útokem,[xviii] Masarykova univerzita v Brně zachytila nový malware zaměřený na své uživatele prostřednictvím zacílené phishingové kampaně,[xix] a Univerzita Palackého v Olomouci detekovala do té doby nezjištěnou formu ransomwaru, která po restartu počítače zašifrovala všechna data.[xx] **Nárůst útoků proti českým vzdělávacím institucím odpovídá celosvětovému trendu.**

Mezi nejzávažnější kybernetické incidenty v absolutním počtu označily vzdělávací instituce stejně jako minulý rok phishingové kampaně v různorodých podobách – od jednoduchých, plošně rozesílaných vyděračských e-mailů až po sofistikované a specificky cílené podvodné e-maily, v nichž se útočníci vydávali za zaměstnance univerzity. V čistě nejzávažnějších hrozbách umístila pětina respondentů na druhé místo útok ransomwarem.

Jedním ze způsobů, jak mohou instituce snižovat hrozbu úspěšného phishingového útoku, je školení svých zaměstnanců v oblasti kybernetické bezpečnosti. Ačkoliv tři čtvrtiny organizací nealokují finance specificky na školení uživatelů, přistupuje k němu přesně polovina respondentů. **Sektor vzdělávání byl nejvíce ze všech sektorů postižen snížením rozpočtů, ke kterému došlo u 65 % respondentů** (Graf 29). K navýšení rozpočtu alespoň o 50 % se vyslovila více než pětina vzdělávacích institucí.

Graf 29: **Jak se změnil rozpočet organizací alokovaný na kybernetickou bezpečnost na rok 2020 oproti roku 2019** (%)



Pro minimalizaci hrozby úspěšného kybernetického útoku na vzdělávací instituci je v první řadě velmi žádoucí provést identifikaci používaných informačních systémů. Od 1. ledna 2021 nabyla účinnosti novelizovaná vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, pod kterou mohou spadat i informační systémy vysokých škol a univerzit.

Více informací naleznete mezi podpůrnými materiály NÚKIB jako Průvodce identifikací VIS na jeho webových stránkách:
www.nukib.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy

DIGITÁLNÍ SLUŽBY: DOSTATEČNÉ FINANCE I PRÁVNÍ EXPERTIZA

České instituce poskytující digitální služby (telekomunikace, digitální infrastrukturu, internetové služby apod.) mají v nadpoloviční většině v rámci procesů krizového managementu zahrnutý krizový scénář řešení kybernetického incidentu. V roce 2020 se téměř polovina respondentů potýkala s jedním až pěti kybernetickými incidenty (Graf 30), z nichž za nejzávažnější považovala pětina organizací DoS/DDoS útoky.

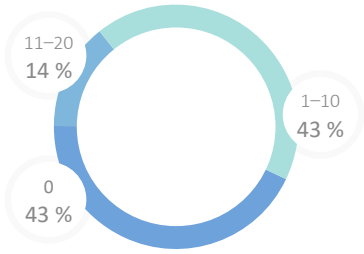
50 %

organizací neuděluje svým dodavatelům žádný přístup do svých sítí

Přesně polovina z respondentů neuděluje svým dodavatelům žádný vzdálený přístup do svých sítí a polovina pouze v omezeném rozsahu po souhlasu uživatele. Pravděpodobně proto hodnotí 57 % respondentů hrozbu kybernetických útoků skrze dodavatelský řetězec jako nízkou či velmi nízkou.

Instituce v sektoru digitálních služeb vynaložily v roce 2020 na náklady do oblasti kybernetické bezpečnosti ve třetině případů od 5 do více než 15 % svého celkového rozpočtu, což je srovnatelná výše jen s finančním sektorem. Tuto částku považují necelé tři čtvrtiny respondentů za dostatečnou a třetina plánuje rozpočet na kybernetickou bezpečnost v příštím roce zvýšit, což odpovídá průměru odpovědí respondentů ze všech sektorů. Instituce digitálních služeb stejně jako sektory průmyslu a energetiky disponují právní expertizou na úrovni vyšší, než představuje průměr všech respondentů.

Graf 30: **Kolik z pokusů o kybernetický útok vyústilo dle respondentů v sektoru digitálních služeb v kybernetický incident, tzn. došlo k narušení důvěrnosti, integrity nebo dostupnosti informací?** (%)



OPATŘENÍ

ČASOVÁ OSA AKTIVIT NÚKIB V BOJI S PANDEMIÍ COVID-19

BŘEZEN

REAKTIVNÍ OPATŘENÍ PRO VYBRANÉ SUBJEKTY VE ZDRAVOTNICTVÍ

Reaktivním opatřením NÚKIB **uložil** vybraným subjektům v oblasti zdravotnictví spadajících pod ZKB provést nezbytné úkony, které vedly k zabezpečení důležitých informačních a komunikačních systémů před kybernetickým bezpečnostním incidentem. V souvislosti s reaktivním opatřením bylo vydáno doporučení, jež NÚKIB zaslal páteřním nemocnicím určeným Ministerstvem zdravotnictví.

KVĚTEN

DOPORUČENÍ PRO BEZPEČNOU PRÁCI NA DÁLKU

Tipy a doporučení pro bezpečnou práci na dálku pro firmy i zaměstnance NÚKIB **publikoval** ve formě krátkého letáku ve spolupráci s dalšími partnery.

ŘÍJEN

UPOZORNĚNÍ NA PODVODNÉ E-MAILY VYDÁVAJÍCÍ SE ZA VÝSLEDKY TESTŮ NA COVID-19

NÚKIB upozornil na hrozbu **podvodných** e-mailů, ve kterých neznámí útočníci rozesílali falešné výsledky testování a odkaz na soubor ke stažení škodlivého kódu, který by útočníkům umožnil přístup do zařízení příjemce e-mailu.

DUBEN

VAROVÁNÍ PŘED HROZBOU KYBERNETICKÝCH ÚTOKŮ NA NEMOCNICE A JINÉ VÝZNAMNÉ CÍLE ČR

Měsíc po vydání reaktivního opatření vydal NÚKIB **varování** před hrozbou v oblasti kybernetické bezpečnosti, spočívající v realizaci rozsáhlé kampaně závažných kybernetických útoků na informační a komunikační systémy v ČR, zejména pak na systémy zdravotnických zařízení. K varování NÚKIB vydal doporučení, které se zaměřovalo na technické a organizační otázky a konkretizovalo postupy definované ve varování.

UPOZORNĚNÍ NA RIZIKA ONLINE KONFERENČNÍCH SLUŽEB

Vzhledem ke zvýšení potřeby online komunikace NÚKIB **upozornil** na rizika spojená s používáním audio a video komunikačních služeb, zejména pak upozornil na zranitelnosti služby Zoom, která se stávala častým cílem útoků.

ČERVENEC

VYDÁNÍ DOKUMENTU MINIMÁLNÍ BEZPEČNOSTNÍ STANDARD PRO ZABEZPEČENÍ MENŠÍCH ORGANIZACÍ

NÚKIB ve spolupráci s NAKIT a MV ČR připravil **dokument** s cílem pomoci s kybernetickou bezpečností organizacím, které nespadají pod ZKB, typicky obecním úřadům, zdravotnickým zařízením nebo školám či soukromým firmám.

PŘÍRUČKA VIDEOKONFERENCE BEZPEČNĚ

Příručka vydaná ve spolupráci s NAKIT obsahuje základní bezpečnostní doporučení a tipy pro bezpečné používání videokonferencí.

NÁRODNÍ STRATEGIE KYBERNETICKÉ BEZPEČNOSTI: DŮLEŽITÝ MILNÍK ROKU 2020

V listopadu 2020 byla vládou České republiky schválena Národní strategie kybernetické bezpečnosti pro následujících pět let, jejímž autorem je NÚKIB. Dokument popisuje hlavní principy, na kterých stojí kybernetická bezpečnost ČR, definuje její budoucí strategické směřování v oblasti kybernetické bezpečnosti a popisuje základní vize v této čím dál důležitější oblasti.

Dokument je rozdělen do tří hlavních pilířů. Každý z nich bude naplňován skrze své strategické cíle.

1. **SEBEVĚDOMĚ V KYBERPROSTORU:** Vzhledem k faktu, že v posledních letech narůstá riziko ohrožení ČR prostřednictvím kyberprostoru, musí ČR reagovat na celé spektrum nových výzev. Sebevědomým a zodpovědným přístupem ke kybernetické bezpečnosti by na národní úrovni měla ČR posilovat svou prosperitu a navíc bude i nadále silným spojencem pro své partnery na mezinárodní úrovni.

2. **SILNÁ A SPOLEHLIVÁ SPOJENECTVÍ:** Stěžejní vizi pro ČR, jakožto moderní evropskou zemi, představuje aktivní role při vytváření dialogu v mezinárodním prostředí, zejména v euroatlantickém prostoru. ČR bude vycházet z koherentních národních pozic a jasně definovaných strategických zájmů. Na tomto základě bude i nadále vytvářet a prohlubovat silná spojenectví se svými partnery v oblasti kybernetické bezpečnosti a obrany.

3. **ODOLNÁ SPOLEČNOST 4.0:** V oblasti rozšíření a využívání moderních technologií patří ČR mezi špičku v Evropě. Česká společnost se díky tomu úspěšně proměňuje ve společnost informační. Nastavený trend však s sebou přináší nejenom nárůst počtu koncových uživatelů v české společnosti, ale i hrozeb, kterým jsou tito uživatelé vystaveni. Jako problém s tím spojený lze identifikovat nedostatečnou digitální hygienu, nedostatečnou mediální gramotnost a kritické myšlení napříč celou společností. ČR se proto musí zaměřit na úspěšnou proměnu české společnosti na tzv. společnost 4.0. Stav, kdy je celá společnost schopna naplno využívat výhod moderních technologií a současně je schopna integrovat je do svého každodenního života tak, aby byla minimalizována bezpečnostní rizika. Kybernetická bezpečnost se proto musí stát nedílnou součástí běžného života občanů.

Národní strategie kybernetické bezpečnosti ČR je ve své podrobnější povaze převedena do konkrétních úkolů v rámci Akčního plánu. Oba dokumenty jsou tvořeny v koordinaci s relevantními subjekty zodpovědnými v podstatných oblastech kybernetické bezpečnosti pro plnění jednotlivých úkolů. NÚKIB bude průběžně sledovat, diskutovat, hodnotit a koordinovat plnění jednotlivých cílů.

Národní strategii kybernetické bezpečnosti lze nalézt na webových stránkách NÚKIB: www.nukib.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan

V roce 2020 byla schválena i Koncepce rozvoje NÚKIB. Ta popisuje kompletní rozsah činností, které NÚKIB v současné době zajišťuje, hodnotí současný stav a zároveň popisuje a zdůvodňuje potřeby budoucího rozvoje úřadu v kontextu vývoje bezpečnostního prostředí, a zejména vývoje hrozeb v kyberprostoru.

Celý dokument ke koncepci rozvoje NÚKIB je k dispozici na webových stránkách pod odkazem www.nukib.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan

LEGISLATIVNÍ UKOTVENÍ: NASTAVENÍ ZÁKLADNÍCH PRAVIDEL PRO VÝZNAMNÉ SUBJEKTY[12]

NOVELA VYHLÁŠKY O VÝZNAMNÝCH INFORMAČNÍCH SYSTÉMECH

NÚKIB během minulého roku pracoval na novele vyhlášky o významných informačních systémech, jejímž cílem bylo zejména zjednodušit a zpřehlednit proces identifikace těchto systémů a skrze její vyšší efektivnost posílit i právní jistotu jejích adresátů. Novela vyhlášky vstoupila v platnost v září 2020 a postupné účinnosti nabývá od 1. ledna 2021. Z důvodu nákladů, které bude nutné vynaložit na zabezpečení nově identifikovaných systémů, došlo k rozložení účinnosti seznamu typových systémů do tří let.

12 Z hlediska zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů, se jedná o subjekty, jejichž informační systémy jsou důležité pro fungování státu.

ODHADOVANÝ NÁRŮST POČTU VÝZNAMNÝCH INFORMAČNÍCH SYSTÉMŮ V DŮSLEDKU NOVELY VYHLÁŠKY O VÝZNAMNÝCH INFORMAČNÍCH SYSTÉMECH

OBDOBÍ	POČET NOVĚ ZAŘAZENÝCH SYSTÉMŮ
Rok 2021	360
Rok 2022	260
Rok 2023	80
Celkem	700

OPRAVY A DOPLNĚNÍ ZÁKONNÝCH USTANOVENÍ

Na počátku roku 2020 došlo k novelizaci ZKB v oblasti změn ustanovení o přestupcích a pokutách, které z nich plynou. Byl tak napraven stav přetrvávající od roku 2017, kdy se nevhodnou novelizací zákona některé přestupky překrývaly a za některé naopak chyběly jakékoliv možnosti udělení pokuty.

POČET URČENÝCH SUBJEKTŮ KE KONCI ROKU 2020:

52 subjektů: správci a provozovatelé informačních a komunikačních systémů kritické informační infrastruktury

120 informačních a komunikačních systémů kritické informační infrastruktury

85 subjektů: správci a provozovatelé významných informačních systémů

177 významných informačních systémů

56 subjektů: správci a provozovatelé informačních systémů základní služby

61 informačních systémů základní služby

DOZOROVÁ ČINNOST NÚKIB V ROCE 2020

Z pohledu kontrolní a auditní činnosti byl rok 2020 negativně ovlivněn pandemií, která měla dopad na nižší počet provedených kontrol a auditů. V roce 2019 bylo provedeno 15 kontrol podle ZKB, zatímco za rok 2020 NÚKIB provedl **8 kontrol či auditů** dle ZKB, respektive vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti (dále „VKB"). Kontrola či audit u povinných orgánů a osob dle ZKB ověřuje plnění povinností plynoucích ze ZKB a VKB. V rámci každé kontroly nebo auditu je ověřováno rámcově 150 kontrolních bodů. **V oblasti kontroly a auditu byl pro NÚKIB zejména ve druhé polovině roku 2020 prioritou sektor zdravotnictví.**

V PRŮBĚHU KONTROLNÍ A AUDITNÍ ČINNOSTI JSOU NEJČASTĚJI IDENTIFIKOVÁNY NEDOSTATKY V TĚCHTO OBLASTECH:

- nedostatek odborníků na kybernetickou bezpečnost
- nastavený systém zajišťování kybernetické bezpečnosti nepokrývá požadavky všech zainteresovaných stran
- nevhodná segmentace sítě
- subjekty nedostatečně řídí aktiva a rizika spojená s kybernetickou bezpečností
- nedostatečný monitoring interní sítě
- bezpečnostní politiky a bezpečnostní dokumentace se často neaplikují v praxi nebo jsou neaktuální
- příliš krátká doba uchovávání log záznamů
- subjekty nedostatečně řídí rizika spojená s dodavateli
- nefunkční systém zajišťování kontinuity činností
- používání zastaralého hardwaru a softwaru, který již jeho výrobce nepodporuje

SPOLUPRÁCE NÚKIB S DALŠÍMI DOZOROVÝMI ORGÁNY V OBLASTI KONTROLY ZA ROK 2020

I v uplynulém roce NÚKIB rozvíjel spolupráci v kontrolní činnosti s dalšími regulátory, jejímž cílem je především snaha minimalizovat zátěž povinných orgánů a osob. Spolupráci NÚKIB navázal například se Státním úřadem pro jadernou bezpečnost skrze memorandum, čímž tyto instituce vzájemně stvrdily oboustrannou podporu a spolupráci nad rámec kontrolní činnosti.

CVIČENÍ KYBERNETICKÉ BEZPEČNOSTI: VELKÝ ZÁJEM, ALE OMEZENÉ MOŽNOSTI

Stejně jako v předchozích letech, tak i v roce 2020 NÚKIB zaznamenal ze strany organizací působících v ČR zvýšenou poptávku po cvičeních. Tato poptávka však nemohla být zcela uspokojena z důvodu **opatření v kontextu krize spojené s celosvětovou pandemií covid-19**. Celkový počet uspořádaných cvičení, jako osvědčeného nástroje pro zvyšování úrovně kybernetické bezpečnosti, negativně poznamenala především nemožnost fyzicky se setkávat a interaktivním způsobem diskutovat otázky představené realistickým scénářem, připraveným na míru konkrétnímu publiku. Omezení k setkávání bylo jak na straně NÚKIB, tak i na straně poptávajících subjektů, které na jednu stranu logicky kladly důraz na **bezpečnost svých zaměstnanců** a na druhou stranu v důsledku krize prioritizovaly i jiné své kritické činnosti.

Navzdory tomu NÚKIB v roce 2020 pořádal či koordinoval **osm národních a mezinárodních cvičení**. V rámci ČR se jich nad rámec zástupců z NÚKIB **aktivně zúčastnilo na 100 účastníků z různých organizací**. Z těchto cvičení lze, mimo níže zmíněné, vyzdvihnout cvičení v rámci Kurzu Generálního štábu či cvičení pro Správu Pražského hradu.

PŘIDANÁ HODNOTA CVIČENÍ KYBERNETICKÉ BEZPEČNOSTI

Cvičení jsou neocenitelným zdrojem nových znalostí, zkušeností a technických schopností. Dávají NÚKIB možnost identifikovat a poukázat na slabá místa v oblasti kybernetické bezpečnosti a představují výborný nástroj pro ověřování i revizi politik a procesů. Jako prostředek pro identifikaci, definici či potvrzení konkrétních trendů dále poskytují vstupy pro přípravu dalších osvětových či edukativních aktivit. Díky cvičením dochází rovněž k prohlubování vztahů mezi účastníky cvičení navzájem, ale i s partnery spolupracujícími s NÚKIB na jejich přípravě.

MEZINÁRODNÍ CVIČENÍ KYBERNETICKÉ BEZPEČNOSTI CYBER COALITION 2020

Pravidelné mezinárodní cvičení pořádané Severoatlantickou aliancí, které je na úrovni ČR koordinováno NÚKIB za civilní část a Velitelstvím kybernetických sil a informačních operací (VeKySIO) za vojenskou část, zaznamenalo oproti předchozím ročníkům kvůli pandemii covid-19 výraznou změnu. Účast koordinujících organizací včetně jejich partnerů byla značně omezena a plánovací proces i samotné cvičení se transformovaly do virtuální formy. I přes nutné přizpůsobení k současné situaci se již třetím rokem v řadě podařilo aktivně zapojit zástupce NÚKIB do užšího plánovacího týmu cvičení, který má na starosti přípravu a organizaci cvičení na nejvyšší úrovni. **Česká republika tak opět maximálně přispěla do jednoho z největších mezinárodních cvičení kybernetické bezpečnosti.**

CYBER COALITION 2020 V ČÍSLECH

13.
ročník světově

10.
ročník pro ČR

1 000
účastníků

29
zemí

JAKÉ OBLASTI PROCVIČUJÍ ÚČASTNÍCI V RÁMCI CYBER COALITION?

- Procesy
- Technické úkoly
- Komunikace
- Právní aspekty

KOMUNIKAČNÍ CVIČENÍ COMM CZECH 2020

Cílem v pořadí již třetího komunikačního cvičení uspořádaného NÚKIB bylo prověřit dostupnost a aktuálnost kontaktních údajů uvedených povinnými subjekty dle ZKB, které jsou důležité pro vládní GovCERT.CZ zejména z hlediska potřeby **náhlé krizové komunikace v rámci řešení kybernetického bezpečnostního incidentu**. Metrikou byla dostupnost kontaktních údajů nahlášených u konkrétních systémů spadajících do prvků KII, VIS či PZS. V reálné situaci by případná nedostupnost

a nemožnost včasné komunikace mohla přinést vážnou újmu nejen danému subjektu, ale v krajním případě celé ČR. Výsledky cvičení byly hodnoceny velmi pozitivně, jelikož převážná většina údajů, respektive systémů, byla dostupná. Cvičení rovněž ověřilo a potvrdilo, že **subjekty již nyní s vládním GovCERT.CZ intenzivně komunikují i v případech prevence**.

VÝZNAMNÉ POZNATKY ZE CVIČENÍ V POSLEDNÍCH LETECH:

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.

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.

OSVĚTA A VZDĚLÁVÁNÍ V ČR: ONLINE ROK 2020

V roce 2020 se potvrdilo, že průběžné a kvalitní vzdělávání v tématech kybernetické bezpečnosti je více než důležité a je nutné mu věnovat patřičný prostor. Epidemiologické okolnosti donutily řadu každodenních činností přestěhovat se do online prostředí a pojmy jako homeoffice či distanční výuka se staly běžnou součástí našeho slovníku. To otevíralo nejen řadu příležitostí, ale i hrozeb, na které bylo třeba různé cílové skupiny uživatelů připravovat.

Vzdělávání uživatelů z **veřejné správy** probíhalo skrze online kurz NÚKIB **Dávej kyber!**, který představuje základy kybernetické bezpečnosti.

KURZ DÁVEJ KYBER! ABSOLVOVALO:

18 209 zaměstnanců státní správy

214 pracovníků Armády ČR

2 000 pracovníků FN Na Bulovce

V rámci osvětových a vzdělávacích aktivit se pro děti v mateřských školách až po studenty vysokých škol a jejich pracovníky podařilo zrealizovat mj. následující projekty:

V rámci odborného vzdělávání s preventivním přesahem absolvovalo **1 690 pracovníků prevence** odborný online kurz **Bezpečně v kyber** připravený NÚKIB ve spolupráci s MŠMT a Zvolsi.info, který je seznamuje s tématy online bezpečnosti a situacemi, se kterými se lze setkat ve školním prostředí.

Ve spolupráci se Svazem knihovníků a informačních pracovníků ČR se NÚKIB podařilo distribuovat naučné deskové hry pro mateřské školy **Městečko Kybernetov**, které dětem nenásilnou formou představují mj. problémy kyberšikany.

Pod záštitou Festivalu bezpečného internetu vznikly ve spolupráci s Rádiem Junior a stanicí Českého rozhlasu pro děti audiopovídky **Vanda a Eda v Onl@jn světě**, které žáky 1. tříd základních škol připravují na jejich první zkušenosti ve světě internetu.

Online interaktivním komiksem NÚKIB **Digitální stopa: Příběh Svůďáka**, který se zaměřuje především na téma kybergroomingu pro žáky 4. a 5. tříd základních škol, prošlo **650 žáků**.

Pro studenty středních škol byla ve školním roce 2019/2020 opět realizována **Středoškolská soutěž kybernetické bezpečnosti**, organizovaná českou pobočkou AFCEA. Do soutěže se zapojilo téměř **4 500 studentů**, z nichž se 1 500 probojovalo do druhého kola.

Během druhého ročníku **Festivalu bezpečného internetu** NÚKIB do škol skrze školní informační systémy **Bakaláři** a **Škola Online** distribuoval videa, hry nebo podcasty, které tak byly nabídnuty až **280 000 uživatelů** přímo na jejich homepage. Zároveň na festivalu realizoval online panelovou diskusi **Efektivita kyberprevence**, jež na různých online platformách zhlédlo **4 500 diváků**, kteří se v rámci programu seznámili například s trendy a efektivními formami osvěty kybernetické bezpečnosti.

Masarykova univerzita otevřela nový **bakalářský obor Kyberbezpečnost**. Studenti tak budou moci studovat předměty jako např. Kyberkriminalita a kybernetická bezpečnost nebo Kybernetická bezpečnost v organizaci.

1 690

pracovníků prevence prošlo kurzem Bezpečně v kyber

650

žáků prošlo komiksem Digitální stopa

4 500

studentů se zapojilo do Středoškolské soutěže kybernetické bezpečnosti

V minulém roce jsme v ČR mohli pozorovat také významnou produkci osvětových a vzdělávacích audiovizuálních materiálů, jako jsou filmy, dokumentární filmy nebo seriály, které se zabývají různými tématy online bezpečnosti. Z nich lze vyzdvihnout:

#martyisdead: seriálový thriller na téma kyberšikany a manipulace, který připravila internetová televize Mall ve spolupráci se sdružením CZ.NIC a jeho projektem Bezpečně na netu. Seriál sklidil úspěch v tuzemsku i zahraničí, kde získal cenu Emmy v kategorii krátkometrážních seriálů.

Datová Lhota: naučný animovaný seriál z produkce České televize, který seznamuje děti ve věku prvního stupně základní školy s technickým zákulisím internetu a napomáhá s budováním návyků bezpečného chování.

V digitálním světě: podobně zaměřená edukační videa pro stejnou cílovou skupinu připravil také Jeden svět na školách, projekt organizace Člověk v tísni.

V síti: velký ohlas veřejnosti vzbudil také dokumentární film, který otevíral problematiku internetových predátorů.

O2 Chytrá škola: projekt Nadace O2, který pomáhá především pedagogům a rodičům lépe se orientovat v příležitostech i nástrahách digitálního světa.

V oblasti výzkumu a vývoje NÚKIB zveřejnil Národní plán výzkumu a vývoje v kybernetické a informační bezpečnosti s cílem identifikovat klíčová výzkumná témata pro rozvoj systému zabezpečení České republiky. NÚKIB se také zapojil do řešení výzkumných projektů, které se zabývají analýzou bezpečnostních rizik optických vláknových sítí a strategickým výzkumem a vývojem systémů pro zabezpečení moderních komunikačních sítí s využitím kvantového ustanovení klíčů a postkvantové kryptografie.

Začátkem roku 2020 bylo slavnostně otevřeno **Junior Centrum Excelence** pro informační bezpečnost Střední školy informatiky, poštovnictví a finančnictví Brno. Posláním Juniorních Center Excelence je zajistit vytvoření budoucí expertní základny, která umožní lépe čelit nejnovějším kybernetickým hrozbám. Tato centra jsou výjimečná a progresivní v přístupu k výuce a vzdělávání v informační bezpečnosti, v implementaci bezpečnostních opatření a v neposlední řadě také v technickém vybavení. S jejich pomocí mohou také další střední školy vyučovat informační bezpečnost.

MEZINÁRODNÍ SPOLUPRÁCE: RŮST VÝZNAMU KYBERNETICKÉ BEZPEČNOSTI NA EVROPSKÉ ÚROVNI

Vývoj regulačních nástrojů ČR závisí do velké míry na vývoji situace v zahraničí a na rozhodnutích přijímaných na evropské i mezinárodní úrovni. Zájmy ČR v oblasti kybernetické bezpečnosti v mezinárodních organizacích a integračních uskupeních, zejména pak v EU, OSN, NATO, ale i OECD, OBSE a MTU, zastupuje NÚKIB společně s Ministerstvem zahraničních věcí (dále jen „MZV"), Ministerstvem obrany a dalšími partnery.[13] V roce 2020 se na unijní úrovni soustředili zástupci ČR především na jednání v oblastech vyjednávání nařízení o kompetenčním centru, agendy certifikací kybernetické bezpečnosti, aplikace Cyber Diplomacy Toolboxu,[14] spuštění sítě CyCLONe,[15] sondážních rozhovorů k revizi

13 Ministerstvo průmyslu a obchodu, Český telekomunikační úřad a další.

14 V červenci 2020 došlo ze strany Evropské unie historicky poprvé k uplatnění sankčního mechanismu, který je součástí tzv. Cyber Diplomacy Toolbox. Sankce byly uvaleny na dva občany ČLR, čtyři občany Ruské federace a celkem tři organizace z ČLR, Ruska a KLDR.[xxi] Ze strany EU se jednalo o potrestání za kyberšpionážní kampaň Cloud Hopper odhalenou v dubnu 2017, za kterou stála čínská skupina APT10, dále za Rusku připisované útoky na Organizaci pro zákaz chemických zbraní (2018) a kybernetický útok NotPetya (2017) a v poslední řadě za ransomwarový útok WannaCry připisovaný KLDR. V říjnu 2020 byly sankce uvaleny na další dva občany a jednu organizaci z Ruské federace.[xxii] Identifikace jednotlivců a organizací z dotyčných zemí neznamená oficiální atribuci útoků ze strany EU, přestože v případě dvou ruských entit se jedná o organizační celky vojenské rozvědky Ruské federace GRU (taktéž GU). Identifikovaným fyzickým a právnickým osobám je zakázáno cestovat do EU a zároveň došlo ke zmrazení jejich finančních prostředků.

15 CyCLONe označuje síť styčných organizací pro řešení kybernetických krizí.

Směrnice NIS[16] nebo dokončení jednání o 5G EU Toolboxu[17] a jeho následné implementace. V rámci OSN pokračovala činnost tzv. Otevřené pracovní skupiny, na jejíž činnosti se NÚKIB a MZV také aktivně podílejí.

PRAGUE 5G SECURITY CONFERENCE 2020 A PŘEDSTAVENÍ PRAGUE 5G SECURITY REPOSITORY

NÚKIB ve spolupráci s Úřadem vlády a Ministerstvem zahraničních věcí uspořádal v září 2020 druhý ročník dvoudenní Prague 5G Security Conference, předního světového fóra pro diskusi o rizicích spojených s budováním 5G infrastruktury. Stejně jako minulý rok proběhla pod záštitou předsedy vlády ČR Ing. Andreje Babiše. I přesto, že se konference s ohledem na situaci spojenou s covid-19 poprvé konala virtuálně, vystoupilo na ní přes 50 řečníků z Evropy, USA, Jižní Koreje, Izraele, Austrálie, Indie a dalších zemí.

Hlavním výstupem druhého ročníku bylo představení a spuštění tzv. **Prague 5G Security Repository**, virtuální knihovny určené ke sdílení legislativních, strategických a dalších nástrojů, které státy v uplynulém roce v oblasti bezpečnosti 5G sítí přijaly. Letošní konference tak navázala na loňské zveřejnění tzv. Pražských návrhů (Prague Proposals), sady doporučení a principů, které by státy při budování 5G infrastruktury měly zohlednit.

Pro řadu států se Pražské návrhy přijaté v roce 2019 staly východiskem pro uzavření bilaterálních dohod v oblasti bezpečnosti 5G sítí a jsou tak explicitně zmíněny například v bilaterálních deklaracích k bezpečnosti 5G infrastruktury mezi USA a Estonskem, Polskem, Rumunskem, Kosovem, Slovinskem, Litvou, Bulharskem, Severní Makedonií nebo Slovenskem.

Třetí ročník Prague 5G Security Conference je plánován na podzim 2021. Jeho stěžejním tématem bude bezpečnost 5G infrastruktury ve spojitosti se vznikajícími a budoucími technologiemi (tzv. emerging technologies), včetně internetu věcí nebo umělé inteligence.

NOVÁ STRATEGIE KYBERNETICKÉ BEZPEČNOSTI EU[xxiii] A NÁVRH SMĚRNICE NAHRAZUJÍCÍ SMĚRNICI NIS[xxiv]

Závěr roku 2020 přinesl nový kybernetický „balíček“ z dílny Evropské unie, na jehož přípravě se podílela i ČR. Vedle vydání a postupné implementace 5G EU Toolboxu[xxv] a dokončení vyjednávání o nařízení o výzkumném kompetenčním centru pro kybernetickou bezpečnost[18] se u přípravy takto zásadních dokumentů s reálným dopadem ukazuje, jak důležitá je nastavená úzká spolupráce ČR v rámci Evropské unie.

Nová **Strategie kybernetické bezpečnosti EU** klade velký důraz na ochranu kritické infrastruktury, upozorňuje na ohrožení mezinárodní bezpečnosti a stability kvůli geopolitickému soupeření mezi státy a hybridním hrozbám a vyzdvihuje důležitost kybernetické bezpečnosti jako zásadního aspektu pro důvěru lidí v inovace a automatizaci.

Větší harmonizace právních předpisů a přístupu členských států v oblasti kybernetické bezpečnosti je předmětem **návrhu Evropské komise na nahrazení Směrnice NIS**. Podle nové směrnice by mělo být upraveno koordinované odhalování zranitelností, rozšířit by se měly sektory povinných osob, sjednotit by se měl způsob identifikace povinných osob a mají vzniknout také nové povinnosti v hlášení incidentů. Přestože je v některých ohledech navrhovaná harmonizace z pohledu ČR zbytečně silná, jedná se o kvalitní základ pro vyjednávání o konečné podobě této důležité unijní úpravy.

Oba dokumenty lze označit za zásadní pro politické a legislativní ukotvení kybernetické bezpečnosti v EU na řadu následujících let. Jejich ambicióznost odráží rostoucí důležitost kybernetické bezpečnosti na evropské i mezinárodní úrovni.

Česká republika se začátkem roku 2020 připojila k celoevropskému projektu, jehož cílem je vybudování celoevropské kvantové komunikační infrastruktury.

Chystaná síť umožní vysoce bezpečný přenos informací uvnitř jednotlivých zemí i mezi různými státy Evropské unie. Plánované komunikační kanály mají prioritně sloužit k zabezpečení kritické informační infrastruktury. Podle odhadů by k samotnému vybudování a spuštění kvantových sítí napříč EU mělo dojít v horizontu deseti let.

16 Oficiální název Directive on Security of Network and Information Systems.
17 Oficiální název EU Toolbox on 5G Cybersecurity.
18 Návrh nařízení Evropského parlamentu a Rady, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center.

VÝHLED TRENDŮ V KYBERNETICKÉ BEZPEČNOSTI V ČR NA ROKY 2021 A 2022

1. **RANSOMWARE**: Využívání vyděračského malwaru, kterým útočníci napadeným institucím zašifrují data a následně od nich požadují výkupné, bude téměř jistě (pravděpodobnost 90–100 %) představovat jednu z nejvýznamnějších kybernetických hrozeb i v následujících dvou letech. Zároveň je velmi pravděpodobné (pravděpodobnost 75–85 %), že bude i nadále pokračovat trend zvýšené sofistikovanosti kampaní a jejich zacílení na konkrétní oběti. Vzhledem k předpokladu přetrvávajícího tlaku na zdravotnická zařízení v letech 2021 a 2022 je téměř jisté (pravděpodobnost 90–100 %), že budou nadále cílem útoků ransomwaru. Mezi další cíle se velmi pravděpodobně (pravděpodobnost 75–85 %) zařadí velké podniky, instituce veřejného sektoru a vzdělávací zařízení.

2. **PHISHING, SPEAR-PHISHING A PODVODNÉ E-MAILY**: Nejzávažnějším hrozbám z roku 2020 bude ČR čelit i v následujících letech, především kvůli přetrvávající možnosti zneužívání tématu pandemie a rozvoji metod sociálního inženýrství, mj. sofistikovanějšího spear-phishingu spojeného s využitím deepfakes. Zároveň je pravděpodobné (pravděpodobnost 55–70 %), že rozšíření deepfakes bude častěji využíváno pro tzv. vishing (spojení slov voice a phishing), zaměřený jak na samotné uživatele, tak i na veřejné a zejména finanční instituce.

3. **NEDOSTATEK ODBORNÍKŮ NA KYBERNETICKOU BEZPEČNOST:** Dlouhodobý nedostatek odborníků představuje faktor, který ovlivňuje celou řadu oblastí a trendů v kybernetické bezpečnosti. Můžeme proto předpokládat, že v následujících letech bude velmi pravděpodobně (pravděpodobnost 75–85 %) narůstat využívání outsourcingu mnoha služeb spojených s IT infrastrukturou a jejím zabezpečením (mimo jiné tzv. Security as a Service).

4. **CLOUD**: Rostoucí obliba cloudového prostředí nadále velmi pravděpodobně (pravděpodobnost 75–85 %) povede k nárůstu kybernetických útoků zaměřených na tuto infrastrukturu. Cloudy budou vystaveny stále častějším útokům, protože jak státní aktéři, tak kyberkriminální skupiny se snaží získat přístup k citlivým datům nebo obchodním tajemstvím. Nedostatky v zabezpečení (např. nevhodná konfigurace) zůstanou pravděpodobně (pravděpodobnost 55–70 %) nejpoužívanějším vektorem útoku na cloudové služby. Nelze vyloučit (pravděpodobnost 25–50 %), že mezi zasaženými klienty těchto služeb se objeví i české organizace nebo společnosti.

5. **KYBERNETICKÉ ÚTOKY PROTI STRATEGICKÝM INSTITUCÍM STÁTU**: Ústřední orgány státní správy ČR budou v letech 2021–2022 velmi pravděpodobně (pravděpodobnost 75–85 %) čelit závažným kybernetickým útokům ze strany sofistikovaných aktérů. Státní sektor, včetně jeho strategických institucí (zejména ústřední orgány státní správy), patří kvůli své viditelnosti a přístupu k citlivým informacím k častým cílům kybernetických zločinců i státních aktérů. Případy ze zahraničí (např. případ SolarWinds) ukazují, že útočníci využívají stále propracovanější metody k proniknutí do systému oběti a útok se tak stává stále hůře detekovatelný. Na základě výše uvedených faktů, vlastních dat a informací od partnerů NÚKIB odhaduje, že trend závažných kybernetických útoků proti státním strategickým institucím se v následujících dvou letech projeví i v ČR a jedna nebo více z nich bude velmi pravděpodobně (pravděpodobnost 75–85 %) čelit závažnému kybernetickému útoku ze strany sofistikovaných aktérů.

SHRNUTÍ PŘÍLOH

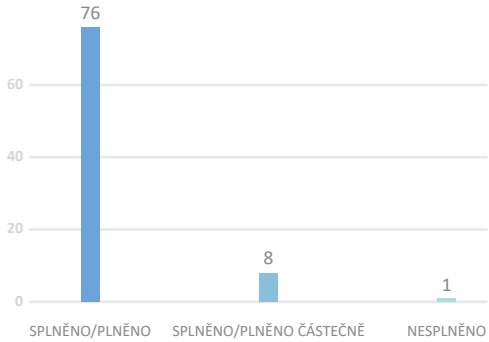
PŘÍLOHA 1: HLÁŠENÍ O STAVU NAPLŇOVÁNÍ AKČNÍHO PLÁNU K NÁRODNÍ STRATEGII KYBERNETICKÉ BEZPEČNOSTI NA OBDOBÍ LET 2015 AŽ 2020

Rok 2020 byl závěrečným rokem pro plnění Akčního plánu k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020 (dále jen „Akční plán"). Podstatná část úkolů byla vyhodnocena jako splněná či plněná. Vlivem pandemie covid-19 vzrostl ve srovnání s minulým rokem počet průběžných úkolů, které byly plněny pouze částečně z důvodu epidemiologických opatření, jež významně ovlivnila aktivity vyžadující osobní součinnost. Jako částečně plněné byly vyhodnoceny např. průběžné úkoly v oblasti kybernetických cvičení, jejichž realizace byla buď zrušena, nebo odložena. Obdobná situace panovala u vzdělávacích aktivit, z nichž byly některé přímo rušeny, odkládány, případně realizovány online formou.

Vyhodnocováno bylo také plnění těch úkolů, které byly v minulých letech plněny či splněny částečně. Jedním z nich bylo vytvoření automatizované platformy pro sdílení informací o kybernetických bezpečnostních hrozbách v gesci NÚKIB. V průběhu roku 2020 byla tato platforma vyvíjena jako součást projektu Neveřejný Web, jehož betatestování probíhá od začátku roku 2021 a od poloviny února 2021 dochází k postupnému připojování osob regulovaných ZKB a partnerů vládního CERT.

Pouze jeden z úkolů měl pevně stanovený termín plnění v daném roce, kterým bylo Plné zajištění kybernetické obrany ČR skrze kooperaci NCKO[19], NCKB, národního CERT a ostatních pracovišť typu CERT/CSIRT. Tento úkol, jehož gestorem bylo Vojenské zpravodajství, byl z důvodu odsunutí schválení nutných legislativních změn potřebných pro plnohodnotný výkon kybernetické obrany ČR vyhodnocen jako splněný částečně a jeho plnohodnotné naplnění bylo prozatím posunuto na rok 2022.

Graf 31: **Vyhodnocení úkolů v Akčním plánu za rok 2020**



PŘÍLOHA 2: VYHODNOCENÍ PLNĚNÍ CÍLŮ NÁRODNÍHO PLÁNU VÝZKUMU A VÝVOJE ZA ROK 2020

NÚKIB v oblasti výzkumu a vývoje zveřejnil **Národní plán výzkumu a vývoje v kybernetické a informační bezpečnosti** s cílem identifikovat klíčová výzkumná témata pro rozvoj systému zabezpečení ČR. Mezi tato témata patří:

1. **Prioritní výzkumná témata budou součástí veřejných soutěží a výzev národních a mezinárodních programů podpory výzkumu, vývoje a inovací.** NÚKIB v závěru roku 2020 zahájil sběr podkladů pro vypracování seznamu výzkumných potřeb za účelem jejich předložení v rámci Programu bezpečnostního výzkumu pro potřeby státu v letech 2022–2027. V rámci tohoto cíle NÚKIB podpořil snahu Ministerstva obrany ČR k posílení výzkumné a vývojové spolupráce v oblasti kybernetické bezpečnosti a obrany.

VYHODNOCENÍ: S ohledem na krátký časový horizont dosud nelze vyhodnotit, zda došlo k nárůstu realizovaných projektů oproti roku 2019.

19 NCKO je nástupcem Národního centra kybernetických sil (NCKS).

2. **Vyšší zapojení uživatelské komunity do systému podpory výzkumu, vývoje a inovací (VaVaI) v kybernetické bezpečnosti včetně posílení schopnosti zavádět výsledky do praxe.** NÚKIB se v roce 2020 zapojil do řešení dvou výzkumných projektů zaměřených na analýzu bezpečnostních rizik optických vláknových sítí a na strategický výzkum a vývoj systémů pro zabezpečení moderních komunikačních sítí s využitím kvantového ustanovení klíčů a postkvantové kryptografie. NÚKIB podal žádost o členství v radě programu TAČR – BETA2.

VYHODNOCENÍ: **NÚKIB oproti roku 2019 zvýšil své zapojení do projektů VaVaI financovaných z národních programů, ale s ohledem na krátký časový úsek nelze vyhodnotit, do jaké míry NÚKIB přispívá k zavádění výsledků VaV do praxe.**

3. **NÚKIB jako informační a analytické zázemí v oblasti VaVaI v kybernetické bezpečnosti** Na webových stránkách NÚKIB jsou pravidelně publikovány newslettery „Výzkum a nové technologie v kybernetické a informační bezpečnosti“ a „Novinky v oblasti výzkumu a vývoje v kybernetické bezpečnosti“. Na sklonku roku 2020 NÚKIB vypracoval souhrnnou zprávu „Trendy v kybernetické a informační bezpečnost v České republice pro roky 2020–2023“, která byla předána partnerům v bezpečnostní komunitě.

VYHODNOCENÍ: **NÚKIB se podařilo nastartovat proces pravidelného informování partnerů o možnostech financování výzkumných projektů, novinkách v oblasti VaVaI a o příležitostech zapojení do výzkumných konsorcií.**

4. **Rozvinutá mezinárodní spolupráce.** V roce 2020 NÚKIB pokračoval v podpoře projektových konsorcií v rámci programů Horizont 2020 a Connecting Europe Facility (CEF). Celkově se jednalo o podporu šesti projektů. NÚKIB dále podpořil připojení ČR k celoevropskému projektu EuroQCI, jehož cílem je vybudování celoevropské kvantové komunikační infrastruktury.

VYHODNOCENÍ: **Naplňování tohoto cíle bylo významně ovlivněno pandemií covid-19 a byl tak splněn pouze částečně. Nízké zapojování NÚKIB do mezinárodních výzkumných projektů je do značné míry ovlivněno nedostatkem vnitřních kapacit.**

5. **ČR aktivním účastníkem společně prováděného VaV v kybernetické bezpečnosti na úrovni EU.** NÚKIB se podílel na připomínkování nových evropských programů Horizont Evropa a Digitální Evropa. V oblasti vzniku Národního koordinačního centra v ČR NÚKIB připravoval národní pozice k návrhu nařízení zřídit Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center. NÚKIB se aktivně podílel na nastavení parametrů programového období 2021–2027, a to konkrétně v programech IROP – výzva Kybernetická bezpečnost, Fond obnovy či ReactEU. NÚKIB podnikl potřebné kroky pro zajištění implementace Aktu o kybernetické bezpečnosti do českého právního řádu v oblasti unijních certifikací kybernetické bezpečnosti.

VYHODNOCENÍ: **S ohledem na všechny aktivity NÚKIB považuje cíl za naplněný.**

ZDROJE

i FireEye. 2020. M-TRENDS.
https://content.fireeye.com/m-trends/rpt-m-trends–2020

ii GCN. 2020. Cyberattacks on state, local government up 50 %.
https://gcn.com/articles/2020/09/04/cyberattacks-state-local-government-climbing.aspx

iii Akutálně.cz. 2020. Na nemocnici v Brně zaútočil vyděračský virus, špitál povolal krizového IT manažera.
https://zpravy.aktualne.cz/domaci/na-nemocnici-v-brne-zautocil-vyderacsky-virus-spital-povolal/r~ff91a02c6aa011eab1110cc47ab5f122/

iv E-government. 2020. Zkušenosti z kybernetických útoků na sektor zdravotnictví.
https://www.egovernment.cz/soubor/zkusenosti-z-kybez-utoku-adam-kucinsky-nukib/

v iRozhlas. 2020. Počítače v Psychiatrické nemocnici Kosmonosy ochromil kyberútok. Péče o pacienty není ohrožena.
https://www.irozhlas.cz/zpravy-domov/pocitace-nemocnice-psychiatrie-kosmonosy-kyberutok-nukib_2003301855_aur

vi Aktuálně.cz. 2020. Další kybernetický útok za nouzového stavu: Hackeři napadli psychiatrickou nemocnici.
https://zpravy.aktualne.cz/domaci/kosmonosy-utok-koronavirus/r~188929ec732511ea9d74ac1f6b220ee8/

vii Bank Info Security. 2018. Cybercrime Groups andNation-State Attackers Blur Together.
https://www.bankinfosecurity.com/cybercrime-groups-nation-state-attackers-blur-together-a–11141

viii IT Security.2021. Healthcare Cyberattacks Doubled in 2020, with 28 % Tied to Ransomware.
https://healthitsecurity.com/news/healthcare-cyberattacks-doubled-in–2020-with–28-tied-to-ransomware

ix TREND MICRO. 2020. Boosting Impact for Profit: Evolving Ransomware Techniques for Tarheted Attacks.
https://www.trendmicro.com/en_us/research/20/i/boosting-impact-for-profit-evolving-ransomware-techniques-for-targeted-attacks.html

x Unit 42, Paloalto Networks. 2021. 2021 Unit 42 Ransomware Threat Report.
2021 Unit 42 Ransomware Threat Report (paloaltonetworks.com)

xi České noviny. 2020. MZe: Na Povodí Vltavy zaútočili hackeři, přehrady nejsou ohrožené.
https://www.ceskenoviny.cz/zpravy/mze-na-povodi-vltavy-zautocili-hackeri-prehrady-nejsou-ohrozene/1876968

xii Lupa. 2020. Počítačové systémy radnice Prahy 3 vyřadil malware.
https://www.lupa.cz/aktuality/pocitacove-systemy-radnice-prahy–3-vyradil-malware/

xiii Catalin Cimpanu. 2020. Microsoft says it identified 40+ victims of the SolarWinds hack.
https://www.zdnet.com/article/microsoft-says-it-identified–40-victims-of-the-solarwinds-hack/

xiv David E. Sanger, Nicole Perlroth a Eric Schmitt. 2020. Scope of Russian Hacking Becomes Clear: Multiple U.S. Agencies Were Hit.
https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html

xv Komerční banka. 2020. Upozornění Vishing (8. 10. 2020).
https://www.kb.cz/cs/o-bance/novinky/bezpecnost/upozorneni-vishing–8–10–2020

xvi Krebs On Security. 2020. Cyber Criminals Take Advantage of Increased Telework Through Vishing Campaign.
Cyber Criminals Take Advantage of Increased Telework Through Vishing Campaign (krebsonsecurity.com)

xvii REUTERS. 2020. U.S. says concerned by threat of cyber attack against Czech Republic healthcare. **https://www.reuters.com/article/us-czech-cyber-usa/us-says-concerned-by-threat-of-cyber-attack-against-czech-republic-healthcare-idUSKBN22000J**

xviii VŠE. 2020. Ransomware útok. **https://ci.vse.cz/blog/2020/02/11/ransomware-utok–11–02–2020/**

xix Masarykova univerzita. 2020. Varování: Sofistikovaný malware zaměřený na uživatele Masarykovy univerzity. **https://csirt.muni.cz/about-us/news/update_june_malware**

xx Centrum výpočetní techniky Univerzity Palackého v Olomouci. 2020. Objevila se nová forma ransomwaru. **https://www.facebook.com/itupol.cz/posts/1903363483128324/**

xxi Rada EU. 2020. EU poprvé uložila sankce za kybernetické útoky. **https://www.consilium.europa.eu/cs/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/**

xxii Rada EU. 2020. Nepřátelské kybernetické útoky: EU uvalila sankce na dvě fyzické osoby a jeden subjekt za hackerský útok v německém Spolkovém sněmu v roce 2015. **https://www.consilium.europa.eu/cs/press/press-releases/2020/10/22/malicious-cyber-attacks-eu-sanctions-two-individuals-and-one-body-over–2015-bundestag-hack/**

xxiii Evropská komise. 2020. Společné sdělení Evropskému parlamentu a Radě: Strategie kybernetické bezpečnosti EU pro digitální dekádu. **https://eur-lex.europa.eu/legal-cotent/CS/TXT/hHTML/?uri=CELEX:52020C0018&qid=1533485886151&from=EN**

xxiv Evropská komise. 2020. Návrh Směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o zrušení směrnice (EU) 2016/1148. **https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52020PC0823&from=EN**

xxv European Commission. 2020. Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures. **https://ec.europa.eu/digital-single-market/en/news/cybersecurity–5g-networks-eu-toolbox-risk-mitigatig-measures**

O NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) je ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany. Dále má na starosti problematiku veřejně regulované služby v rámci družicového systému Galileo. NÚKIB vznikl 1. srpna 2017 na základě zákona č. 205/2017 Sb., kterým se změnil zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

NÚKIB v současnosti pomáhá zajišťovat kybernetickou bezpečnost České republiky a jejích obyvatel prostřednictvím:

poskytování včasných, jasných a relevantních informací subjektům kritické informační infrastruktury, provozovatelům základní služby i orgánům veřejné správy;

zajišťování bezpečnosti utajovaných informací v informačních a komunikačních systémech včetně kryptografické ochrany;

přípravy národních bezpečnostních standardů, zákonů a podzákonných norem v oblasti kybernetické bezpečnosti;

pořádání tréninků a kybernetických cvičení na národní i mezinárodní úrovni;

analýzy trendů v oblasti kybernetické bezpečnosti;

poskytování technické pomoci a dalších služeb, např. prověření zabezpečení pomocí technik penetračního testování nebo poskytování skenů zranitelností;

vedení operativní reakce na kybernetické incidenty s využitím expertizy a přístupu k informacím pro efektivní zvládnutí incidentů;

poskytování metodické podpory, vzdělávání a osvěty v tématech spojených s oblastí kybernetické bezpečnosti;

provádění výzkumu a vývoje v oblasti kybernetické bezpečnosti;

vyhodnocování rizik v oblasti kybernetické bezpečnosti a přijímání příslušných nápravných a preventivních opatření;

provádění kontroly dodržování požadavků zákona o kybernetické bezpečnosti u regulovaných osob;

zastupování České republiky v orgánech mezinárodních organizací působících v oblasti kybernetické bezpečnosti;

spolupráce s veřejným, soukromým a akademickým sektorem na národní i mezinárodní úrovni.

Pro více informací o NÚKIB navštivte naše webové stránky **www.nukib.cz** nebo sledujte aktuality z oblasti kybernetické bezpečnosti v ČR na našich sociálních sítích **Facebook**, **Instagram** nebo **Twitter**.