NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

ZPRÁVA O STAVU KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY ZA ROK 2021

ZPRÁVA O STAVU KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY ZA ROK 2021

Úvodní slovo ředitele

Vážené čtenářky, vážení čtenáři,
vítám Vás u čtení Zprávy o stavu kybernetické bezpečnosti České republiky za rok 2021. V úvodu minulé Zprávy jsem zmiňoval vliv pandemie na kybernetickou bezpečnost i to, že se naše pracovní i soukromá komunikace přesunula ve velké míře na internet. Tato situace se za dva roky trvání pandemie výrazně nezměnila, komunikace na dálku se stala samozřejmostí, v některých případech i nezbytností. Opětovný nárůst kybernetických útoků pak znovu potvrdil, že internet je místem, ke kterému je třeba přistupovat s respektem a opatrností.
V roce 2021 jsme jako Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) museli řešit řadu kyberbezpečnostních výzev, vydali jsme dvě reaktivní opatření, z toho jedno kvůli velice závažné zranitelnosti Log4Shell. Historicky poprvé jsme také vydali ochranné opatření.
Důležitým krokem k posílení naší bezpečnosti bylo schválení Akčního plánu k Národní strategii kybernetické bezpečnosti České republiky na období let 2021 až 2025 (dále jen „Akční plán“). Akční plán stanovuje konkrétní kroky k dosažení cílů a vizí Národní strategie kybernetické bezpečnosti. Akční plán odráží celospolečenský přístup naší strategie a potřebu spolupráce napříč státní správou, soukromým sektorem i akademickou sférou. Právě účinná spolupráce je pro ochranu kyberprostoru naprosto nezbytná. Kyberprostor nás všechny propojuje a záleží na každém z nás, abychom ho společně dokázali chránit a udržovat bezpečný.
V průběhu celého roku jsme analyzovali hrozby a snažili se preventivně působit. V případě potřeby jsme pomáhali s řešením dopadů kyberútoků. Účastnili jsme se řady domácích i zahraničních akcí, organizovali jsme cvičení, školení, semináře a konference s domácími či zahraničními partnery i s veřejností. Rozvíjeli jsme mezinárodní spolupráci, podporovali jsme výzkum a vývoj v naší odbornosti a snažili jsme se dále rozvíjet spolupráci s partnery v soukromém sektoru.
To vše a mnoho dalšího jsme s pomocí řady partnerů i veřejnosti dělali, abychom posílili bezpečnost a odolnost České republiky v kyberprostoru.
Vzhledem k době, kdy je tato Zpráva vydávána, nemohu nezmínit agresivní válku, kterou v Evropě rozpoutala Ruská federace. Je to něco, co si většina z nás donedávna neuměla představit. Je příliš brzy hodnotit všechny dopady. Jedno je však jisté. Bezpečnostní prostředí, ve kterém jsme v posledních letech žili, se radikálně mění a dopady těchto změn se projeví i v kybernetickém prostoru. Musíme ještě urgentněji posilovat naše schopnosti a kapacity, včetně dostatečného množství vysoce kvalifikovaných odborníků. Musíme vybudovat bezpečnou a odolnou informační infrastrukturu. Musíme dále připravovat a vzdělávat naše spoluobčany. A musíme to dělat rychle.
Spolupráce při ochraně kybernetického prostoru bude čím dál důležitější. I proto bych zde rád poděkoval 283 organizacím, které se formou vypracování našich dotazníků podílely na přípravě Zprávy o stavu kybernetické bezpečnosti za rok 2021. Kybernetickým hrozbám lze čelit jen s partnery po boku a my si vážíme Vaší důvěry a podpory.

Karel Řehka

Shrnutí Zprávy o stavu kybernetické bezpečnosti České republiky za rok 2021

- Rok 2021 se vyznačoval **nárůstem škodlivých kybernetických aktivit**, ke kterým docházelo plošně na celém území ČR. Meziročně vzrostl počet kybernetických incidentů evidovaných NÚKIB i CSIRT.CZ a podle Policie ČR vykazovaly rostoucí trend také kyberkriminální aktivity.

- V roce 2021 zaznamenal NÚKIB celkem 157 kybernetických bezpečnostních incidentů oproti 99 incidentům v roce 2020. Meziročně vzrostl také poměr incidentů hlášených neregulovanými subjekty. Za tímto nárůstem pravděpodobně stojí proaktivita NÚKIB, větší povědomí o činnosti NÚKIB, ale také závažnost incidentů, se kterými se subjekty potýkaly. Nejčastějšími typy útoků byly v roce 2021 **phishing, podvodné e-maily a skenování vnější sítě**.

- Mezi nejvážnější hrozby pro kybernetickou bezpečnost v ČR patřily v roce 2021 **nově zveřejněné zranitelnosti, ransomwarové útoky a phishing či spear-phishing**. České instituce a společnosti ovlivnily zejména zranitelnosti ProxyLogon, ProxyShell a Log4Shell, jež způsobily téměř pětinu všech incidentů evidovaných NÚKIB. Zaznamenán byl také výrazný nárůst ransomwarových útoků, z nichž velká část nově zahrnovala ransomwary, které jsou poskytovány jako služba (tzv. RaaS, ransomware-as-a-service). Phishingové útoky podobně jako v minulých letech představovaly jeden z nejčastějších vektorů útoků a nadále vykazovaly rostoucí míru sofistikovanosti.

- Během roku vydal NÚKIB v reakci na aktuální hrozby celkem **26 upozornění.** V souvislosti se zranitelnostmi Microsoft Exchange Server a Log4Shell se NÚKIB rozhodl přistoupit k vydání **dvou reaktivních opatření**. Z důvodu nutnosti zabezpečení komunikace správců a provozovatelů informačních systémů příslušných subjektů pak došlo k historicky prvnímu využití institutu **ochranného opatření.**

- NÚKIB uspořádal ve spolupráci s Ministerstvem zahraničních věcí a pod záštitou Úřadu vlády **třetí ročník Prague 5G Security Conference**, který se zaměřil na otázky spojené s bezpečností 5G sítí a přelomových technologií (Emerging Disruptive Technologies, EDTs). [1] V průběhu konference vystoupilo téměř sedmdesát řečníků z Evropy i celého světa (např. z Izraele, Koreje, Japonska, Austrálie, USA, Kanady či Indie). Dvoudenní konference byla rozdělena na několik tematických panelů, kterých se virtuálně zúčastnily stovky mezinárodních posluchačů. Na závěr konference byly představeny tzv. **Pražské návrhy týkající se kybernetické bezpečnosti přelomových technologií a Pražské návrhy týkající se diverzity dodavatelů telekomunikací**.

- V roce 2021 NÚKIB pokračoval ve vzdělávání zaměstnanců veřejné správy a v rámci online kurzů **Dávej kyber!** a **Šéfuj kyber!** proškolil přes 26 500 uživatelů. Kurz základů rizikového chování na internetu **Bezpečně v kyber!** absolvovalo přes 2 800 uživatelů. Větší pozornost byla věnována vzdělávání zaměstnanců ve zdravotnictví. Úřad během roku spustil e-learningový kurz **Kyber nemocnice!**, který absolvovalo přes 4 400 zaměstnanců. Stejně jako v minulých letech probíhala také celá řada **osvětových a vzdělávacích aktivit pro děti, mládež i širší veřejnost**.

- Rok 2021 se nesl ve znamení návratu k fyzickému konání cvičení, kterých se na národní i mezinárodní úrovni uskutečnilo celkem 14. NÚKIB zorganizoval například cvičení **Health Czech**, historicky první sektorové cvičení kybernetické bezpečnosti ve zdravotnictví. Z aktivit na mezinárodní úrovni lze zmínit úspěch v podobě 3. místa českého týmu v rámci cvičení **Locked Shields 2021.**

[1] Mezi EDTs patří např. umělá inteligence, kvantové technologie, autonomní systémy či Massive Internet of Things.

Obsah

Seznam použitých zkratek

AFCEA – Armed Forces Communications & Electronics Association
ČR – Česká republika
DoS/DDoS – Denial of Service / Distributed Denial of Service
EDTs – Emerging and Disruptive Technologies
ENISA – Agentura Evropské unie pro kybernetickou bezpečnost
EU – Evropská unie
FREAK – Factoring RSA Export Keys
INCD – Israel National Cyber Directorate
JCU – Joint Cyber Unit
ITU – International Telecommunication Union
KII – Kritická informační infrastruktura
NATO – Severoatlantická aliance
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
OEWG – Open-Ended Working Group
OSN – Organizace spojených národů
RaaS – Ransomware-as-a-Service
SIEM – Security Information and Event Management
SSL – Secure Sockets Layer
TLS – Transport Layer Security
VeKySIO – Velitelství kybernetických sil a informačních operací
VKB – Vyhláška kybernetické bezpečnosti
VoIP – Voice over Internet Protokol
ZKB – Zákon o kybernetické bezpečnosti

2021: Kybernetická bezpečnost ČR v datech

476
hlášení kybernetických incidentů obdržených NÚKIB

157
kybernetických incidentů řešeno NÚKIB

8
velmi významných kybernetických incidentů řešených NÚKIB

1 726
bezpečnostních incidentů řešených CSIRT.CZ – národním bezpečnostním týmem ČR

1 281
řešených phishingových útoků CSIRT.CZ

9 518
trestných činů v oblasti kybernetické kriminality a kriminality páchané na internetu

490
účastníků cvičení kybernetické bezpečnosti uspořádaných NÚKIB

14
cvičení kybernetické bezpečnosti provedených NÚKIB

33 832
proškolených uživatelů kurzy NÚKIB

60
subjektů kritické informační infrastruktury

131
informačních a komunikačních systémů kritické informační infrastruktury

162
správců a provozovatelů významných informačních systémů

379
významných informačních systémů

124
provozovatelů základní služby

147
informačních systémů základní služby

O dokumentu

NÚKIB na začátku roku 2022 rozeslal dotazník se 79 otázkami, a to jak subjektům regulovaným zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „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 283 subjektů, z toho 199 regulovaných a 84 neregulovaných. Z těchto dat NÚKIB čerpal informace pro potřeby Zprávy o stavu kybernetické bezpečnosti České republiky za rok 2021 (dále také jen „Zpráva"). 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 používáme pravděpodobnostní výrazy, viz níže. 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 2021 potýkala, stejně jako aktivity, které napomáhají jejich zmírnění.

Pravděpodobnostní výrazy použité ve Zprávě o stavu kybernetické bezpečnosti za rok 2021

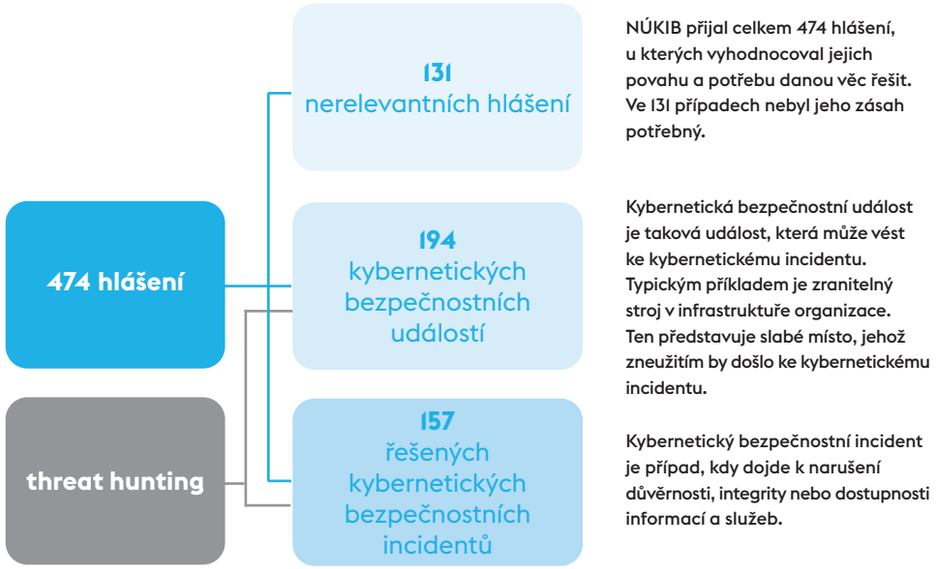
Pravděpodobnostní výrazy a vyjádření jejich procentuálních hodnot:

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 ČR v roce 2021 [2)]

Počet kybernetických bezpečnostních incidentů v roce 2021 registrovaných NÚKIB

NÚKIB v roce 2021 obdržel celkem 474 hlášení, z nichž značnou část vyhodnotil jako kybernetické bezpečnostní incidenty. **Na základě obdržených hlášení i z vlastní proaktivní činnosti (tzv. threat hunting) řešil NÚKIB v roce 2021 celkem 157 kybernetických bezpečnostních incidentů.**



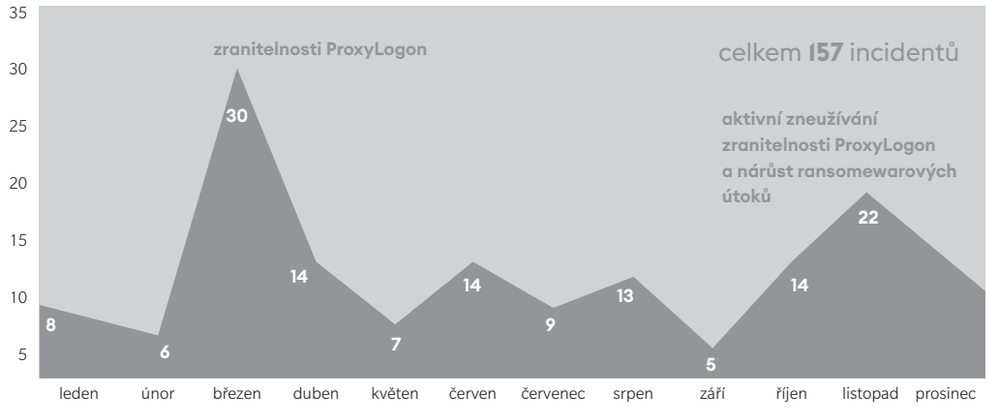
NÚKIB přijal celkem 474 hlášení, u kterých vyhodnocoval jejich povahu a potřebu danou věc řešit. Ve 131 případech nebyl jeho zásah potřebný.

Kybernetická bezpečnostní událost je taková událost, která může vést ke kybernetickému incidentu. Typickým příkladem je zranitelný stroj v infrastruktuře organizace. Ten představuje slabé místo, jehož zneužitím by došlo ke kybernetickému incidentu.

Kybernetický bezpečnostní incident je případ, kdy dojde k narušení důvěrnosti, integrity nebo dostupnosti informací a služeb.

Rekordním měsícem se s 30 incidenty stal březen, kdy probíhalo masivní zneužívání zranitelnosti ProxyLogon, která cílí na kompromitaci široce využívané služby Microsoft Exchange Server. Druhým nejrušnějším měsícem byl listopad, kdy byla napříč ČR aktivně zneužívána zranitelnost ProxyShell ve stejné službě a zároveň došlo k nárůstu ransomwarových útoků.

Graf I: **Počet řešených incidentů v průběhu roku 2021**



[2)] Prezentované informace vycházejí ze zdrojů NÚKIB a z vyhodnocení 283 dotazníků (viz část O dokumentu výše).

Oproti předchozímu roku narostl počet incidentů hlášených neregulovanými subjekty. Zatímco v roce 2020 to byla třetina z řešených incidentů, teď jejich podíl vzrostl na 40 %. Za větším počtem nahlášených incidentů neregulovanými subjekty pravděpodobně (55–70 %) stojí větší povědomí o činnosti NÚKIB a také závažnost jednotlivých incidentů. Neregulované subjekty NÚKIB hlásily především ransomwarové útoky, které měly dopad na jejich fungování.

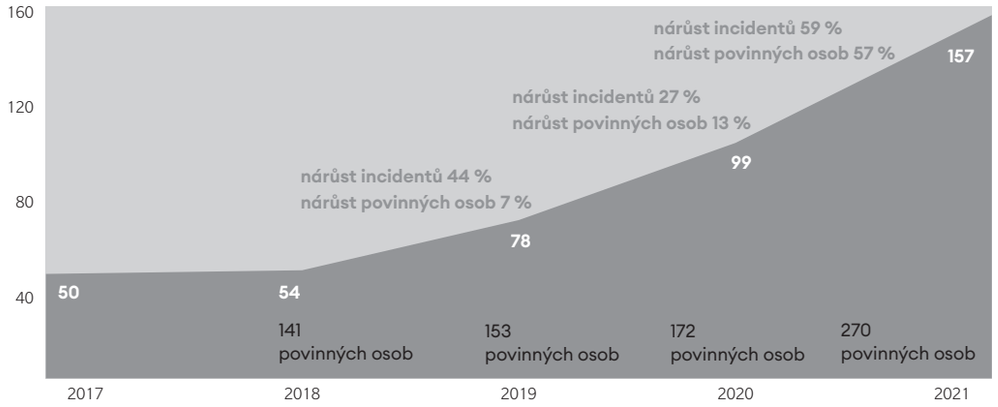
Regulované subjekty	Neregulované subjekty
94 incidentů	**63** incidentů

Srovnání počtu incidentů s předchozími lety: rostoucí trend ovlivněný několika faktory

NÚKIB detekuje neustále se zvyšující počet incidentů. Během roku 2021 řešil celkem 157 incidentů, což představuje **59 % nárůst oproti předchozímu roku**, kdy incidentů bylo 99. Za nárůstem pravděpodobně (55–70 %) stojí několik faktorů. Prvním a nejdůležitějším z nich je zvyšující se počet regulovaných subjektů. S tím, jak se počet povinných subjektů zvyšuje, roste i počet kybernetických incidentů, které subjekty hlásí. Nicméně jak ukazuje Graf 2, počet povinných subjektů není jediným faktorem, který za nárůstem počtu incidentů stojí. Počet incidentů roste rychleji, než počet povinných subjektů. Významnou roli hraje i větší aktivita útočníků, včetně kyberkriminálních skupin provozujících ransomware, a proaktivní vyhledávání napadených stanic ze strany NÚKIB.

Je velmi pravděpodobné (75–85 %), že počet kybernetických bezpečnostních incidentů bude narůstat i v následujících letech. V souvislosti s připravovanou revizí evropské směrnice NIS [3] se v příštích letech bude nadále zvyšovat počet povinných subjektů a vzhledem k finanční výnosnosti útoků pravděpodobně (55–70 %) dál poroste i aktivita kyberkriminálních útočníků.

Graf 2: **Závislost nárůstu incidentů na nárůstu povinných osob v jednotlivých letech** [4]



[3] Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii. Více k návrhu revize této směrnice viz část Mezinárodní spolupráce.

[4] Procentuální nárůsty jsou uvedeny vždy vůči předešlému roku.

Klasifikace kybernetických incidentů nahlášených NÚKIB [5]

Do klasifikace incidentů se z velké části promítly trendy uplynulého roku v podobě ransomwarových útoků a zneužívání zranitelností:

1. Dostupnost: Nejvíce incidentů minulého roku negativně ovlivnilo dostupnost služeb. Promítly se do toho DDoS útoky, technické chyby i ransomwarové útoky, které kvůli špatně řešeným zálohám omezily fungování napadených organizací.
2. Škodlivý kód: Druhou nejčastější kategorií se staly škodlivé kódy. Stojí za nimi především ransomwarové útoky. Ty nicméně nenapáchaly větší škody, jelikož napadené organizace měly své zálohy dobře vyřešené. Po zašifrování infrastruktury se jim tedy podařilo provoz rychle obnovit a dostupnost jejich služeb nebyla narušena. Vedle ransomwarových útoků NÚKIB v této kategorii řešil také případy malwaru, které na našem území hostovaly své kontrolní servery, především TrickBot, Emotet nebo Dridex.
3. Průniky: K výraznému nárůstu oproti roku 2020 došlo v incidentech, které NÚKIB klasifikoval jako průnik. Loni tvořily průniky 9 % všech incidentů, letos se číslo navýšilo na 22 %. Zatímco se škodlivé kódy a incidenty s dostupností objevovaly stabilně v průběhu celého roku, průniky přicházely skokově při zveřejnění nových zranitelností, jako např. v případě březnové kampaně zneužívání zranitelností MS Exchange Server.

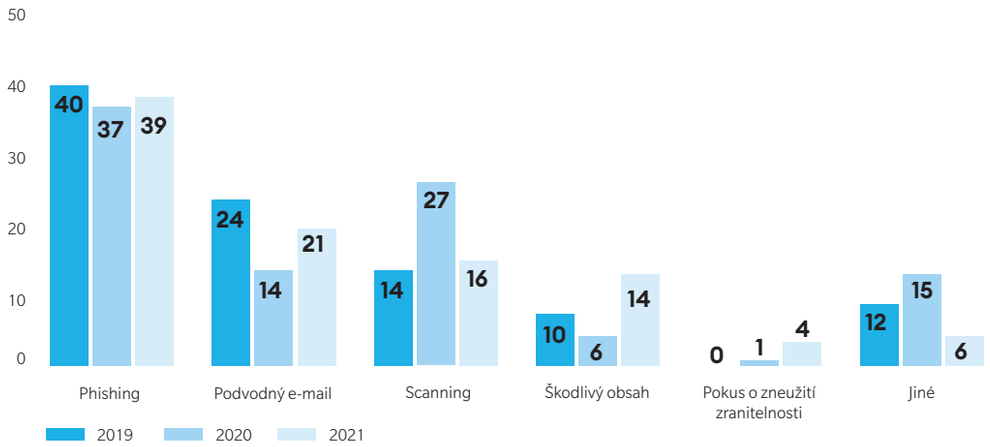
	Zastoupení v incidentech v %		Vývoj v průběhu roku
	2020	2021	
Dostupnost např. narušení dostupnosti způsobené DoS/DDoS útokem nebo sabotáží	29%	34%	
Škodlivý kód např. virus, červ, trojský kůň, dialer, spyware	36%	25%	
Průnik např. kompromitace aplikace nebo uživatelského účtu	9%	22%	
Podvod např. phishing, krádež identity nebo neoprávněné využití ICT	15%	10%	
Informační bezpečnost např. neautorizovaný přístup k datům, neautorizovaná změna informace	4%	8%	
Pokus o průnik např. pokus o zneužití zranitelnosti, pokus o přihlášení apod.	4%	1%	
Sběr informací např. skenování, sniffing, sociální inženýrství	2%	0%	

[5] Klasifikace kybernetických incidentů je založena na taxonomii ENISA: Reference Incident Classification Taxonomy — ENISA. V tabulce nahoře nejsou vyobrazeny kategorie „Urážlivý obsah“ a „Ostatní“. Ani jedna z nich nebyla v minulých dvou letech v incidentech zastoupena.

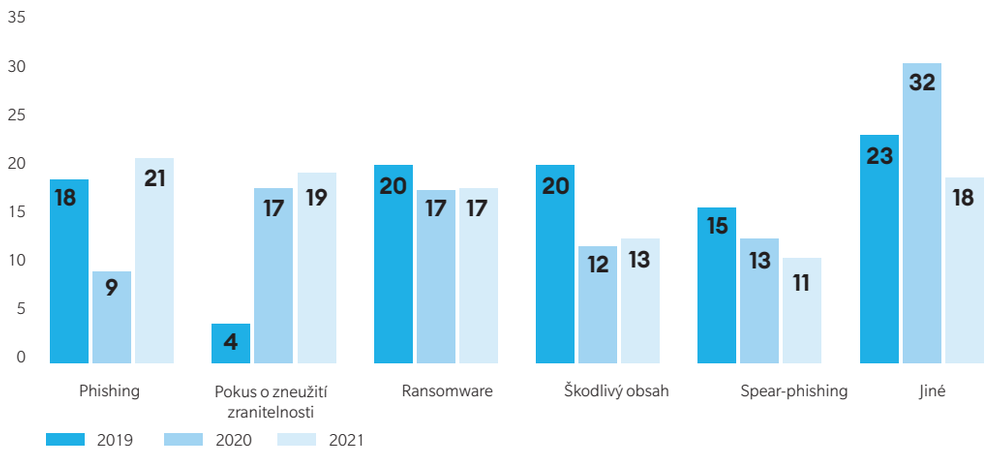
Incidenty pohledem subjektů: nárůst závažnosti phishingu a zneužívání zranitelností

Mezi nejčastější typy kybernetických útoků, se kterými se dotazované instituce a organizace setkaly v roce 2021, patřily phishing, podvodné e-maily a skenování vnější sítě (Graf 3).[6] Obdobně jako tomu bylo v minulých letech, mezi nejčastěji detekovanými útoky byly technicky méně náročné a zároveň snáze detekovatelné typy útoků. **Za nejzávažnější typy útoků v roce 2021 považovali respondenti phishing, pokusy o zneužití zranitelností a ransomware** (Graf 4). Zatímco ransomware patří mezi typy útoků, které subjekty dlouhodobě řadí mezi nejzávažnější, phishing a pokusy o zneužití zranitelností se dostaly do popředí v roce 2021 poprvé. Změna ve vnímání závažnosti těchto typů útoků je pravděpodobně (55–70 %) do značné míry ovlivněna stále rostoucí sofistikovaností phishingových útoků a zároveň častějším zneužíváním zranitelností škodlivými aktéry (více viz kapitolu Kybernetické hrozby a aktéři). Ačkoli téměř tři čtvrtiny dotazovaných subjektů zaznamenaly v roce 2021 pokus o kybernetický útok, **pouze u čtvrtiny respondentů došlo následkem útoku k narušení důvěrnosti, integrity nebo dostupnosti informací nebo služeb** (Graf 5). U většiny zasažených subjektů se pak počet zaznamenaných incidentů pohyboval mezi jedním a pěti.

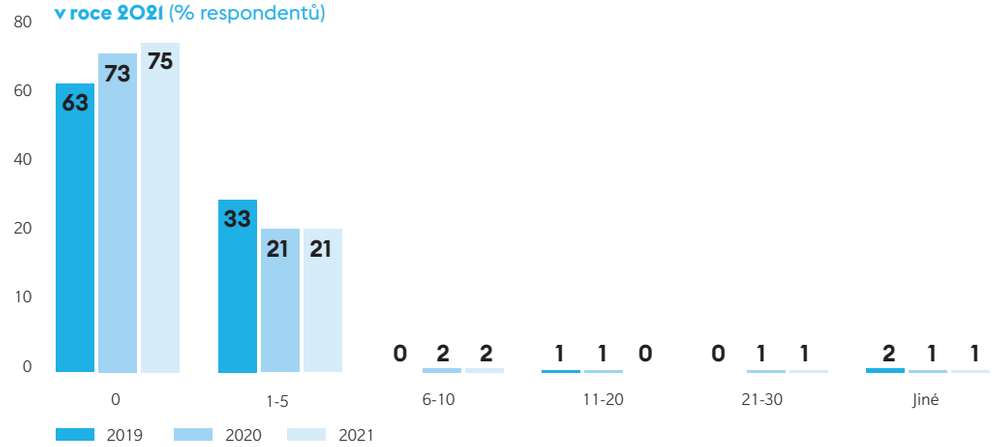
Graf 3: **Kategorie nejčastějších typů kybernetických útoků v letech 2019–2021** (%)



Graf 4: **Kategorie nejzávažnějších typů kybernetických útoků v letech 2019–2021** (%)



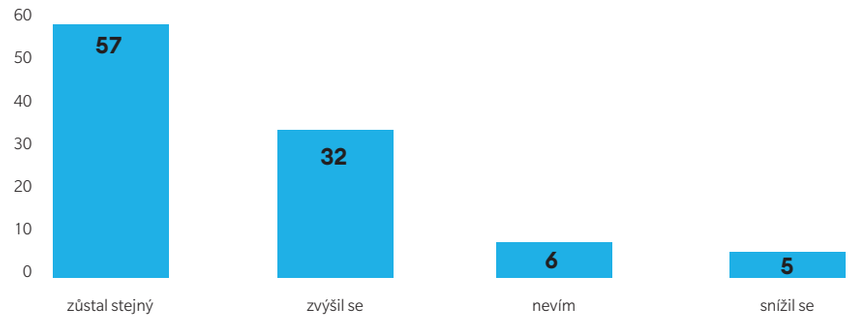
Graf 5: **Podíl útoků, u kterých došlo k narušení důvěrnosti, integrity nebo dostupnosti informací v roce 2021** (% respondentů)



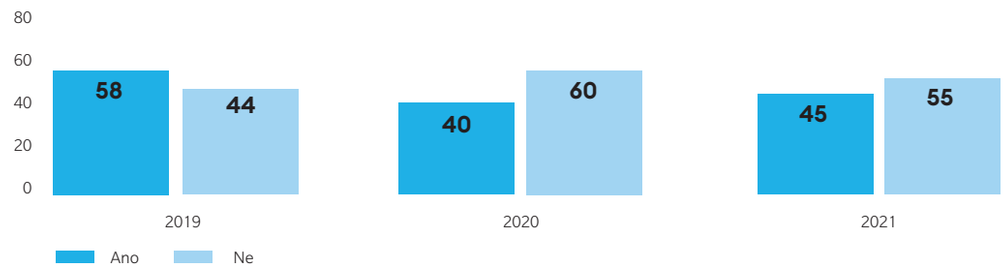
Finance vynaložené na kybernetickou bezpečnost: mírné, ale žádoucí navýšení rozpočtů

Zatímco u více jak poloviny respondentů zůstal rozpočet alokovaný na kybernetickou bezpečnost oproti minulému roku stejný, u necelé třetiny subjektů došlo k jeho navýšení (Graf 6). **Jde o zásadní zlepšení vývoje oproti roku 2020**, poznamenaném pandemickou krizí, kdy se ve 43 % případů finance alokované pro oblast kybernetické bezpečnosti snížily. **Navzdory tomu však i nadále více než polovina respondentů nepovažuje finance alokované na kybernetickou bezpečnost za dostatečné** (Graf 7). Podobně jako v minulých letech se u většiny respondentů podíl vynaložených nákladů na kybernetickou bezpečnost v roce 2021 pohyboval v rozmezí 0–5 % z celkového rozpočtu dotazovaných subjektů.

Graf 6: **Vývoj rozpočtů respondentů alokovaných na kybernetickou bezpečnost oproti roku 2020** (%)

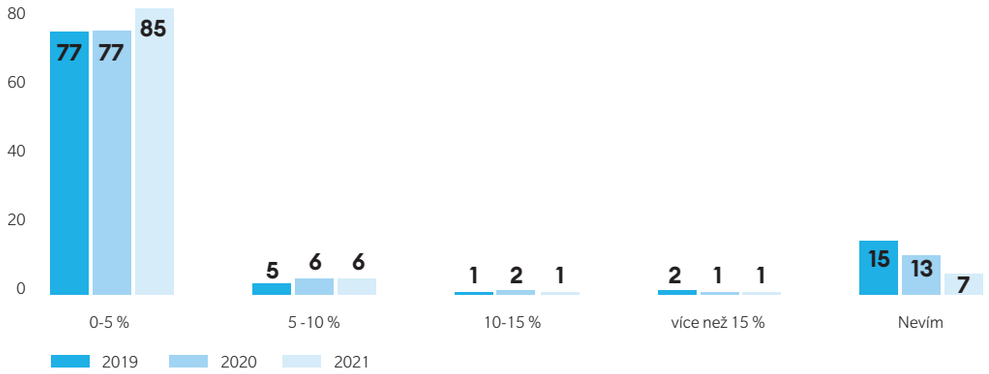


Graf 7: **Byly finance alokované na kybernetickou bezpečnost v letech 2019–2021 podle respondentů dostatečné?** (%)



[6] Vzhledem k zaokrouhlování výsledků dat z dotazníků se součet procent v uváděných grafech nemusí rovnat přesně stu.

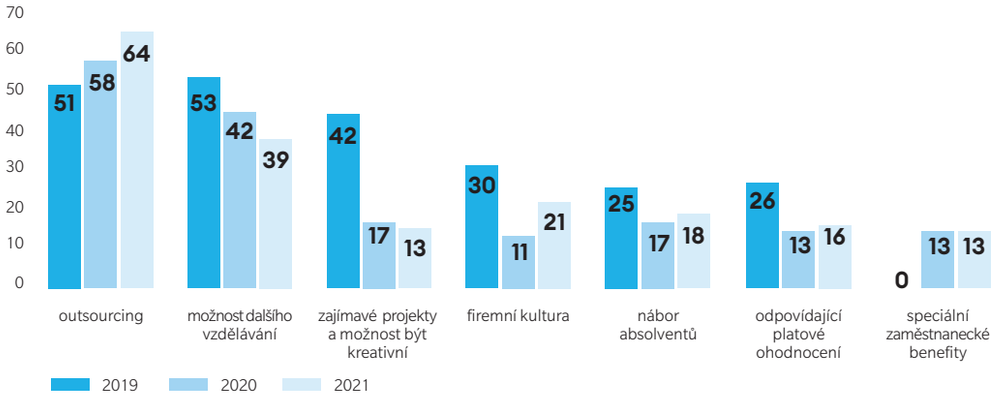
Graf 8: **Podíl rozpočtu alokovaného na kybernetickou bezpečnost z celkového rozpočtu organizací v letech 2019- 2021** (% respondentů)



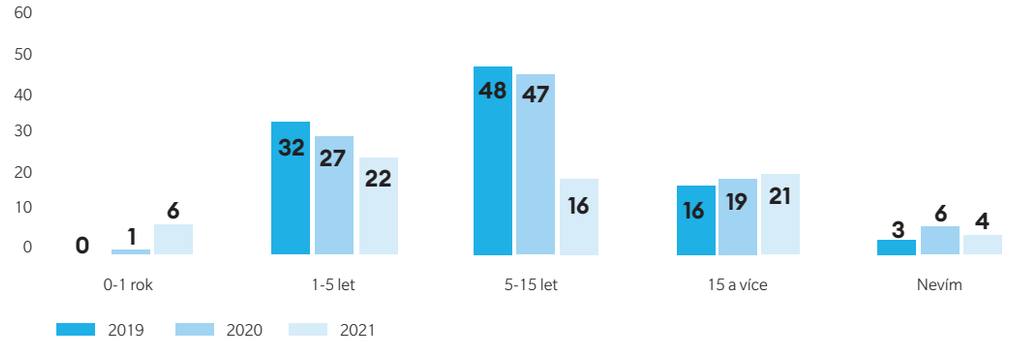
Lidé – odborníci: problém finančního ohodnocení a rostoucí počet méně zkušených zaměstnanců

Zajištění odborníků na kybernetickou bezpečnost představuje klíčovou výzvu, se kterou se potýká velká část českých institucí a organizací. Problém v tomto ohledu představuje zejména vysoká poptávka a s ní související vysoké nároky na finanční ohodnocení zaměstnanců. **Necelé tři čtvrtiny respondentů uvedly, že úroveň finančního ohodnocení je zásadním faktorem odrazujícím uchazeče při náborech na místa v oblasti kybernetické bezpečnosti.** Řada organizací zkrátka nemá dostatečné finanční prostředky na zaplacení potřebných odborníků, a proto je nucena situaci řešit jinými způsoby než odpovídajícím platovým ohodnocením. **Téměř dvě třetiny respondentů potýkajících se s nedostatkem odborníků jej řeší prostřednictvím outsourcingu.** Dotazované subjekty se snaží zaměstnance z oblasti kybernetické bezpečnosti nalákat a udržet také prostřednictvím různých firemních benefitů, například skrze možnost dalšího vzdělávání či možnost podílet se na zajímavých a perspektivních projektech (Graf 9). **Ačkoli počet organizací, které řeší problém neobsazených pozic náborem absolventů, zůstal oproti předešlému roku zhruba stejný, došlo v roce 2021 k nárůstu zaměstnanců s méně než jedním rokem praxe** (Graf 10). To může mimo jiné naznačovat, že subjekty nově přijímají na místa v oblasti kybernetické bezpečnosti také zaměstnance z jiných oborů.

Graf 9: **Jak se organizace v letech 2019–2021 snažily vypořádat s nedostatkem odborníků v oblasti kybernetické bezpečnosti?** (%)



Graf 10: **Průměrná relevantní praxe zaměstnanců zajišťujících kybernetickou bezpečnost v organizacích respondentů** (%)



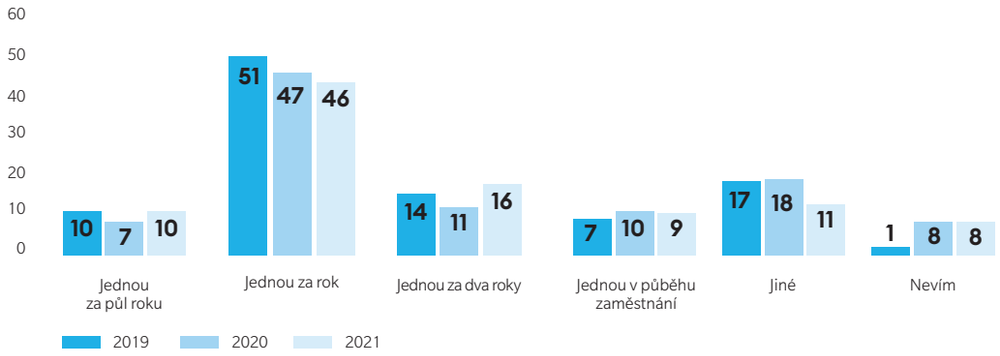
Pozitivním faktorem je to, že se finanční podmínky výrazněji neprojevují na fluktuaci odborníků na kybernetickou bezpečnost. V roce 2021 zaznamenalo odchod jednoho či více zaměstnanců v oblasti kybernetické bezpečnosti pouze 15 % respondentů (Graf 11), přičemž v 75 % případů nebyla výše finančního ohodnocení hlavním důvodem jejich odchodu. Nelze vyloučit (25–50 %), že důvodem tak nízkého počtu odchozích zaměstnanců je malý počet dedikovaných odborníků na kybernetickou bezpečnost u institucí, organizací a firem respondentů.

Graf 11: **Kolik zaměstnanců z oblasti kybernetické bezpečnosti odešlo z Vaší organizace během roku 2021 do 12 měsíců od nástupu?** (%)

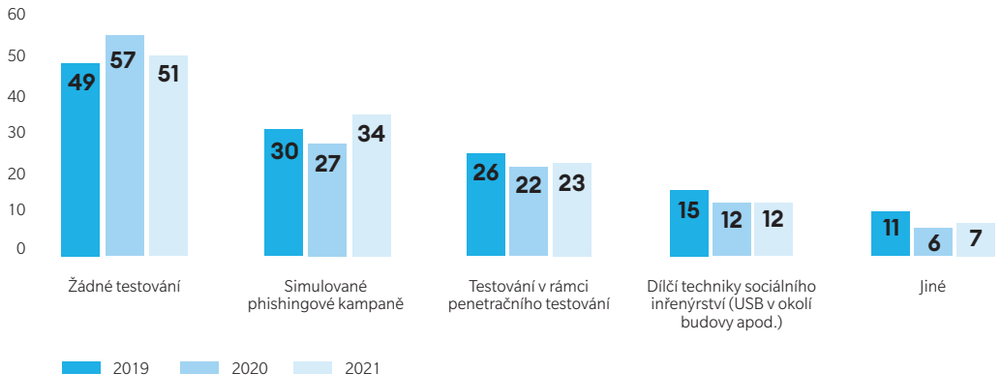
Lidé – uživatelé: školení i testování odolnosti zaměstnanců

Většina českých institucí a organizací se v rámci zajišťování své kybernetické bezpečnosti zaměřuje také na jeden z jejích klíčových prvků – uživatele. **Celkem 86 % dotazovaných subjektů školí uživatele v oblasti kybernetické bezpečnosti a seznamuje je s aktuálními kybernetickými hrozbami.** Nejčastěji tato školení probíhají jednou za rok (Graf 12), přičemž zhruba dvě třetiny organizací své zaměstnance školí skrze interní školení či e-learning. **Téměř polovina organizací se zároveň snaží zlepšovat odolnost svých zaměstnanců proti kybernetickým hrozbám.** Testování odolnosti probíhá převážně prostřednictvím simulovaných phishingových kampaní a dále také v rámci penetračního testování či skrze dílčí techniky sociálního inženýrství (Graf 13).

Graf 12: **Frekvence školení uživatelů v oblasti kybernetické bezpečnosti v organizacích v letech 2019- 2021** (% respondentů)



Graf 13: **Formy testování odolnosti zaměstnanců proti kybernetickým hrozbám v organizacích v letech 2019- 2021** (% respondentů)



Kybernetické hrozby a aktéři

Zranitelnosti v roce 2021: příčina téměř pětiny incidentů

Kybernetickou bezpečnost v ČR i v zahraničí v roce 2021 výrazně ovlivnily nově zveřejněné zranitelnosti. **Do kybernetických bezpečnostních incidentů NÚKIB se promítly především zranitelnosti ProxyLogon, ProxyShell a Log4Shell.** Ty způsobily necelých 18 % všech incidentů, které NÚKIB v roce 2021 evidoval. Jde o zranitelnosti, jež jsou mimořádně závažné. Systémy, kterých se dotýkají, jsou rozšířené po celém světě, jejich zneužití není technicky náročné a útočníkům mohou umožnit téměř cokoli, včetně kompletní kompromitace serveru. Vysokou míru zneužívání zranitelností zaznamenaly také dotazované subjekty. Pokus o zneužití zranitelností detekovalo celkem 40 % organizací, což představuje 14% nárůst oproti roku 2020.

Počet incidentů spojených se zranitelnostmi nahlášených NÚKIB v roce 2021:

21	5	2
ProxyLogon	ProxyShell	Log4Shell

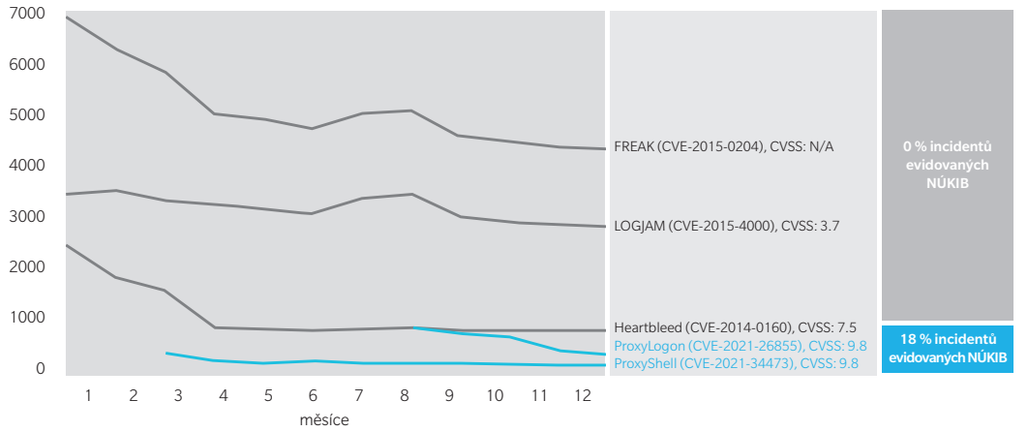
Březnová kampaň zneužívání zranitelností ProxyLogon, kdy útočníci kompromitovali e-mailové servery Microsoft Exchange, zasáhla 21 organizací. Jedenáct z nich byly organizace veřejné správy a několik z těchto případů se objevilo i v médiích. Zasaženy byly např. systémy Hlavního města Prahy. [1] Pražský magistrát v návaznosti na upozornění NÚKIB objevil napadené servery, které obratem odpojil a nahradil čistými instalacemi. Následkem incidentu došlo k omezení dostupnosti e-mailového serveru, data ale podle dostupných dat ztracena nebyla.

ProxyLogon je sada zranitelností postihující Microsoft Exchange Server, která byla zveřejněna 2. března 2021. ProxyLogon umožní bez autentizace a uživatelské interakce přístup k e-mailovým schránkám na serveru a následné vzdálené spuštění kódu. Útoky na e-mailové servery Microsoft Exchange představují pro útočníky lákavý cíl. Microsoft Exchange Server patří k nejrozšířenějším poštovním serverům na světě. Používají ho jak velké společnosti, tak státní organizace. Z povahy věci obsahují mnoho citlivých informací a útočníci je v případě napadení mohou zneužít nejen pro účely špionáže, ale i jako vstupní bod do sítě organizace.

Jak ukazuje Graf 14, **zneužívané zranitelnosti ProxyLogon, ProxyShell a Log4Shell nebyly na konci roku v ČR nejrozšířenější**. Podle nástroje Shodan je nejvíce strojů v ČR zranitelných vůči třem starým zranitelnostem FREAK, LOGJAM a Heartbleed. Žádná organizace v roce 2021 nicméně incident spojený s těmito zranitelnostmi NÚKIB nenahlásila. Je to pravděpodobně tím, že všechny tři zranitelnosti postihují staré verze šifrovacích protokolů (SSL/TLS, které jsou obsaženy v OpenSSL verzí starších než 1.01k). Tyto verze nevyhovují doporučením NÚKIB [7] a povinné osoby dle ZKB by je tak ve své infrastruktuře neměly používat.

[7] Viz dokument Minimální požadavky na kryptografické algoritmy.

Graf 14: **Vývoj zranitelnosti v roce 2021** [8)]



Zranitelnost Log4Shell, která byla zveřejněna 9. prosince, se do incidentů hlášených NÚKIB výrazněji nepromítla. Vzhledem k rozšířenosti zranitelnosti a jejímu plošnému zneužívání však mohlo být napadených organizací více než NÚKIB evidoval. I přesto následky Log4Shell nebyly tak rozsáhlé, jak bylo v souvislosti s natolik kritickou zranitelností očekáváno.[III]

Zranitelnost **Log4Shell** se nachází v logovacím nástroji Log4j, jenž využívají stovky systémů a aplikací. Celkový počet zranitelných systémů byl v době odhalení zranitelnosti odhadován na vyšší stovky milionů systémů po celém světě. Zranitelnost umožňuje napadnout i systémy, které nejsou přímo dostupné z internetu, spustit v nich kód zcela bez autentizace a získat plnou kontrolu nad serverem. Útočníci tak mohou získat přístupové údaje, číst a exfiltrovat data či instalovat další škodlivé kódy, včetně ransomwaru. To vše při relativně malém úsilí, protože zneužití této zranitelnosti není technicky náročné.

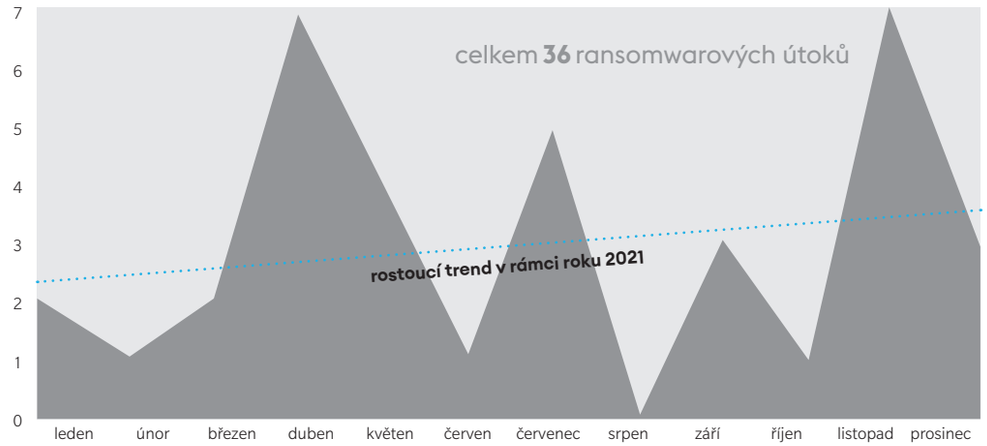
Nejčastější technika roku: zneužívání aplikací otevřených do internetu

Technikou, kterou útočníci v incidentech NÚKIB používali v roce 2021 nejčastěji,[9)] **bylo zneužívání aplikací otevřených do internetu** (Exploit Public-Facing Application).[III] Tato technika se vztahuje také na sérii zranitelností Microsoft Exchange ProxyLogon a ProxyShell, kde jsou servery přístupné na portu 443, a tudíž jsou otevřené do internetu. Tato skutečnost potvrzuje, že zranitelnosti v roce 2021 hrály v české kybernetické bezpečnosti zásadní roli.

Ransomware jako služba: nárůst aktivity a měnící se modus operandi

NÚKIB v roce 2021 řešil 36 ransomwarových útoků. Oproti předchozímu roku, kdy ransomware způsobil 21 incidentů, to představuje 71% nárůst. Ransomwarové útoky měly rostoucí tendenci i v roce 2021. Během posledního roku vzrostly přibližně o čtvrtinu (Graf 15). Nejvíce byl ransomware zastoupen v dubnových a listopadových incidentech. V dubnu dokonce tvořil polovinu všech kybernetických bezpečnostních incidentů nahlášených NÚKIB.

Graf 15: **Počet ransomwarových útoků v incidentech NÚKIB za rok 2021** [10)]



Ačkoli NÚKIB evidoval výrazný nárůst ransomwarových útoků, samotné subjekty zaznamenaly 11 % pokles tohoto typu útoků či pokusu o ně. **To může napovídat, že je tento typ útoku stále cílenější a zároveň efektivnější. Za tímto stavem však mohou stát také další faktory.** V roce 2021 například došlo k nárůstu incidentů hlášených neregulovanými subjekty, přičemž značná část z nich byla způsobena právě ransomwarovými útoky.

Během posledních let se stále více rozmáhá fenomén nazývaný ransomware jako služba (ransomware-as-a-service, dále jen „RaaS“). Kyberkriminální skupiny operující na bázi RaaS nabízejí své produkty za finanční obnos komukoliv, kdo chce provést ransomwarový útok a nabízené služby se liší v závislosti na druhu ransomwaru a výši platby za využití služby. Balíček služeb může zahrnovat uživatelskou podporu 24/7 nebo informace o aktuálním stavu infekce a počtu zašifrovaných souborů.[IV]

Jedním z typických rysů RaaS se v roce 2021 stalo tzv. double extortion (dvojí vydírání). V daném případě útočníci soubory oběti nejen zašifrují, ale zároveň také exfiltrují. Obětem pak vyhrožují, že pokud nezaplatí výkupné, jejich data zveřejnění nebo prodají dále. **V řešených incidentech NÚKIB se dvojí vydírání dotklo 14 % obětí ransomwarových útoků.** V jednom z útoků, jenž v roce 2021 NÚKIB řešil, se útočníci posunuli i k tzv. triple extortion (trojí vydírání), v jehož rámci provozovatelé ransomwaru nejprve zašifrovali data, exfiltrovali je a vedle jejich zveřejnění vyhrožovali oběti i DDoS útokem (viz box).

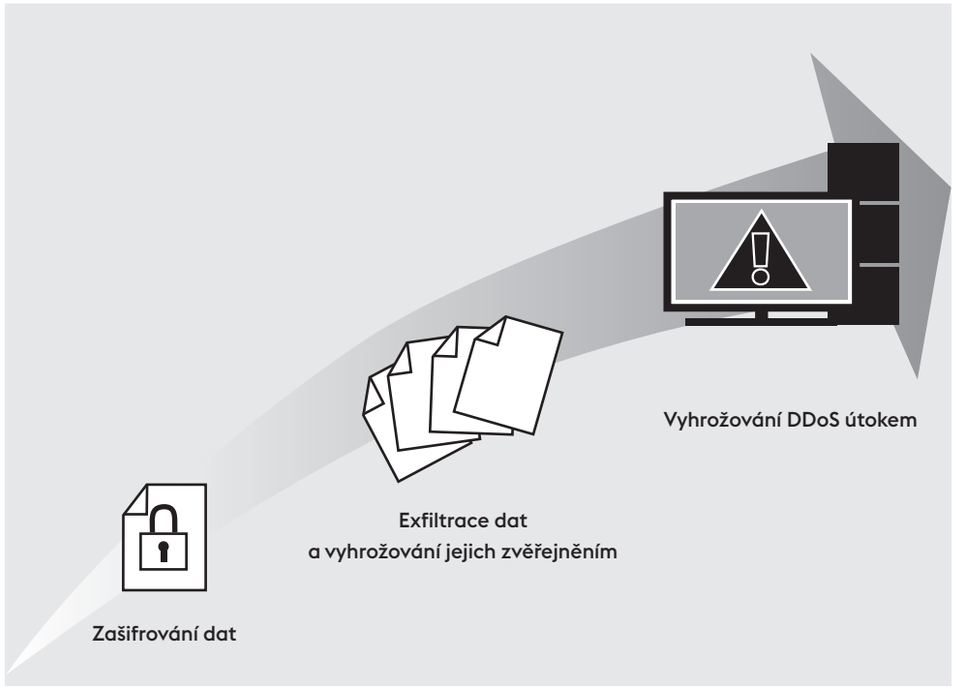
[8)] Zdrojem dat je nástroj Shodan. Zranitelnost Log4Shell v grafu uvedena není, a to z toho důvodu, že ji nástroje jako Shodan neevidují, protože sken této zranitelnosti by byl natolik intruzivní, že by se z něj stal de facto incident.

[9)] NÚKIB vyhodnocuje kybernetické incidenty na základě rámce MITRE ATT&CK, který slouží jako přehled známých technik a taktik používaných při kybernetických útocích. NÚKIB na jeho základě určuje i to, jak často útočníci technik a taktik ve svých útocích využívají.

[10)] Tento graf vychází pouze z incidentů hlášených NÚKIB. Na základě monitoringu darkwebu má NÚKIB povědomí o dalších českých obětech ransomwarových skupin.

V dubnu zašifroval ransomware Avaddon sítě statutárního města Olomouc. Útočníci se podle informací magistrátu dostali do infrastruktury skrze její prvek, který byl přístupný z internetu. Před zašifrováním stanic ze sítě exfiltrovali data a po magistrátu pak požadovali zaplacení 100 000 dolarů. Když jim magistrát výkupné nezaplatil, útočníci data zveřejnili na svých darkwebových stránkách. Byly mezi nimi například kontaktní údaje z plateb za komunální odpad nebo údaje pracovníků magistrátu. Když ale magistrát na výhrůžky nereagoval, útočníci se na něj pokusili vyvinout další tlak a začali proti jeho systémům provádět DDoS útoky. Celé vydírání a útoky trvaly více jak měsíc a magistrát bezprostředně po útoku odhadoval škody na přibližně jeden milion korun.

Schéma trojího ransomwarového vydírání



Phishing, spear-phishing a podvodné e-maily: nejčastější vektory útoků vykazují rostoucí sofistikovanost

V roce 2021 se s phishingovými e-maily setkalo 90 % respondentů, se spear-phishingovými e-maily 47 % respondentů a s podvodnými e-maily 84 % respondentů. Phishing představuje jeden z nejčastějších vektorů útoků, čemuž odpovídá i pravidelnost, se kterou se objevuje v incidentech hlášených NÚKIB. Za celý rok totiž NÚKIB nezaznamenal phishingové, spear-phishingové nebo vishingové kampaně pouze ve třech měsících.

NÚKIB v reakci na phishingové kampaně vydal v roce 2021 dvě upozornění. V rámci jedné z kampaní se útočníci snažili uživatele nalákat ke kliknutí na podvodný odkaz a vyplnění přihlašovacích údajů, po jejichž získání zneužívali schránku k rozesílání phishingu dále.

- **Upozornění na novou vlnu podvodných vyděračských e-mailů**
- **Upozorňujeme na novou vlnu phishingových mailů**

Další dvě upozornění pak NÚKIB vydal v návaznosti na vlny podvodných telefonních hovorů (vishing), v rámci nichž se útočníci vydávali za zaměstnance bankovních institucí či za technickou podporu společnosti Microsoft.

- **Upozornění na podvodné telefonáty od falešné technické podpory Microsoft**
- **Upozornění na vishing zneužívající identitu bankovních institucí**

https://www.nukib.cz/cs/infoservis/hrozby/1670-upozorneni-na-novou-vlnu-podvodnych-vyderacskych-emailu/
https://www.nukib.cz/cs/infoservis/hrozby/1680-upozornujeme-na-novou-vlnu-phishingovych-mailu/
https://www.nukib.cz/cs/infoservis/aktuality/1699-upozorneni-na-podvodne-telefonaty-od-falesne-technicke-podpory-microsoft/
https://www.nukib.cz/cs/infoservis/hrozby/1705-upozorneni-na-vishing-zneuzivajici-identitu-bankovnich-instituci/

90 %
dotazovaných organizací uvedlo, že na ně byl v roce 2021 veden **phishingový útok** nebo pokus o něj

84 %
dotazovaných organizací uvedlo, že na ně byl v roce 2021 veden útok nebo pokus o něj formou **podvodného e-mailu**

47 %
dotazovaných organizací uvedlo, že na ně byl v roce 2021 veden **spear-phishingový útok** nebo pokus o něj

11 %
dotazovaných organizací uvedlo, že na ně byl v roce 2021 veden **vishingový útok** nebo pokus o něj

Phishingové útoky jsou navíc rok od roku sofistikovanější. Již v minulých letech se phishingové e-maily vyznačovaly poměrně kvalitní češtinou, propracovanějšími formáty a různorodostí motivů (např. exekutorské výzvy, zápisy z jednání či témata spojená s koronavirem).[VI] **V roce 2021 někteří útočníci ve snaze rozšířit dosah a zvýšit efektivitu svých útoků přistoupili ke dvoufázovému schématu**. Během první fáze posílali phishingové zprávy s podvrženou adresou odesílatele a výzvou ke kliknutí na odkaz či otevření přílohy. V případě úspěšného útoku pak útočníci ve druhé fázi využili kompromitovaných emailových schránek a rozesílali z nich phishingové zprávy dále ve snaze proniknout do dalších institucí či organizací. V některých případech navíc phishingové e-maily navazovaly na přechozí e-mailovou korespondenci své oběti.

Útoky na dodavatelský řetězec: rozdílné vnímání závažné hrozby

V roce 2021 došlo na mezinárodní scéně k řadě významných útoků na dodavatelský řetězec. **Jedním z nejvýznamnějších se stal ransomwarový útok na dodavatelský řetězec společnosti Kaseya** (viz box níže), **který se navzdory své rozšířenosti nepromítl do incidentů registrovaných NÚKIB.** Zmínit však lze kybernetický incident, během něhož došlo k ransomwarovému útoku na server české společnosti, která svým zákazníkům poskytuje ICT řešení. V důsledku útoku došlo ke ztrátě dat všech klientů, kteří napadený server využívali, a to včetně záloh. Z dostupných informací nicméně nelze určit, zda útočník cílil přímo na data klientů společnosti, nebo jen na server dodavatele a jeho klienti se stali vedlejšími oběťmi útoku.

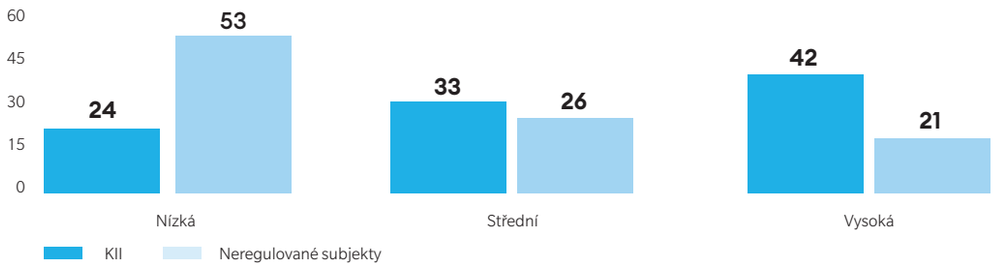
Ransomwarový útok na společnost Kaseya

V červenci 2021 došlo k dosud největšímu ransomwarovému útoku vedenému skrze dodavatelský řetězec, kdy ransomwarový gang REvil napadl společnost Kaseya, dodavatele softwarových řešení. Útočníci zneužili zranitelnost ke kompromitaci softwaru Kaseya VSA, jejž využívají poskytovatelé spravovaných služeb (Managed Service Providers, MSP). REvil kompromitoval stovky serverů MSP, z nichž byl poté ransomware šířen k jejich klientům. Celkem byly napadeny systémy více než 1 500 společností v osmnácti zemích světa.

Útok skrze dodavatele služeb či pokus o něj zaznamenalo v roce 2021 zhruba 6 % institucí či organizací. Oproti roku 2020 jde o zhruba dvojnásobný nárůst, nicméně i nadále zůstává tento typ útoku mezi nejméně častými. To je pravděpodobně (50–70 %) způsobeno kombinací několika faktorů, a to zejména nízkým výskytem tohoto typu útoku v ČR, nízkou schopností detekce ze strany organizací nebo snahou útočníků o nepozorovanou přítomnost v systémech oběti.

Dlouhodobě nízký výskyt zaznamenaných útoků skrze dodavatelský řetězec pravděpodobně (55–70 %) vede k tomu, že většina subjektů tuto hrozbu vnímá jako nízkou. Vnímání této hrozby se nicméně liší v závislosti na tom, do které kategorie subjekty spadají. Zatímco většina neregulovaných subjektů tuto hrozbu vnímala jako nízkou, **zhruba tři čtvrtiny povinných osob spadajících do kritické informační infrastruktury ji považovaly za střední či vysokou** (Graf 16).

Graf 16: **Jak velká byla hrozba kybernetických útoků ze strany dodavatele služeb, softwaru a hardwaru v roce 2021?** (% respondentů z KII a neregulovaných subjektů)

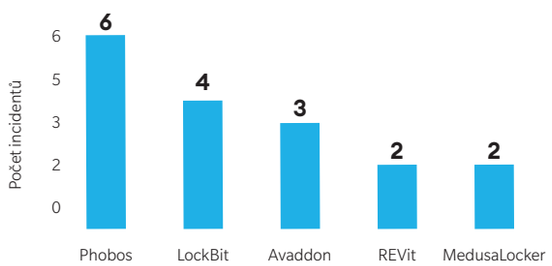


Aktéři kybernetických hrozeb

Aktivity státem podporovaných aktérů v kybernetickém prostoru a kybernetická kriminalita dlouhodobě patří mezi nejvážnější hrozby pro kybernetickou bezpečnost ČR.

Státem podporované skupiny jsou zpravidla vysoce sofistikovanými aktéry, kteří k dosažení svých cílů využívají širokou škálu technik a neustále zdokonalují své nástroje. **V posledních letech tyto skupiny v rámci svých útoků stále častěji využívají open source nástroje a zaměřují se na aktivní zneužívání zranitelností nultého dne.**[VII] Tento trend pokračoval také v roce 2021[VIII], přičemž nelze vyloučit (25–50 %), že některé z incidentů řešených NÚKIB a souvisejících s nově zveřejněnými zranitelnostmi byly provedeny státem sponzorovanými skupinami.

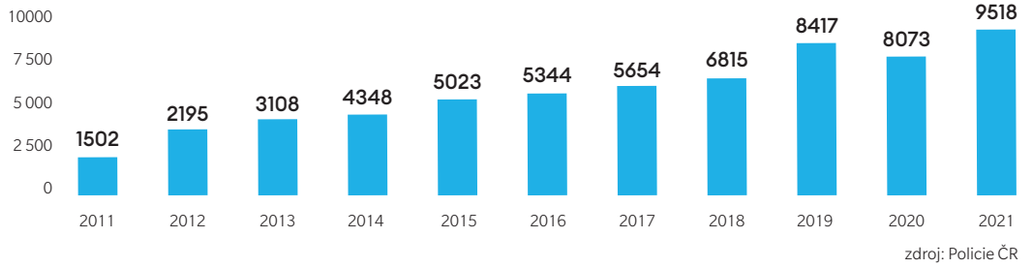
Graf 17: **Nejaktivnější ransomwarové skupiny v ČR**



Kyberkriminální uskupení se v roce 2021 zaměřovala zejména na různé druhy podvodného jednání zahrnujícího například opakující se vlny podvodných e-mailových či jiných zpráv nebo investiční podvody. Významnou součástí kyberkriminality byla také činnost ransomwarových gangů, v jejímž rámci byl viditelný trend přesunu k modelu RaaS. **Ransomwary, které se v incidentech NÚKIB objevovaly nejčastěji, jsou všechny nabízeny jako služba** (Graf 17). Je pravděpodobné (55–70 %), že RaaS model bude v útocích na české instituce a organizace převažovat také v následujícím roce.

Ze statistik Policie ČR vyplývá, že počet případů kybernetické kriminality a kriminality páchané na internetu dlouhodobě roste (Graf 18). Vzestupný trend narušila v roce 2020 novelizace trestního zákoníku, která zvýšila hranici výše škody nutné pro naplnění jednotlivých skutkových podstat trestních činů. Za rok 2021 již bylo registrováno celkem 9 518 skutků spadajících do kategorie kybernetické kriminality a ostatní kriminality páchané v kyberprostoru, což značí meziroční nárůst o 18 %. Na základě dosavadního vývoje je tak velmi pravděpodobné (75–85 %), že protiprávní jednání v rámci internetového prostředí bude mít vzrůstající charakter také v následujících letech.

Graf 18: **Vyšetřované kyberkriminální případy v ČR mezi lety 2011 a 2021**



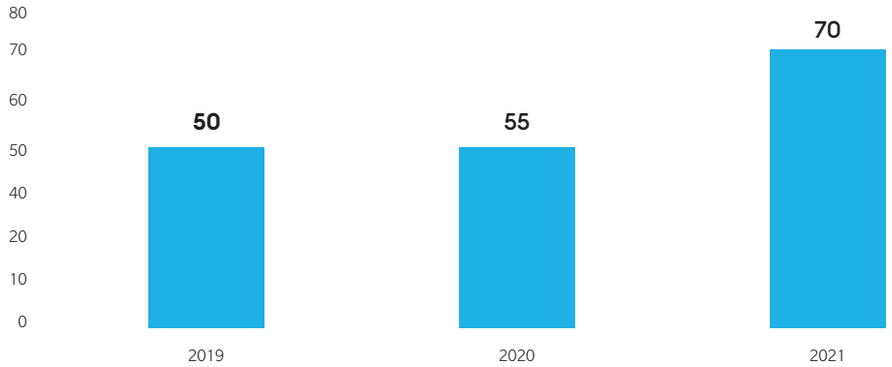
zdroj: Policie ČR

Cíle kybernetických útoků

Kritická informační infrastruktura: vysoké nároky na zajištění dostupnosti služeb

Podobně jako v minulých letech byly subjekty kritické informační infrastruktury (dále jen „KII“) v roce 2021 vystaveny stovkám až tisícům pokusů o kybernetický útok. Počet incidentů registrovaných NÚKIB v dané kategorii se nicméně meziročně snížil zhruba o čtvrtinu. **Narostl však podíl incidentů, které vyústily v omezení dostupnosti služeb, a to na celkových 70 %** (Graf 19). Dostupnost je u KII jedním z klíčových prvků, jehož narušení může mít zásadní dopady (viz box). Toho jsou si útočníci dobře vědomi a zejména ransomwarové gangy při svých útocích spoléhají na vysoký tlak na udržení či obnovení produkce u KII, který může zvýšit pravděpodobnost zaplacení výkupného.

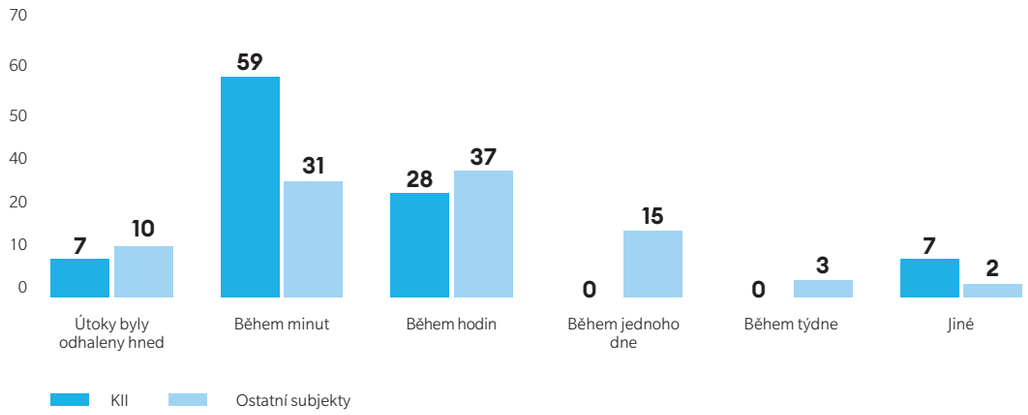
Graf 19: **Vývoj podílu incidentů hlášených NÚKIB v kategorii KII vedoucích k omezení dostupnosti v letech 2019–2021** (%)



Kritickou informační infrastrukturou je podle § 2 písm. b) ZKB prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti. Kritická infrastruktura samotná je podle § 2 písm. g) zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů, definována jako prvekm kritické infrastruktury nebo systém prvků kritické infrastruktury, narušení jehož funkce by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu. Mezi typické prvky kritické infrastruktury 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).**

Vysoká míra útoků směřujících na omezení dostupnosti se pravděpodobně (55–70 %) promítla také do rychlosti identifikace kybernetických útoků. Zatímco u KII bylo 92 % útoků odhaleno do několika hodin, u ostatních subjektů bylo do této doby identifikováno pouze 77 % útoků. Vypořádávání se s následky incidentů nicméně bylo pro subjekty KII náročnější. Až 21 % subjektů KII zabralo řešení následků incidentů týdny či měsíce (Graf 20), zatímco u ostatních činil tento průměr 17 %.

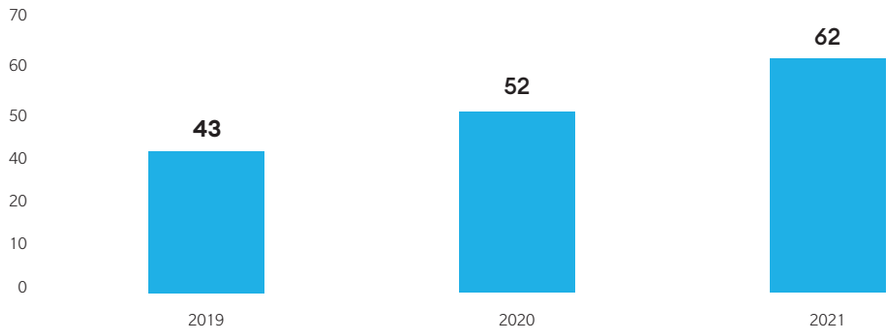
Graf 20: **Průměrný čas potřebný k identifikaci kybernetického útoku respondenty v roce 2021** (%)



Veřejný sektor: vysoký počet incidentů a mírné zlepšení financování

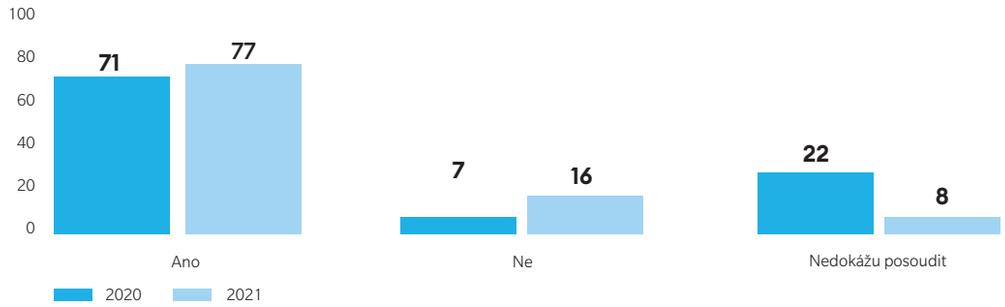
Veřejný sektor patřil v roce 2021 mezi jedny z nejvíce zasažených sektorů. **Téměř ke 40 % všech kybernetických bezpečnostních incidentů registrovaných NÚKIB došlo právě ve veřejném sektoru.** Počet incidentů v tomto sektoru navíc kontinuálně narůstá (Graf 21). Mezi nejčastěji zaznamenanými typy útoků byly podobně jako v předešlém roce phishing, podvodné maily a skenování vnější sítě. Jako nejzávažnější hodnotily instituce zejména ransomware a pokusy o zneužití zranitelností.

Graf 19: **Vývoj počtu incidentů ve veřejném sektoru evidovaných NÚKIB v letech 2019–2021**



Navzdory poměrně vysokému počtu incidentů **vnímají více jak tři čtvrtiny subjektů z veřejného sektoru úroveň zajištění kybernetické bezpečnosti jako dostatečnou** (Graf 22). Až 89 % respondentů se domnívá, že se úroveň jejich kybernetické bezpečnosti zvýšila. To může do jisté míry souviset se skutečností, že oproti roku 2020 poznamenaném pandemickou krizí se alespoň částečně zlepšila situace týkající se rozpočtů alokovaných na kybernetickou bezpečnost. Zatímco v roce 2020 se u téměř poloviny institucí rozpočty snížily, v roce 2021 došlo ke snížení pouze u 8 % subjektů. U dvou třetin zůstal rozpočet stejný, a u téměř jedné pětiny se dokonce zvýšil.

Graf 22: **Vnímáte úroveň zajištění kybernetické bezpečnosti ve Vaší organizaci jako dostatečnou?** (% srovnání let 2020–2021)



Finanční sektor: zabezpečení i financování na poměrně dobré úrovni

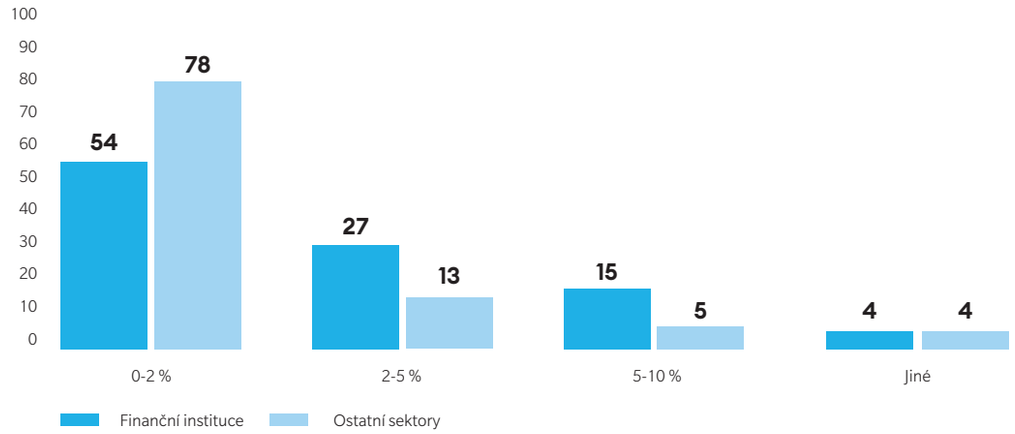
Český finanční sektor bývá označován za jedno z nejlépe zabezpečených odvětví, čemuž nasvědčuje také absence vážnějších incidentů v roce 2021. Navzdory poměrně dobrému zabezpečení se tomuto sektoru pokusy o kybernetické útoky nevyhýbají. **Až 81 % finančních institucí zaznamenalo v roce 2021 pokus o útok. Nejčastějšími typy útoků směřující vůči finančnímu sektoru byly phishing, podvodné e-maily a různé škodlivé kódy.** V nejméně jeden kybernetický incident pak vyústila necelá čtvrtina zaznamenaných útoků. Útočníci se v roce 2021 poměrně často zaměřovali nejen na finanční instituce, ale také na jejich klienty. V tomto ohledu byl viditelný zejména nárůst vishingových kampaní (viz box). [X]

Vishingové útoky nadále pokračují

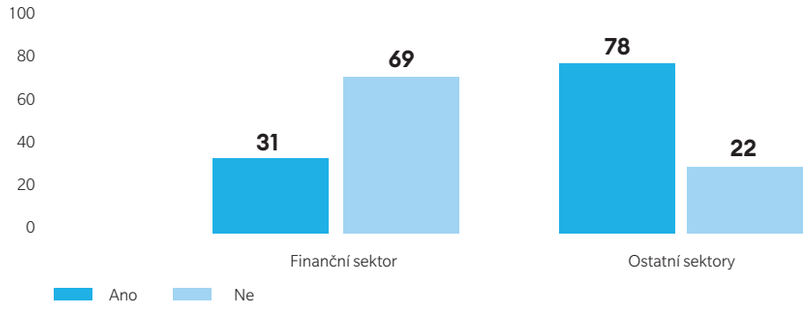
Trend vishingových útoků vůči klientům finančních institucí, pokračoval také v roce 2021. Před vlnami podvodných telefonních hovorů opakovaně varoval nejen NÚKIB, ale také například Česká národní banka, jejíž jméno bylo během jedné z vishingových kampaní zneužíváno.[X] Útočníci v rámci těchto útoků běžně zneužívají jména legitimních institucí. Svoje útoky však nadále zdokonalují a ke zvýšení efektivity využívají například podvržené články, služby Voice over Internet Protokol (VoIP) pro podvržení telefonního čísla nebo nabádají uživatele k instalaci softwaru pro vzdálenou správu. Některé banky zaznamenaly také trend, kdy útočníci začali zneužívat rostoucího zájmu o investice do kryptoměn.[XI]

Velká část finančních institucí se neustále snaží zlepšovat úroveň své kybernetické bezpečnosti. Svědčí o tom mimo jiné skutečnost, že 43 % z nich plánuje v následujícím roce navýšit rozpočet na kybernetickou bezpečnost. **Ve srovnání s ostatními sektory přitom finanční instituce průměrně investovaly do oblasti kybernetické bezpečnosti nejvyšší procento ze svého rozpočtu** (Graf 23). To se odráží také na schopnosti zaplatit potřebné odborníky na kybernetickou bezpečnost. Více jak dvě třetiny finančních institucí nemají problém nabídnout těmto odborníkům dostatečné finanční ohodnocení (Graf 24). Až 90 % respondentů navíc disponuje finančními prostředky na jejich pravidelné školení.

Graf 23: **Jaké procento financí z celkového rozpočtu organizací směřovalo v roce 2021 do nákladů na kybernetickou bezpečnost?** (%)



Graf 24: **Srovnání podílu subjektů z finančního sektoru a ostatních odvětví, pro které byla v roce 2021 úroveň finančního ohodnocení zásadním faktorem odrazujícím uchazeče při náborech na místa v oblasti kybernetické bezpečnosti** (%)



Průmysl a energetika: ransomware jako hlavní hrozba

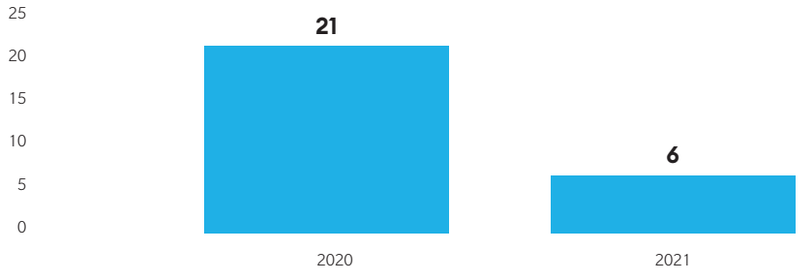
Mezinárodní dění na poli kybernetické bezpečnosti v sektorech průmyslu a energetiky bylo v roce 2021 určováno zejména masivními ransomwarovými útoky s bezprecedentními dopady. Zmínit lze například útok na největšího světového producenta masa JBS Foods, výrobce elektroniky Acer či útok na americkou společnost Colonial Pipeline, který vedl k výpadku dodávek ropných produktů pro východní pobřeží USA (viz box). **K ransomwarovému útoku, který vyústil v zastavení výroby jednoho z dodavatelů pro energetický sektor, došlo v roce 2021 také v České republice.**

Útok na produktovod společnosti Colonial Pipeline

Energetický sektor v USA v roce 2021 poznamenal jeden z dosud největších ransomwarových útoků. Společnost Colonial Pipeline provozující největší síť produktovodů v USA se stala cílem ransomwarové skupiny DarkSide. Útok zasáhl provozní část sítě (účetní systémy), nicméně společnost byla nucena vypnout také systémy v průmyslové síti, což vedlo k zastavení hlavního zdroje dodávek ropných produktů pro celé východní pobřeží USA. Celý případ poukázal na vzájemnou propojenost obchodních a průmyslových procesů, resp. na významnou závislost průmyslové sítě na síti provozní.

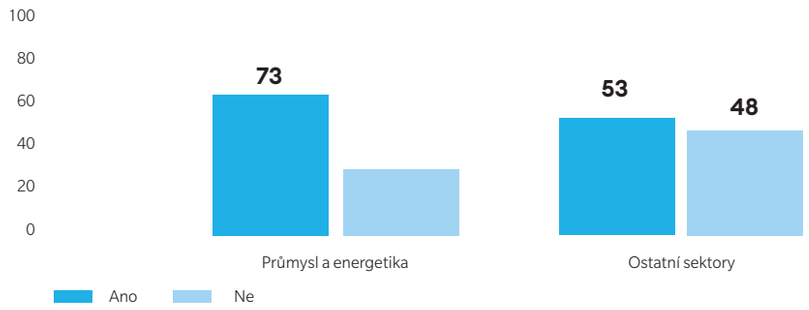
Zajištění kontinuity produkce a poskytování služeb je prioritním cílem pro sektory průmyslu a energetiky. Z tohoto důvodu představuje ransomware pro organizace z těchto sektorů zásadní hrozbu. Odpovídá tomu skutečnost, že **ačkoli ransomwarový útok či pokus o něj v roce 2021 zaznamenalo pouze 6 % respondentů, byl považován za jednu z nejzávažnějších hrozeb.**

Graf 25: **Meziroční srovnání zaznamenaných ransomwarových útoků či pokusů o ně v rámci sektorů průmyslu a energetiky** (%)



Velký důraz na zajištění kontinuity provozu a produkce v rámci sektorů průmyslu a energetiky se promítá také do připravenosti na potenciální incident. V rámci procesů krizového managementu má zahrnutý krizový scénář řešení kybernetického incidentu celkem 73 % dotazovaných průmyslových a energetických společností. Až 97 % respondentů z daných sektorů vytváří off-line zálohy kritických systémů a 78 % je také pravidelně testuje. Téměř 80 % subjektů má zároveň zavedeny procesy Business Continuity Management (BCM). Ve všech výše zmíněných atributech si průmyslový a energetický sektor stojí značně nad průměrem (viz např. Graf 26).

Graf 26: **Pokud má Vaše organizace nastavené procesy krizového managementu, patří mezi krizové scénáře proces řešení kybernetického incidentu?** (%)



Zdravotnictví: mírný pokles ransomwarových útoků a stále nedostatečné finance

Počet incidentů ve zdravotnictví registrovaných NÚKIB se meziročně zvýšil o 34 %, přičemž až polovina incidentů byla hodnocena jako významná či velmi významná.[11] Tento nárůst může do jisté míry souviset s navýšením regulovaných subjektů ve zdravotnictví, které mají povinnost incidenty hlásit (viz box). **Naopak počet zaznamenaných ransomwarových útoků mírně poklesl, což koresponduje s daty dostupnými NÚKIB**. Spolu s tím se snížilo také vnímání závažnosti, kdy ransomware již nebyl považován za nejzávažnější hrozbu. Jako nejzávažnější typy útoků v roce 2021 vnímaly zdravotnické subjekty phishing, spear-phishing a pokusy o zneužití zranitelností.

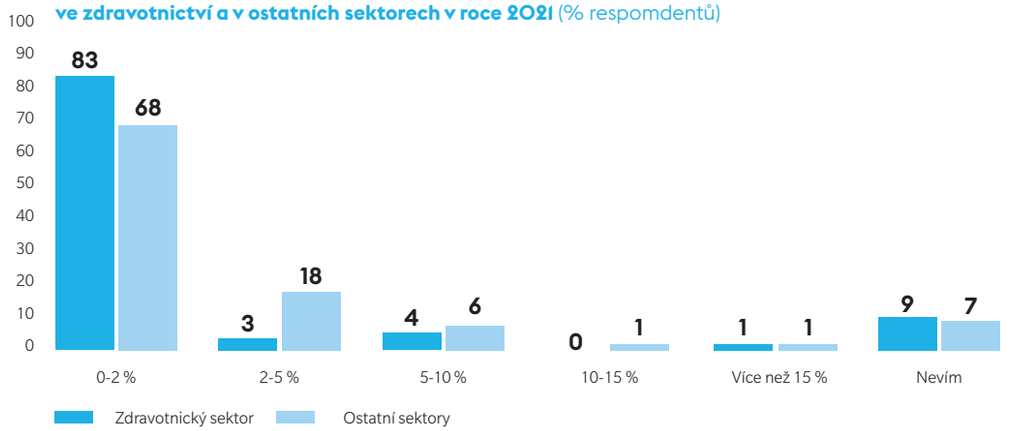
Novela vyhlášky o provozovatelích základních služeb v odvětví zdravotnictví

V reakci na kybernetické incidenty, kterým v roce 2020 čelila zdravotnická zařízení v České republice, vypracoval NÚKIB ve spolupráci s Ministerstvem zdravotnictví novelu vyhlášky č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby, ve znění pozdějších předpisů, která nabyla účinnosti 1. ledna 2021. Účelem této novely bylo změnit určující kritéria v odvětví zdravotnictví tak, aby došlo k rozšíření počtu nemocnic, které jsou určeny jako provozovatelé základních služeb. Krátce po účinnosti novely došlo k zahájení určovacích správních řízení s relevantními nemocnicemi, která díky připravenosti na obou stranách proběhla velmi rychle a bezproblémově. Během roku 2021 bylo určeno celkem 28 nemocnic a počet provozovatelů základních služeb v odvětví zdravotnictví se tak zvýšil na 44.

Celé znění vyhlášky č. 573/2020 Sb., kterou se mění vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby lze nalézt zde: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=39032

Ačkoli se oproti minulému roku u více než třetiny subjektů finanční prostředky alokované na kybernetickou bezpečnost navýšily, u naprosté většiny se pohybovaly v rozmezí 0–2 % z celkového rozpočtu, což je značně pod průměrem ostatních sektorů (Graf 27). **Téměř 70 % respondentů přitom považovalo finance na zajištění kybernetické bezpečnosti za nedostatečné.** Více jak třetina z nich by svůj rozpočet na kybernetickou bezpečnost navýšila o více než sto procent. Navzdory nepříliš příznivému stavu v oblasti financí se 88 % zdravotnických subjektů domnívá, že se úroveň jejich kybernetické bezpečnosti zlepšila.

Graf 27: **Podíl rozpočtu alokovaného na kybernetickou bezpečnost na celkovém rozpočtu ve zdravotnictví a v ostatních sektorech v roce 2021** (% respomdentů)



[11] Závažnost kybernetických incidentů je definována ve vyhlášce č. 82/2018 Sb. a v interní metodice NÚKIB.

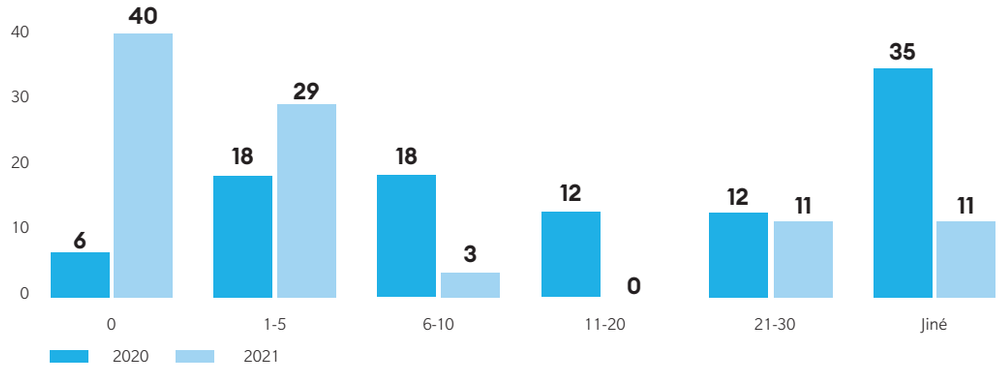
Vzdělávání: několikanásobný nárůst kybernetických incidentů

V roce 2021 došlo ve vzdělávacím sektoru více jak k šestinásobnému nárůstu incidentů evidovaných NÚKIB. Ačkoli v daném roce došlo k navýšení regulovaných subjektů ve školství v důsledku novelizace vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích (viz box), ve znění pozdějších předpisů, tato změna neměla významnější vliv na počet registrovaných incidentů. **Většina incidentů ve vzdělávacím sektoru byla totiž hlášena neregulovanými subjekty.**

> Dne 1. ledna 2021 nabyla účinnosti vyhláška č. 360/2020 Sb., kterou se mění vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, ve znění vyhlášky č. 205/2016 Sb., na jejímž základě mohou do kategorie významných informačních systémů spadat také informační systémy ve školství. NÚKIB v souvislosti s tím vydal podpůrný materiál Významné informační systémy ve školství, který poskytuje odpovědi na nejčastější otázky týkající se identifikace těchto systémů:
>
> https://www.nukib.cz/download/publikace/podpurne_materialy/2021-09-22_VISskoly_ FAQ_v.01.pdf

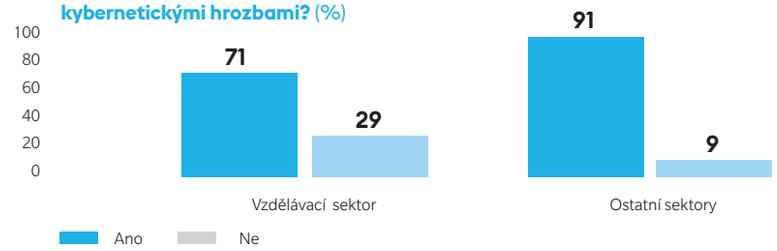
Navzdory vysokému počtu incidentů evidovaných NÚKIB se počet útoků či pokusů o útok zaznamenaných subjekty ve školství spíše snížil (Graf 28). Nelze však vyloučit (25–50 %), že tento pokles může být způsoben nízkou schopností detekce ze strany vzdělávacích institucí či snahou útočníků o udržení nepozorované přítomnosti. Druhý jmenovaný scénář je relevantní zejména pro vysokoškolské instituce, jejichž **akademický výzkum představuje velmi atraktivní cíl pro státem sponzorované skupiny.**

Graf 28: **Meziroční srovnání zaznamenaných útoků či pokusů o ně ve vzdělávacím sektoru v roce 2021** (% respomdentů)



Vzdělávací sektor byl v minulých letech terčem řady phishingových kampaní. V roce 2021 označily vzdělávací instituce phishing za nejčastější a zároveň jeden z nejzávažnějších typů útoku. **Phishingový útok či pokus o něj zaznamenaly více než tři čtvrtiny dotazovaných subjektů**. Vysoká míra těchto útoků zvyšuje nároky na vzdělávání a osvětu zaměstnanců těchto institucí i dalších relevantních uživatelů. Školení uživatelů však provádí pouze 71 % subjektů ve školství, což je o 15 % méně než u ostatních sektorů (Graf 29). Pouze čtvrtina vzdělávacích institucí pak alokuje finance specificky na školení uživatelů.

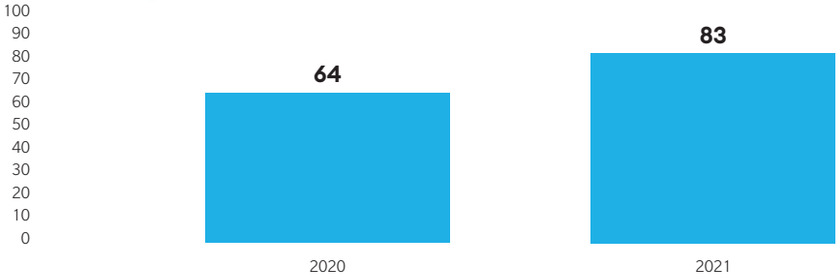
Graf 29: **Školíte uživatele na kybernetickou bezpečnost a seznamujete je s aktuálními kybernetickými hrozbami?** (%)



Digitální služby: rostoucí počet útoků pomocí škodlivých kódů a důraz na řízení rizik spjatých s dodavateli

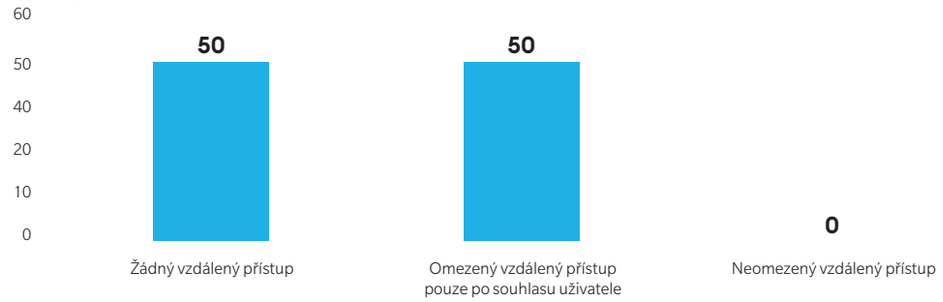
České subjekty poskytující digitální služby (telekomunikace, digitální infrastrukturu, internetové služby apod.) v roce 2021 čelily nejčastěji skenování vnější sítě, phishingu a škodlivým kódům. **Útok pomocí škodlivého kódu či pokus o něj zaznamenalo celkem 83 % organizací, což oproti minulému roku značí téměř pětinový nárůst** (Graf 30). Tento typ útoku měl navíc nadpoloviční zastoupení v incidentech NÚKIB pro daný sektor. I to je nejspíš jeden z důvodů, proč naprostá většina subjektů označila škodlivý kód za nejzávažnější typ útoku.

Graf 30: **Meziroční srovnání zaznamenaných útoků pomocí škodlivého kódu či pokusů o ně v rámci sektoru digitálních služeb** (%)



Instituce a organizace ze sektoru digitálních služeb si uvědomují nutnost zabezpečení dodavatelského řetězce, a proto řídí bezpečnostní rizika spjatá s dodavateli. Všichni respondenti mají stanovená minimální bezpečnostní opatření pro smluvní vztahy a někteří rizika řídí také skrze technická či organizační opatření. Žádný z dotazovaných subjektů neumožňuje svým dodavatelům neomezený vzdálený přístup do svých sítí, polovina umožňuje omezený přístup pouze se souhlasem uživatele (Graf 31). Značný důraz na řízení rizik mezi subjekty poskytujícími digitální služby je pravděpodobně (55—70 %) jedním z faktorů vedoucích k tomu, že celkem 80 % z nich vnímá hrozbu kybernetických útoků skrze dodavatele služeb jako nízkou.

Graf 31: **Jak rozsáhlý přístup do svých sítí udělujete dodavatelům?** (% subjektů v rámci sektoru digitálních služeb)



Opatření

Časová osa opatření a vybraných upozornění NÚKIB v roce 2021

Březen

Reaktivní opatření v souvislosti se zranitelností Microsoft Exchange Server
Na začátku března NÚKIB upozornil na aktivní zneužívání závažných zranitelností postihujících Microsoft Exchange Server. V návaznosti na toto upozornění vydal NÚKIB reaktivní opatření a uložil tak subjektům podléhajícím ZKB povinnost bezodkladně provést příslušné bezpečnostní aktualizace a zároveň prověřit, zda nedošlo ke kompromitaci jejich systémů.
https://www.nukib.cz/download/uredni_deska/Opatreni_obecne_povahy_2021_03_11.pdf

Duben

Upozornění na zvýšené riziko kybernetických útoků proti ČR
Následující měsíc vydal NÚKIB v reakci na vnitrostátní i mezinárodní dění upozornění před zvýšeným rizikem kybernetických útoků proti ČR obsahující analýzu nejčastěji využívaných technik útočníků a nejčastěji zneužívaných zranitelností.
https://www.nukib.cz/cs/infoservis/aktuality/1703-hrozi-zvysene-riziko-kybernetickych-utoku-vuci-ceske-republice/

Květen

Upozornění na kampaň ransomwaru Avaddon
K dalšímu upozornění vedla probíhající kampaň útočníků provozujících ransomware Avaddon, kteří se mj. zaměřovali také na české instituce a organizace. Na začátku června nicméně došlo k ukončení činnosti tohoto ransomwaru.
https://www.nukib.cz/cs/infoservis/hrozby/1717-upozorneni-na-probihajici-kampan-ransomwaru-avaddon/

Srpen

Upozornění na aktivní zneužívání zranitelnosti Microsoft Exchange Server – ProxyShell
V průběhu srpna NÚKIB upozornil na sérii zranitelností postihující Microsoft Exchange Server. Ačkoli zranitelnosti byly opraveny bezpečnostními aktualizacemi vydanými v předešlých měsících, nově je šlo v kombinaci zneužít k útoku zvanému ProxyShell.
https://www.nukib.cz/cs/infoservis/hrozby/1739-upozorneni-na-aktivni-zneuzivani-zranitelnosti-microsoft-exchange-server-proxyshell/

Říjen

Ochranné opatření formou opatření obecné povahy k zabezpečení e-mailových schránek
S cílem zabezpečení komunikace správců a provozovatelů informačních systémů, které jsou klíčové pro fungování státu a bezpečí jeho obyvatel, došlo k historicky prvnímu využití institutu ochranného opatření. Toto opatření uložilo povinným osobám zavedení sady technických opatření k většímu zabezpečení elektronické pošty. Kromě samotného opatření vydal NÚKIB také podrobný metodický návod.
https://www.nukib.cz/download/uredni_deska/2021-10-08_OchranneOpatreni_final.pdf

Listopad

Upozornění na kampaň zneužívající zranitelnosti Exchange Server
Nová vlna zneužívání zranitelnosti Proxyshell k sofistikovanému doručování phishingových zpráv s malwarem vedla k vydání upozornění, které doporučilo všem správcům provozujícím Exchange Server bezodkladnou aktualizaci.
https://www.nukib.cz/cs/infoservis/hrozby/1766-upozorneni-na-kampan-zneuzivajici-zranitelnosti-exchange-server/

Prosinec

Reaktivní opatření v souvislosti se zranitelností Log4Shell
Krátce po upozornění na závažnou zranitelnost v komponentě Apache Log4j, která postihovala velké množství široce používaných produktů a aplikací, přistoupil NÚKIB k vydání reaktivního opatření obsahujícího povinné úkony a metodické pokyny k zabezpečení systémů.
https://www.nukib.cz/download/uredni_deska/2021-12-15_RO-NUKIB-Log4Shell.pdf

Národní úroveň kybernetické bezpečnosti: akční plán a bezpečnost 5G sítí

Akční plán k Národní strategii kybernetické bezpečnosti na období let 2021 až 2025

V červenci 2021 byl vládou schválen **Akční plán**. Ačkoli gestorem jeho zpracování byl NÚKIB, na jeho vzniku se významně podílely všechny veřejné instituce ČR, které sehrávají důležitou roli při zajišťování kybernetické bezpečnosti.

Akční plán představuje implementační část k již schválené Národní strategii kybernetické bezpečnosti ČR. Oba dokumenty jsou úzce propojené a dávají jasnou představu, kam se ČR plánuje v zajišťování kybernetické bezpečnosti v následujících pěti letech ubírat. Akční plán stanovuje na období let 2021 až 2025 celkově 105 úkolů, u nichž uvádí subjekty zodpovědné za jejich realizaci, stejně tak i časový harmonogram jejich plnění. Některé z úkolů jsou nastaveny jako průběžné (např. v oblasti vzdělávání nebo organizaci cvičení), jiné vyžadují komplexnější změny (např. zpracování návrhu národní politiky koordinovaného zveřejňování zranitelností). Vyhodnocení Akčního plánu za rok 2021 lze nalézt v příloze 1 této Zprávy.
Akční plán je veřejně dostupný na webu NÚKIB www.nukib.cz/cs/kybernetickabezpecnost/ strategie--akcni-plan/.

Nastavování bezpečnosti 5G sítí

NÚKIB se v roce 2021 ve spolupráci s dalšími státními institucemi rovněž podílel na nastavování pravidel bezpečnosti 5G sítí, a to prostřednictvím přípravy návrhů pro zavedení některých opatření EU 5G Toolboxu do českého právního řádu. Kromě NÚKIB, který byl iniciátorem a koordinátorem této aktivity, se na ní podíleli také zástupci dalších státních institucí, do jejichž působnosti spadá bezpečnost sítí elektronických komunikací a ochrana bezpečnostních zájmů ČR.
Na základě usnesení Bezpečnostní rady státu připravil NÚKIB ve spolupráci s dalšími státními institucemi možnosti dalšího postupu pro zajištění kybernetické bezpečnosti sítí 5G. Po následném výběru nejvhodnější varianty Bezpečnostní radou státu zpracoval NÚKIB spolu s ostatními zapojenými institucemi koncepci s názvem **„Mechanismus pro posuzování a omezování rizik spojených s dodavateli 5G sítí“**, která by měla být následně rozpracována do věcného záměru zákona.
Po celý rok 2021 se také konala jednání pracovní skupiny pro kybernetickou bezpečnost 5G Aliance, platformy pro pravidelnou komunikaci státu se sektorem telekomunikací, v jejímž rámci byli zástupci sektoru pravidelně informováni o nejnovějším vývoji v oblasti bezpečnosti 5G sítí na národní úrovni.

Čelení hybridnímu působení

Pod koordinací Ministerstva obrany a za spolupráce dalších institucí byla zpracována **Národní strategie pro čelení hybridnímu působení**, která je v českém prostředí první svého druhu. Jejím cílem je reagovat na proměňující se bezpečnostní prostředí a stanovit nástroje potřebné k ochraně životních, strategických a dalších významných zájmů ČR před nepřátelským hybridním působením. Strategie definuje cíle v těchto oblastech:

- **odolná společnost, stát, kritická infrastruktura;**
- **systémový a celostní přístup;**
- **schopnost adekvátní a včasné reakce.**

Strategii lze nalézt na webu https://mocr.army.cz/images/id_40001_50000/46088/N__rodn___strategie_pro___elen___hybridn__mu_p__soben__.pdf

Legislativní ukotvení: nárůst povinných subjektů a změny v oblasti cloud computingu

Určování a přezkum kritické informační infrastruktury, významných informačních systémů a informačních systémů základní služby

Určování a přezkum kritické informační infrastruktury, významných informačních systémů a informačních systémů základní služby Určování KII provádí NÚKIB na základě zmocnění uvedeném v ZKB a v krizovém zákoně,[12] v souladu s nařízením vlády o kritériích pro určení prvku KII, a to již od roku 2015. ZKB také ukládá NÚKIB povinnost ověřovat každé dva roky aktuálnost určení prvků KII. Prvkem KII je pak informační nebo komunikační systém, který naplňuje kritéria daná výše zmíněným nařízením, ta určují jeho důležitost pro zachování vitálních funkcí státu. Správci prvků KII jsou jak organizační složky státu (OSS), tak i soukromé subjekty. **V roce 2021 bylo určeno 8 nových správců KII a zároveň byly přezkoumány již určené prvky KII u 28 správců KII.** NÚKIB tak v současné době eviduje celkem 60 subjektů, které spravují 131 prvků KII.
Dne 1. ledna nabyla účinnosti novela vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejích určujících kritériích, ve znění pozdějších předpisů. U organizačních složek státu a krajů byly zavedeny tzv. typové významné informační systémy, které jsou uvedeny ve výčtu v § 2 odst. 1 zmíněné vyhlášky. Tento paragraf má tzv. dělenou účinnost, a tedy bude nabíhat postupně a každý rok budou přidávány nové typové systémy, dokud v roce 2023 vyhláška nenaběhne do cílového stavu. **V roce 2021 bylo určeno celkem 90 orgánů veřejné moci a 196 významných informačních systémů.**

Odhadovaný nárůst počtu významných informačních systémů v důsledku novely vyhlášky o významných informačních systémech	
Období	Počet nově zařazených systémů
Rok 2022	610
Rok 2023	690
Celkem	690

Proces určování provozovatelů základní služby v roce 2021 probíhal zejména v odvětvích zdravotnictví, energetiky, vodního hospodářství a dopravy. **Celkem bylo provozovatelem základní služby nově určeno 70 subjektů, přičemž 51 správních řízení bylo ukončeno rozhodnutím o neurčení.** Ke konci roku 2021 tak byl celkový počet určených provozovatelů základní služby, resp. správců informačních systémů základní služby 124 a informačních systémů základní služby 147.

Počet určených subjektů ke konci roku 2021:

- **správci a provozovatelé informačních a komunikačních systémů kritické informační infrastruktury: 60 subjektů;**
- **informační a komunikační systémy kritické informační infrastruktury: 131 informačních a komunikačních systémů;**
- **správci a provozovatelé významných informačních systémů: 162 subjektů;**
- **významné informační systémy: 372 informačních systémů;**
- **správci a provozovatelé informačních systémů základní služby: 124 subjektů;**
- **informační systémy základní služby: 147 informačních systémů.**

[12] Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů, v souladu s nařízením vlády č 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, ve znění pozdějších předpisů.

Legislativní změny v oblasti cloud computingu a posuzování splnění bezpečnostních kritérií

Ministerstvo vnitra od srpna 2020 posuzuje poskytovatele a služby cloud computingu. Do tohoto posuzování je NÚKIB výrazně zapojen. NÚKIB v této oblasti provádí posouzení splnění bezpečnostních kritérií, která musejí poskytovatelé cloud computingu splnit, aby mohli dodávat služby veřejné správy. Do konce roku 2021 v této oblasti NÚKIB vydal již celkem 145 stanovisek.

V roce 2021 došlo k významným legislativním změnám spojeným s problematikou cloud computingu:

- novela zákona o informačních systémech veřejné správy upravila a upřesnila proces posuzování poskytovatelů cloud computingu a jednotlivých služeb cloud computingu v případě, že jsou poskytovány orgánům veřejné správy;
- vyhláška č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci definuje kritéria pro zařazování informačních a komunikačních systémů orgánů veřejné moci do bezpečnostních úrovní;
- vyhláška č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu, blíže rozvádí požadavky, které musí poskytovatelé cloud computingu naplnit, aby mohli být spolu se svými nabízenými službami zapsáni v katalogu cloud computingu.

Během roku 2021 NÚKIB posoudil ještě čtyři poskytovatele dle požadavků stanovených vyhláškou č. 316/2021. V roce 2021 nebyl dle požadavků stanovených vyhláškou posouzen žádný cloud computing, protože NÚKIB neobdržel žádnou žádost o posouzení cloud computingu oproti požadavkům stanovených vyhláškou. To je dáno tím, že nejdříve musí dojít k posouzení poskytovatele a až následně je možné podat žádost o posouzení cloud computingu.

Konzultace, workshopy a podpůrné materiály NÚKIB

V roce 2021 proběhla řada konzultací týkajících se implementace zákona o kybernetické bezpečnosti. Kromě individuálních konzultací proběhly také workshopy k problematice identifikace významných informačních systémů, kterých se zúčastnilo 246 osob z 68 státních organizací. NÚKIB i nadále pokračuje ve vydávání veřejných podpůrných materiálů určených jak povinným osobám spadajícím pod ZKB, tak odborné veřejnosti. Mezi materiály vydané či aktualizované v roce 2021 patří například:

- **pravidla určování kritické informační infrastruktury;**
- **požadavky na smlouvy s dodavateli;**
- **provozovatel informačního nebo komunikačního systému;**
- **průvodce zařazením poptávaného cloud computingu do bezpečnostní úrovně.**

K poměrně velké aktualizaci došlo také v oblasti FAQ na internetových stránkách NÚKIB, která nyní obsahuje více informací a odpovědí na dotazy, se kterými se NÚKIB setkává:
https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/faq/.

Dozorová činnost NÚKIB v roce 2021

Rok 2021 byl z pohledu kontrolní a auditní činnosti NÚKIB ovlivněn zejména mapováním stavu kybernetické bezpečnosti u nejvýznamnějších zdravotnických zařízení v ČR. **Počet kontrol** či **auditů** podle ZKB, respektive jeho prováděcí vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „VKB"), **se v roce 2021 zvýšil z 8 na 22**. Kontrola či audit u povinných orgánů a osob podle § 3 ZKB ověřuje plnění povinností plynoucích ze ZKB a VKB. V rámci každé kontroly nebo auditu je rámcově ověřováno cca 150 kontrolních bodů.

Kromě sektoru zdravotnictví se NÚKIB v roce 2021 zaměřil i na další subjekty jako například na prověření systému zajišťujícího zpracování a prezentaci výsledků voleb u Českého statistického úřadu. NÚKIB provedl tzv. komplexní audit zahrnující cvičné phishingové kampaně, skenování zranitelností, provedení interních a externích penetračních testů či zátěžových testů. Součástí komplexního auditu bylo také table-top cvičení, díky kterému měl Český statistický úřad možnost procvičit svoji připravenost na krizové situace při zpracování a prezentaci výsledků voleb včetně mediální linky. V neposlední řadě také proběhl audit souladu systému s požadavky VKB.

Spolupráce NÚKIB s dalšími dozorovými orgány v oblasti kontroly za rok 2021

NÚKIB i v roce 2021 dále rozvíjel spolupráci v kontrolní činnosti s dalšími regulátory. Jmenovitě například s Úřadem pro civilní letectví, se kterým bylo v lednu podepsáno memorandum o spolupráci nejen v oblasti kontroly. Praktická spolupráce v oblasti kontroly se rozvinula i s Českou národní bankou při společné kontrole, kde byli zaměstnanci NÚKIB součástí kontrolní skupiny v pozici přizvané osoby. Důležitým cílem spolupráce mezi NÚKIB a spolupracujícími úřady v oblasti kontroly je především snaha minimalizovat zátěž povinných orgánů a osob.

V průběhu kontrolní a auditní činnosti jsou nejčastěji identifikovány nedostatky v těchto oblastech:

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

Cvičení kybernetické bezpečnosti: nové zkušenosti na národní i mezinárodní úrovni

Rok 2021, ač stále ovlivněn epidemickou situací, se nesl ve znamení návratu k fyzickému konání cvičení a dalších aktivit. NÚKIB proto směřoval své úsilí jak na přípravu nových cvičení, tak na organizaci těch, které se v roce 2020 uskutečnit nemohla.

Národní cvičení	Mezinárodní cvičení
9	**5**

Úspěchem v tomto ohledu bylo zejména uspořádání Health Czech, historicky prvního sektorového cvičení kybernetické bezpečnosti ve zdravotnictví. Mezi účastníky byli zástupci z celkem 16 nemocnic, jejichž týmy byly sl ženy z pracovníků IT, odborníků na (kybernetickou) bezpečnost, ale také právníků, tiskových mluvčích a pracovníků léčebně preventivní péče. Cílem cvičení bylo zapojit všechny tyto rozdílné role a přispět tak k jejic vzájemné spolupráci a společnému náhledu a přístupu ke kybernetické bezpečnosti. Poznatky získané při konání Health Czech budou uplatněny také při dalším cvičení určeném pro zdravotnický sektor, které se bude konat v roce 2022.

Výhled budoucího směřování cvičení kybernetické bezpečnosti:

Vzhledem k narůstajícímu počtu regulovaných subjektů a poptávky po cvičeních, se jako nejvhodnější jeví cesta sektorových cvičení zahrnujících větší počty relevantních účastníků. Další směřování lze spatřovat také v zaměření na koncept **„train-the-trainer"**, kdy odborníci z NÚKIB mohou předávat své know-how a best practices odborníkům z jednotlivých subjektů tak, aby byli schopni vytvořit si cvičení co nejvíce na míru své organizaci. Konzultace k vytváření cvičení, o které byl NÚKIB v loňském roce požádán, proto budou v rámci dostupných kapacit pokračovat i v následujícím období.

V roce 2021 proběhlo také několik cvičení kybernetické bezpečnosti s mezinárodním přesahem. Prvním z nich bylo největší cvičení kybernetické bezpečnosti na světě s názvem Locked Shields 2021. Toto cvičení se vůbec poprvé ve své historii konalo vzdáleně a většina organizátorů, mezi něž patřili mj. zástupci NÚKIB, i samotní účastníci cvičení tak museli své úkoly řešit prostřednictvím online kolaboračních a komunikačních platforem. Vzdálený formát s sebou přinesl řadu cenných zkušeností a otestoval schopnost spolupráce jak na vnitrostátní, tak na mezinárodní úrovni. Cvičení bylo zaměřeno na ochranu civilních i armádních IT systémů a systémů kritické infrastruktury a zahrnovalo nejen technickou část, ale mělo také právní, komunikační a analytický rozměr. **Národní tým České republiky tvořený zástupci NÚKIB a dalších státních složek, soukromého sektoru i akademické sféry se umístil na 3. místě z 22 týmů a navázal tak na úspěšné výsledky z minulých let.**

Umístění ČR na cvičení Locked Shields během posledních 5 let				
2017	2018	2019	2020	2021
1.	3.	2.	zrušeno	3.

Dalšími mezinárodními cvičeními, které se v minulém roce uskutečnily, byly Cyber Coalition a CRISIS-X. Cvičení Cyber Coalition je mezinárodní cvičení kybernetické bezpečnosti pořádané Severoatlantickou aliancí. Na úrovni České republiky je toto cvičení koordinováno NÚKIB za civilní část a VeKySIO za část vojenskou. Samotný název cvičení podtrhuje jeho cíl – podporu silného společenství a vzájemné spolupráce. Toho je docíleno pomocí scénářů, které se zaměřují jak na řešení technických výzev, tak na podnícení jednotlivých států ke spolupráci a k vytvoření společného situačního povědomí. CRISIS-X bylo historicky prvním společným cvičením NÚKIB a Israel National Cyber Directorate (INCD), v jehož rámci si týmy jednotlivých úřadů prověřili nejen schopnost zvládání incidentů na národní úrovni, ale také vzájemnou komunikaci se svým protějškem.

Významné poznatky ze cvičení v posledních letech:

- **Metodické a další podpůrné materiály vytvořené NÚKIB v návaznosti na nové či novelizované právní normy a vydaná opatření jsou přínosné a relevantním zaměstnancům mnoha subjektů poskytují užitečnou podporu při implementaci výše zmíněného.**
- **Častým problémem v zajišťování kybernetické bezpečnosti je problematika chybějících financí a lidských zdrojů. Dostatek finančních zdrojů však nemusí zajistit dostatečně kvalifikovaný personál, jehož je v ČR nedostatek.**
- **Subjekty si stále více uvědomují, že vzdělávání řadových zaměstnanců je klíčové pro zajišťování kybernetické bezpečnosti.**

Osvěta a vzdělávání v ČR: zaměření na cílové skupiny i širší veřejnost

Vzdělávání a osvěta v oblasti kybernetické bezpečnosti zůstaly důležitými celospolečenskými tématy. I nadále v důsledku epidemiologické situace rostla potřeba vyrovnat se s bezpečnostním aspektem vyšší míry zapojení digitálních technologií do všech oblastí života společnosti. To s sebou neslo zvýšené nároky na připravenost občanů ČR k bezpečnémupoužívání digitálních technologií a pohybu v online světě napříč všemi sociálními skupinami jak při výkonu pracovních činností, tak při studiu apod.
Zvyšování úrovně povědomí zaměstnanců veřejné správy a povinných organizací o problematice kybernetické bezpečnosti probíhalo podobně jako v minulých letech prostřednictvím kurzu základů kybernetické bezpečnosti (**Dávej kyber!**) a kurzu určeného pro odborníky na kybernetickou bezpečnost (**Šéfuj kyber!**).
Vyšší pozornost byla v loňském roce věnována vzdělávání a osvětě v sektoru zdravotnictví. NÚKIB připravil a v průběhu jara 2021 spustil online kurz základů kybernetické bezpečnosti pro zaměstnance ve zdravotnictví (**Kyber nemocnice!**). Na základě zpětné vazby z nemocnic NÚKIB reagoval také na potřeby vzdělávání zdravotnického personálu, který digitální zařízení a informační technologie používá pouze na základní uživatelské úrovni, a vytvořil pro něj kurz **Startuj kyber!** Kurz základů rizikového chování na internetu **Bezpečně v kyber!**, jenž je primárně určen pro pracovníky vzdělávání a prevence, pedagogy a ředitele škol, byl nově otevřen také pro laickou veřejnost.

Počet uživatelů, kteří absolvovali kurzy NÚKIB	
Dávej kyber!	26 146
Šéfuj kyber!	441
Kyber nemocnice!	4 407
Bezpečně v kyber!	2 841

Velké úsilí směřovalo v roce 2021 také na osvětu a vzdělávání na mateřských, základních, středních a vysokých školách. V loňském roce tak v tomto směru došlo k realizaci následujících aktivit a projektů:

- NÚKIB zveřejnil nový **rozcestník osvětových materiálů pro školy** s materiály vhodnými pro šíření osvěty kybernetické bezpečnosti ve školní výuce na úrovni mateřských, základních i středních škol.
- NÚKIB se zapojil do podpory tvorby knihy **„Kyberpohádky“**, jež je zaměřená na různá nebezpečí, které mohou děti v kybernetickém světě potkat. Autorem projektu je Centrum kybernetické bezpečnosti, z. ú.
- NÚKIB vytvořil ve spolupráci s ENISA speciální **sérii vzdělávacích příspěvků**, které byly po celý říjen sdíleny prostřednictvím instagramového účtu **@petr.vytrzny** v rámci Evropského měsíce kybernetické bezpečnosti. Na příspěvky bylo více než 3 500 reakcí.
- Safer Internet Centrum distribuovalo ve spojení se společností Zásilkovna **nástěnky bezpečného internetu** do všech základních škol v České republice. Distribuci podpořil NÚKIB a Ministerstvo školství, mládeže a tělovýchovy.
- Do 200 škol byly rozmístěny **interaktivní panely Ámos Vision**, kde mají žáci možnost vyzkoušet si vzdělávací aktivity NÚKIB ke kybernetické bezpečnosti.
- Vzdělávací aktivity **Digitální stopa: Příběh Báry a Digitální stopa: Příběh Svůďáka** prošly aktualizací a rozšíření o aktuální témata kybernetické bezpečnosti. Druhý z jmenovaných kurzů byl ve spolupráci s iniciativou EduKids přepracován do podoby chatbota. Za první měsíc provozu jej využilo přes 3 900 uživatelů.

- NÚKIB ve spolupráci se Smíchovskou střední průmyslovou školou a řadou známých influencerů vytvořil osvětový **videokurz** NÚKIB pro žáky základních a středních škol s názvem **Jsem netvor, tvor, který žije na netu!**, který žáky seznamuje s nástrahami světa digitálních technologií.
- NÚKIB připravil **videokurz Jsem netvor na střední** pro neinformatické obory středních škol k šíření osvěty kybernetické bezpečnosti.
- Do **6. ročníku národní soutěže v kybernetické bezpečnosti** organizovaného AFCEA ČR se přihlásilo téměř 400 škol a 5 500 studentů z celé republiky.
- V rámci **konference CyberCon** proběhl první ročník veletrhu studijních příležitostí Studuj kyber! určený pro všechny žáky základních škol a studenty středních škol. Veletrh měl za úkol představit školy a obory zaměřené na kybernetickou a informační bezpečnosti a informační technologie.
- NÚKIB nadále rozšiřoval spolupráci s vysokými školami, které připravují odborníky kybernetické bezpečnosti. NÚKIB podepsal memorandum o spolupráci s Univerzitou obrany v oblasti vzdělávání specialistů kybernetické bezpečnosti.

V roce 2021 proběhla také řada osvětových a vzdělávacích aktivit určených pro širší veřejnost:

- Významnou událostí byl **7. ročník evropského finále European Cyber Security Challenge** v Praze organizovaného Českou pobočkou AFCEA ve spolupráci s ENISA. Finále se zúčastnilo 163 soutěžících z 19 zemí. Součástí byly doprovodné akce, bilaterální a multilterální jednání a odborná konference věnovaná problematice kybernetické bezpečnosti a umělé inteligence.
- Pod taktovkou Masarykovy univerzity vznikl kurz **„Příběhy sociálního inženýrství“** zaměřený na podvodnou komunikaci, techniky sociálního inženýrství a způsoby, jak se jim bránit.
- Proběhla osvětová **„Kyberkampaň“** zaměřená na phishing (vishing), která vznikla ve spolupráci Policie ČR, České bankovní asociace a společnosti ESET, jejíž součástí je interaktivní tréninkový nástroj „Kybertest“ sloužící k nácviku odhalení podvodné komunikace.
- Úspěšným projektem byl **kurz kybernetické bezpečnosti pro seniory**, který společnými silami realizoval kybernetický tým a Univerzita třetího věku Masarykovy univerzity.
- V uplynulém roce byly dostupné také kurzy **Sherlock senior** od společnosti Seznam.cz, zaměřený na mediální vzdělávání seniorů, a **Digitální Odysea** od společnosti Vodafone, jehož cílem je poskytnout základní informace o používání chytrých telefonů i tabletů a lépe tak adaptovat seniory na dnešní dobu, v níž se stále více služeb digitalizuje.

Konference CyberCon 2021

V září 2021 NÚKIB uspořádal již sedmý ročník konference CyberCon Brno. Hlavním cílem konference je poskytnout prostor pro propojení veřejného, akademického a soukromého sektoru v oblasti kybernetické bezpečnosti. Během třídenního programu konference si přes 300 účastníků z řad odborné i široké veřejnosti mohlo poslechnout rozličné příspěvky reflektující technické, právní, politické aspekty kybernetické bezpečnosti v podání 37 domácích i zahraničních řečníků. Sedmý ročník CyberConu se oproti předešlým v mnohém lišil. Největší změnou bylo rozšíření konference o mezinárodní den probíhající v anglickém jazyce, jenž zahrnoval debaty o novelizaci směrnice NIS, Cyber law toolkitu či problematice kvantové výpočetní techniky. V rámci CyberConu byl také zahájen projekt „Protecting the Healthcare Sector from Cyber Harm“. Součástí konference byl i doprovodný program, který zahrnoval například veletrh studijních příležitostí Studuj kyber!, technický workshop či ukázku table-top cvičení kybernetické bezpečnosti. Více informací o konferenci lze nalézt na webu www.cybercon.cz.

Mezinárodní spolupráce: aktivní zapojení ČR nejen na evropské úrovni

Vývoj regulačních a koordinačních 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 ITU, zastupuje NÚKIB společně s Ministerstvem zahraničních věcí, Ministerstvem obrany a dalšími partnery.[13]
V roce 2021 se na unijní úrovni soustředili zástupci ČR především na jednání ohledně **revize směrnice NIS, sondážních rozhovorů k možné revizi aplikace opatření**[14] **ze Cyber Diplomacy Toolboxu**[15] či na prvotní jednání k iniciativě **Společné kybernetické jednotky (tzv. JCU**). V rámci OSN se i v uplynulém roce konala zasedání tzv. Otevřené pracovní skupiny k bezpečnosti informačních a komunikačních technologií (OEWG), na jejíž činnosti se NÚKIB s Ministerstvem zahraničních věcí aktivně podílejí. V roce 2021 se na zasedání OEWG členským státům podařilo najít shodu a přijmout Závěrečnou věcnou zprávu, která obsahuje doporučení v oblasti problematiky stávajících a vznikajících kybernetických hrozeb, mezinárodního práva, opatření pro budování důvěry či budování kapacit.

Prague 5G Security Conference a Prague Proposals

NÚKIB uspořádal ve spolupráci s Ministerstvem zahraničních věcí a pod záštitou Úřadu vlády na přelomu listopadu a prosince 2021 **třetí ročník Prague 5G Security Conference**. Tento ročník konference, konající se kvůli pandemickým opatřením hybridní formou, se zaměřil na otázky spojené s bezpečností 5G sítí a přelomových technologií (Emerging Disruptive Technologies, EDTs). V průběhu konference vystoupilo téměř sedmdesát řečníků z Evropy i celého světa (např. z Izraele, Koreje, Japonska, Austrálie, USA, Kanady či Indie). Na konferenci nechyběli zástupci veřejného, akademického, neziskového, ale i soukromého sektoru. Dvoudenní konference byla rozdělena na několik tematických panelů, kterých se virtuálně zúčastnily stovky mezinárodních posluchačů.
Na závěr konference byly představeny tzv. Pražské návrhy týkající se kybernetické bezpečnosti přelomových technologií (**„Prague Proposals on Cyber Security of EDTs“**). Zúčastněné země se v nich shodly na možných principech budoucího přístupu k přelomovým technologiím. Dokument zmiňuje například důležitost zohlednění technických i netechnických rizik, bezpečnosti dodavatelského řetězce, transparentnosti, důvěryhodnosti a diverzifikace i demokratických a etických hodnot při rozvoji nových technologií. Výsledkem třetího ročníku jsou dále i druhé Pražské návrhy, které se týkají diverzity dodavatelů telekomunikací (**„Prague Proposals on Telecommunications Supplier Diversity“**).

Nově představené Pražské návrhy:

- **Prague Proposals on Cyber Security of EDTs**
  https://www.nukib.cz/download/Prague_Proposals_on_Cyber_Security_of_EDTs.pdf
- **Prague Proposals on Telecommunications Supplier Diversity**
  https://www.nukib.cz/download/Prague_Proposals_on_Telecommunications_Supplier_Diversity.pdf

[13] Ministerstvo průmyslu a obchodu, Český telekomunikační úřad a další.
[14] Soubor nástrojů pro společnou diplomatickou reakci EU na nepřátelské činnosti v kyberprostoru.
[15] Iniciativa Evropské komise usilující o posílení spolupráce mezi orgány, institucemi a jinými subjekty EU a orgány členských států v případech, kdy by různé kybernetické komunity měly úzce spolupracovat v boji proti závažným přeshraničním kybernetickým incidentům nebo hrozbám.

Revize směrnice NIS a příprava českého předsednictví v Radě EU

Česká republika se v roce 2021 zapojila do naplňování konkrétních iniciativ Strategie kybernetické bezpečnosti EU. Strategie spolu s návrhem revize směrnice NIS představují klíčové dokumenty ukotvující politické a legislativní směrování kybernetické bezpečnosti v EU.

Revize směrnice NIS

Návrh revize směrnice NIS má zásadním způsobem rozšířit sektory subjektů povinných osob, přičemž by mělo dojít i ke sjednocení způsobu jejich identifikace. Dále by měl upravovat koordinované odhalování zranitelností, sjednotit by se měl způsob identifikace povinných osob a mají vzniknout také nové povinnosti v hlášení incidentů, a to s cílem dosažení větší harmonizace právních předpisů a přístupu členských států v oblasti kybernetické bezpečnosti.
Koncem roku 2021 došlo k přijetí obecného přístupu Rady EU (tj. společné pozice členských států EU) a úspěšné dokončení vyjednávání o konečné podobě návrhu je prioritou i pro rok 2022.

NÚKIB v roce 2021 rovněž naplno zahájil přípravu historicky druhého předsednictví ČR v Radě EU, které ČR převezme po Francii v červenci roku 2022. V průběhu roku 2021 se proto zástupci ČR účastnili přípravných a koordinačních jednání, jež jsou stěžejní pro úspěšnou organizaci i průběh samotného předsednictví. Tato jednání probíhala nejen vnitrostátně, ale také s unijními institucemi a v neposlední řadě i s Francií a Švédskem, s nimiž ČR tvoří tzv. předsednické trio.

Výhled trendů v kybernetické bezpečnosti v ČR na roky 2022 a 2023

1. Ransomware
Využívání vyděračského malwaru bude téměř jistě (90–100 %) představovat jednu z nejvýznamnějších kybernetických hrozeb i v následujících dvou letech. Nastupující trendy RaaS a vícenásobných vydírání budou v období následujících dvou let téměř jistě (90–100 %) dále sílit. S nástupem nyní dominantního RaaS modelu a postupným slábnutím pandemie viru covid-19 můžeme pozorovat mírný ústup trendu ransomwarových útoků na zdravotnický sektor, a namísto něj lze sledovat vysoce sofistikované útoky proti velkým a lukrativním ekonomickým subjektům. Tento trend bude v následujícím období velmi pravděpodobně (75–85 %) dál pokračovat. Mimo to pravděpodobně (55–70 %) dojde k dalšímu vývoji a inovacím v rámci modelu RaaS.

2. Zranitelnosti
Trend plošného zneužívání nově zveřejněných závažných zranitelností bude velmi pravděpodobně (75–80 %) pokračovat i v následujících letech. Rychlost, s jakou si útočníci přidávají nové zranitelnosti do svých nástrojů, se stále zvyšuje. V případě Log4Shell útočníci začali zranitelnost zneužívat ke svým útokům již během prvních 24 hodin od jejího zveřejnění. Na zneužívání zranitelností se budou velmi pravděpodobně (75–85 %) podílet nejen státní aktéři, ale také kyberkriminální skupiny, zejména ransomwarové gangy. Tento trend se v následujících letech pravděpodobně (55–70 %) dotkne také českých institucí a organizací a zvýší nároky na efektivní řízení zranitelností.

3. Phishing, spear-phishing a podvodné e-maily
Je téměř jisté (90–100 %), že ČR bude nadále čelit phishingovým a spear-phishingovým kampaním. Tyto metody stále představují jeden z nejefektivnějších způsobů, jak proniknout do systému obětí, a jsou proto hojně využívány škodlivými aktéry. Velmi pravděpodobně (75–85 %) bude dále narůstat i jejich sofistikovanost. Vzhledem k postupnému ústupu pandemie pravděpodobně (50–70 %) dojde k poklesu zneužití koronavirových témat. V minulém období se v České republice vyskytly také vishingové kampaně a je velmi pravděpodobné (75–85 %), že v následujícím období bude těchto útoků přibývat.

4. Útoky na dodavatelský řetězec
Dodavatelské řetězce výpočetních technologií soustavně nabírají na komplexitě a tento trend bude téměř jistě (90–100 %) pokračovat. Pro útočníky tyto komplexní struktury představují cestu, jak potenciálně kompromitovat velké množství obětí, čehož využívají nejen státní aktéři, ale stále častěji také kyberkriminální aktéři. Útoky na dodavatelský řetězec proto jako globální trend budou v následujícím období velmi pravděpodobně (75–85 %) nabírat na síle a je pravděpodobné (50–70 %), že jejich široké dopady mohou zasáhnout i subjekty v České republice.

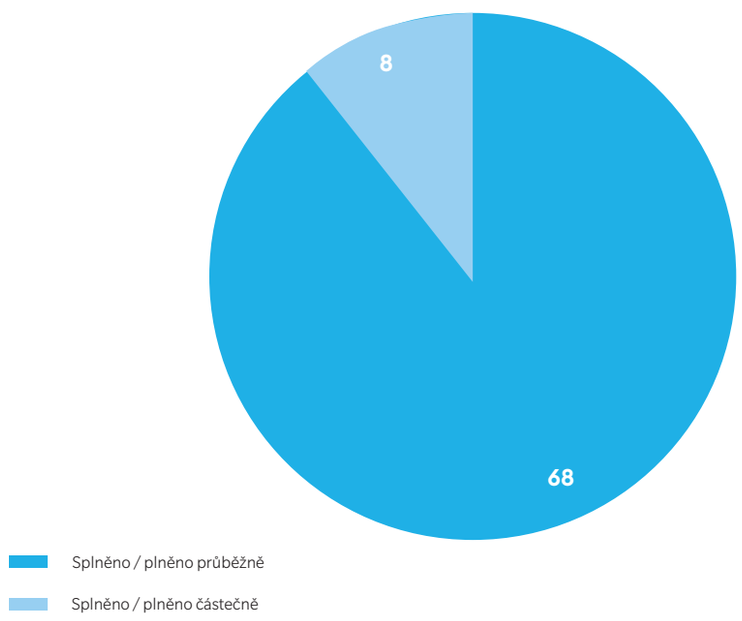
5. Kybernetické útoky proti strategickým institucím státu
Státní sektor, včetně jeho strategických institucí, dlouhodobě patří k častým cílům kybernetických zločinců i státních aktérů. Jelikož někteří státem zaštítění aktéři mohou mít zvláštní zájem cílit na české instituce kvůli geopolitickým postojům ČR vůči vybraným zahraničněpolitickým a bezpečnostním tématům, může pravděpodobnost útoku ovlivnit také vývoj na mezinárodní scéně. Kromě toho existuje reálná možnost (25–50 %), že některé z ústředních orgánů státní správy jsou dlouhodobým cílem kompromitace s persistencí útočníků. NÚKIB odhaduje, že trend závažných kybernetických útoků proti státním strategickým institucím se v následujícím období velmi pravděpodobně (75–85 %) projeví i v ČR.

Příloha: Naplňování Akčního plánu k Národní strategii kybernetické bezpečnosti na období let 2021 až 2025

Rok 2021 byl prvním rokem vyhodnocování Akčního plánu. NÚKIB nejenže koordinuje vyhodnocení celého Akčního plánu, ale podílí se z pozice gestora / spolupracujícího subjektu na plnění 101 z celkových 105 úkolů. **Pro rok 2021 bylo předmětem vyhodnocení 76 úkolů, přičemž 71 je v režimu průběžného plnění.**
Téměř 90 % hodnocených úkolů bylo splněno nebo je plněno průběžně. Pouze 8 úkolů bylo splněno či naplněno částečně, za nesplněný nebyl vyhodnocen žádný z úkolů (Graf 32). Příkladem úkolu, který byl terminován a splněn v roce 2021, je analýza právních možností rychlého operativního nákupu technických nebo programových prostředků k nasazení protiopatření v období krizových stavů. NÚKIB za připomínkování a konzultací od Ministerstva vnitra a Ministerstva pro místní rozvoj zpracoval interní souhrnný materiál. Z něj vyplynulo, že právní řád umožňuje reagovat na specifika jednotlivých situací a zohlednit při výběru dodavatele veřejné zakázky případnou časovou tíseň nebo potřebu chránit bezpečnostní zájmy státu, a není tak třeba přistupovat ke změně legislativy.

Vliv na plnění mnoha úkolů měla i nadále pandemie covidu-19 a na ni navázaná opatření. Ta totiž do značné míry limitovala osobní součinnost, která je důležitou podmínkou ke splnění mnoha úkolů. Takovým příkladem může být úkol vytvořit ucelenou národní pozici ČR k interpretaci stávajícího mezinárodního práva v oblasti kybernetické bezpečnosti a obrany. Prezenční jednání pracovní skupiny, která má tuto národní pozici vytvářet, byla vlivem pandemických opatření obnovena až na podzim roku 2021, a nedošlo tak ke zpracování ucelené národní pozice. U řady úkolů se však aktéři dokázali přizpůsobit pandemickým opatřením a efektivně docházelo k jejich plnění distanční formou, jako tomu bylo například u cvičení Locked Shields 2021. Na částečně splněných a částečně plněných úkolech se bude pracovat i v roce 2022, aby došlo k jejich plnohodnotnému naplnění.

Graf 32: **Vyhodnocení úkolů Akčního plánu za rok 2021**



Zdroje

I **Lupa.cz. 2021. IT systémy Prahy a dalších státních úřadů byly napadeny kybernetickým útokem.**
https://www.lupa.cz/aktuality/it-systemy-prahy-byly-napadeny-kybernetickym-utokem-servery-jsou-odstaveny/

II **NÚKIB. 2022. Měsíc od vydání reaktivního opatření ke zranitelnosti Log4Shell: NÚKIB plošné zneužívaní v ČR neeviduje, přesto obezřetnost zůstává na místě.**
https://www.nukib.cz/cs/infoservis/aktuality/1794-mesic-odvydani-reaktivniho-opatreni-ke-zranitelnosti-log4shell-nukib-plosne-zneuzivani-v-cr-neeviduje-prestoobezretnost-zustava-na-miste/

III **The MITRE Corporation. 2021. Exploit Public-Facing Application**.
https://attack.mitre.org/techniques/T1190/

IV **CrowdStrike. 2021. Ransomware as a Service (RaaS) explained.**
https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/

V **iROZHLAS. 2021. Olomoucký magistrát čelí několik týdnů hackerským útokům. Odmítá zaplatit výkupné.**
https://www.irozhlas.cz/zpravy-domov/olomouc-magistrat-hackersky-utok-hackeri-ransomware-avaddon_ 2105221133_ako

VI **NÚKIB. Zpráva o stavu kybernetické bezpečnosti ČR za rok 2020.**
https://www.nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_KB_2020.pdf;
NÚKIB. Zpráva o stavu kybernetické bezpečnosti ČR za rok 2019.
https://www.nukib.cz/download/publikace/zpravy_o_stavu/NUKIB_ZSKB_2019.pdf

VII **Accenture. 2020. 2020 Cyber Threatscape Report.**
https://www.accenture.com/_acnmedia/PDF-136/Accenture-2020-Cyber-Threatscape-Full-Report.pdf

VIII **Securelist. 2021. APT annual review 2021.**
https://securelist.com/apt-annual-review-2021/105127/

IX **Policie České republiky. 2022. Vývoj registrované kriminality v roce 2021.**
https://www.policie.cz/clanek/vyvojregistrovane-kriminality-v-roce-2021.aspx

X **Česká národní banka. 2021. Vishing: Upozorňujeme na telefonáty zneužívající jméno ČNB.**
https://www.cnb.cz/cs/dohled-financni-trh/ochrana-spotrebitele/upozorneni/Vishing-Upozornujeme-natelefonaty- zneuzivajici-jmeno-CNB/

XI **Moniová, Eva. 2021. Spořitelna varuje před dalším útokem. Lidé naživo sledují, jak jsou okrádáni.**
https://www.seznamzpravy.cz/clanek/sporitelna-varuje-pred-dalsim-utokem-nachytaly-se-uz-desitky-lidi-174563

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;**
- **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;**
- **pořádání tréninků a kybernetických cvičení na národní i mezinárodní úrovni;**
- **analýzy trendů v oblasti kybernetické bezpečnosti;**
- **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.

NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost