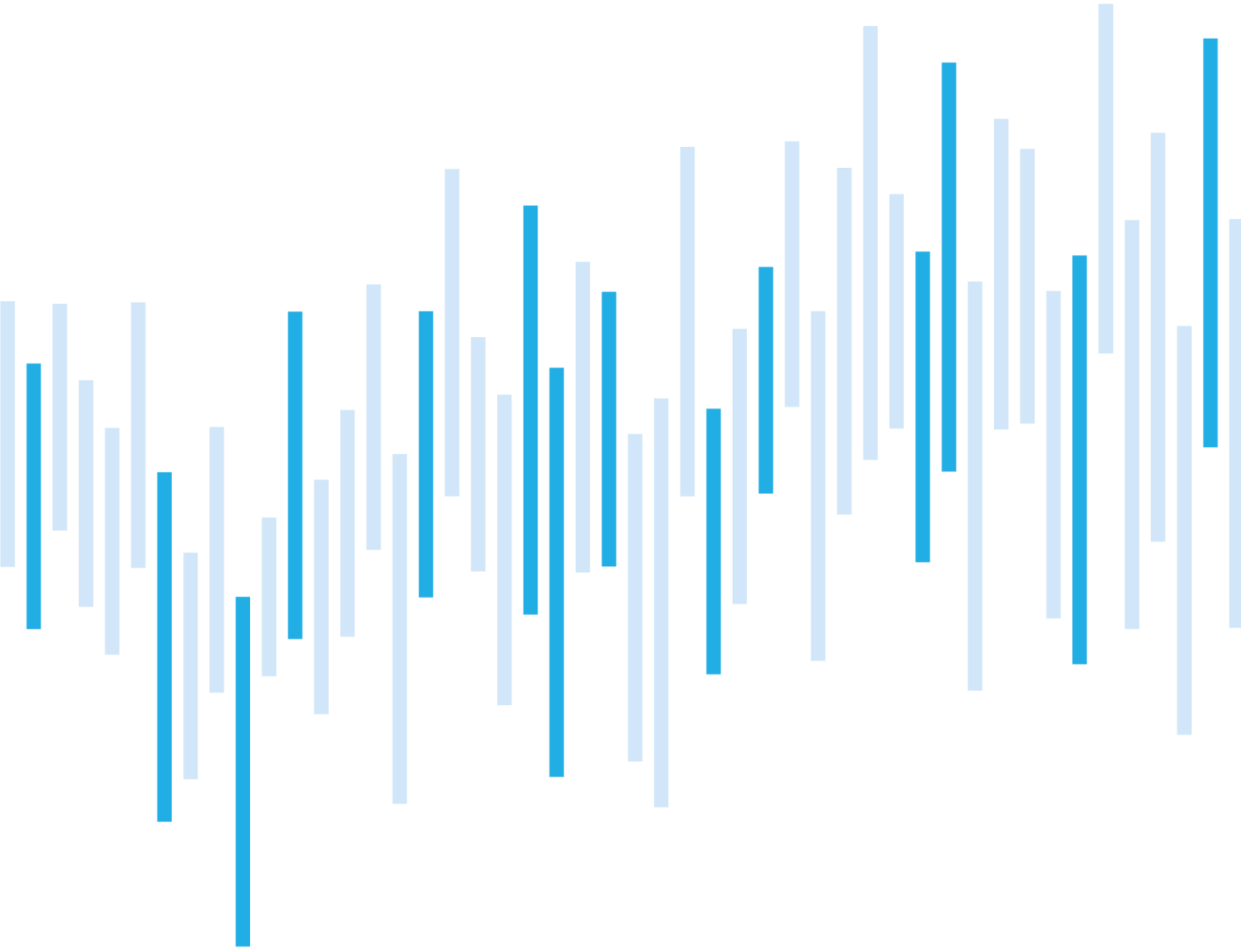
Kybernetické incidenty pohledem NÚKIB

Září 2021



Národní úřad
pro kybernetickou
a informační bezpečnost

Shrnutí měsíce

Září se s ohledem na kybernetické incidenty stalo nejklidnějším měsícem posledního roku. NÚKIB řešil pouze pět incidentů a žádný z nich neměl natolik závažné dopady, aby byl klasifikován jako velmi významný.

Po měsíci se do incidentů vrátil ransomware. NÚKIB řešil tři případy s rozdílnými dopady. Jedné oběti se podařilo obratem obnovit data ze zálohy, u zbylých dvou došlo následkem ransomwaru k částečné ztrátě dat a výpadku služeb. NÚKIB v tuto chvíli nemá informace o tom, že by útočníci data obětí exfiltrovali.

Mezi zářiovými incidenty se objevil i jeden spojený s českou vzdělávací institucí. Tento rok je to již 13. incident spojený se vzdělávacím sektorem, což v porovnání s předchozími roky představuje výrazný nárůst. Za nárůstem velmi pravděpodobně (75–85 %) stojí i fakt, že si od začátku roku 2021 začaly vysoké školy určovat své informační systémy na základě vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, a nově jsou tak povinny incidenty NÚKIB hlásit.

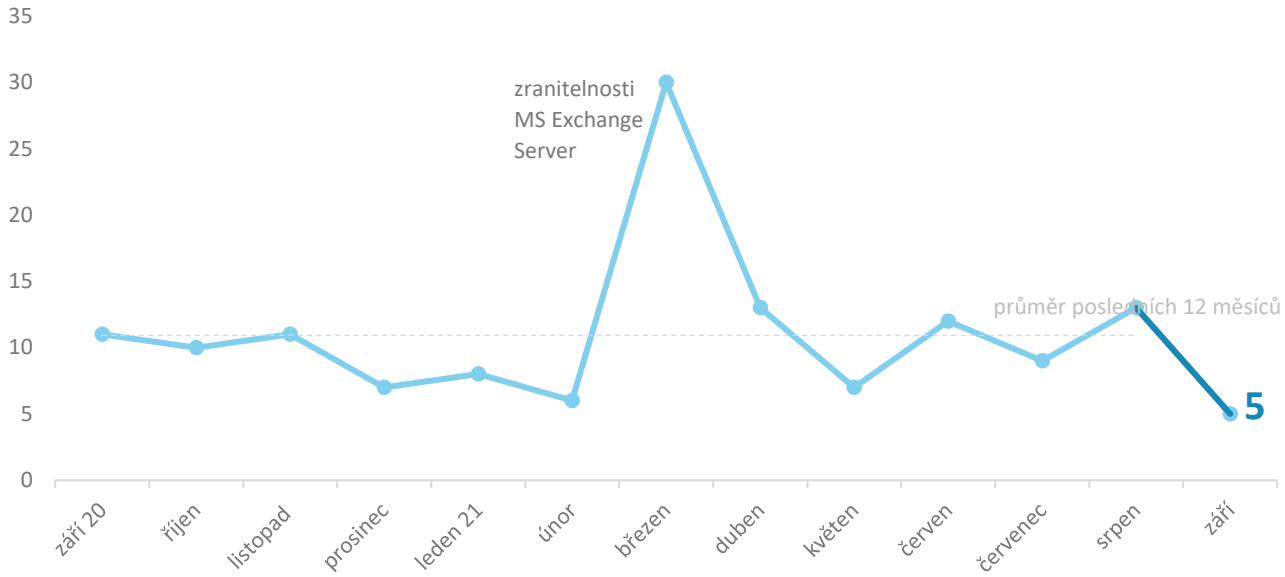
Obsah

Následující report shrnuje dění měsíce. Data, informace a závěry v něm obsažené primárně vychází z kybernetických incidentů nahlášených NÚKIB. Pokud report v některých částech obsahuje informace z otevřených zdrojů, je vždy uveden původ těchto informací.

Připomínky a náměty na zlepšení reportu můžete posílat na adresu komunikace@nukib.cz.

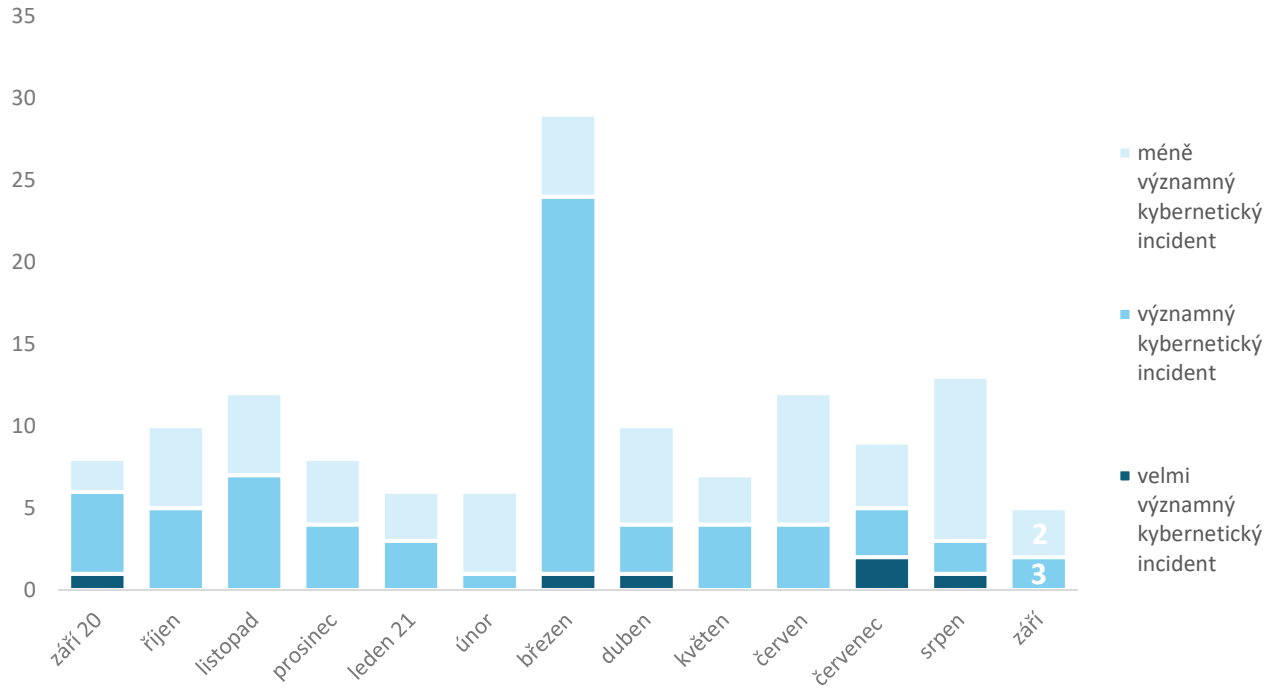
Počet kybernetických incidentů nahlášených NÚKIB

Září se s pěti incidenty stalo co do počtu nejklidnějším měsícem posledního roku.[1]



Závažnost řešených kybernetických incidentů[2]

Poklidnost měsíce se projevila i v relativně nízké závažnosti kybernetických incidentů. Žádný neměl natolik vážné dopady, aby ho NÚKIB klasifikoval jako velmi významný.

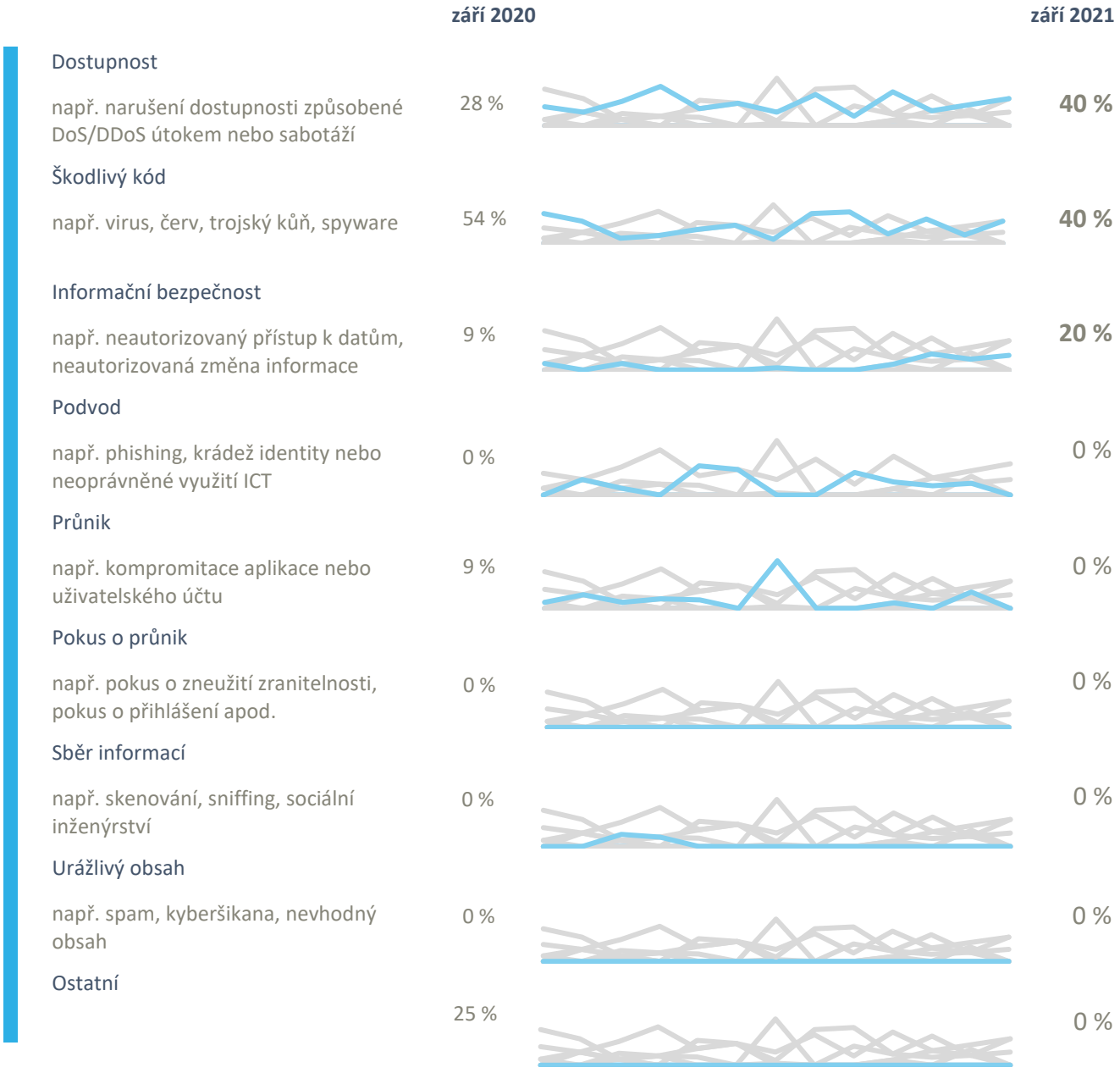


[1] Pouze jeden z incidentů nahlásila povinná osoba dle zákona o kybernetické bezpečnosti. Zbylé čtyři incidenty NÚKIB nahlásily subjekty, které pod tento zákon nespadají.
[2] Závažnost kybernetických incidentů je definována ve vyhlášce č. 82/2018 Sb.

Klasifikace incidentů nahlášených NÚKIB[3]

Podobně jako v předchozích měsících převažují v zářiových statistikách NÚKIB kybernetické incidenty zapříčiněné škodlivým kódem (dva případy) a narušením dostupnosti (dva případy). Poslední z incidentů NÚKIB eviduje jako narušení informační bezpečnosti, protože při něm došlo k úniku dat klientů dotčené společnosti.

Tři z těchto incidentů zapříčinil ransomware. Jelikož útoky měly rozdílné dopady, spadají tyto incidenty do několika kategorií. Jeden z ransomwarových útoků NÚKIB eviduje jako škodlivý kód, protože se obětem podařilo obratem zašifrovaná data obnovit ze záloh. Ve zbylých dvou případech došlo k částečné ztrátě dat a výpadku služeb. Tyto incidenty jsou proto klasifikovány jako narušení dostupnosti.



[3] Klasifikace kybernetických incidentů je založena na taxonomii ENISA: Reference Incident Classification Taxonomy — ENISA (europa.eu)

Trendy v kybernetické bezpečnosti za září pohledem NÚKIB[4]

Phishing, spear-phishing a sociální inženýrství

Phishing se už tradičně objevil v řešených incidentech NÚKIB i tento měsíc. Tentokrát se stal vektorem útoku pro jeden z ransomwarových útoků. NÚKIB vedle toho také eviduje phishingovou kampaň proti klientům jedné z českých komerčních bank.

V září pokračoval i vishing. Útočníci se opět vydávali za klientskou podporu Microsoftu a snažili se pracovníky vládní instituce přesvědčit o tom, že se stali oběťmi hackerského útoku, že jejich data jsou v ohrožení a že by pro nápravu situace měli navštívit webovou stránku útočníků.

Malware

Vedle ransomwaru se v incidentech objevil jediný škodlivý kód, který infikoval webové stránky oběti. Jednalo se o webshell, který neznámý útočník na stránku nahrál s využitím i zranitelnosti z roku 2016. Nelze vyloučit (25–50 %), že se návštěvníkům po přístupu na stránku dostaly do počítače nakažené soubory.

Zranitelnosti

V ČR zůstává stále vysoký počet strojů zranitelných na sérii zranitelností ProxyShell, o které NÚKIB informoval v srpnu. Podle nástroje Shodan bylo k 30. září v ČR zranitelných 692 serverů.

NÚKIB vydal upozornění na závažné zranitelnosti, které ohrožují systémy Linux v Azure, a zranitelnost virtualizačních serverů společnosti VMware, kterou útočníci aktuálně aktivně zneužívají.

Ransomware

Tři z kybernetických incidentů, které NÚKIB v září řešil, byly způsobené ransomwarovým útokem. Oproti srpnu, kdy ransomware v incidentech chyběl, se jedná o nárůst.

NÚKIB upozornil na nově zveřejněný nástroj k obnově dat zašifrovaných ransomwarem REvil. Dekryptor je ale možné použít jen k obnově dat zašifrovaných před 13. červencem a REvil tak dál představuje vážnou hrozbu, a to i pro české organizace, na které již v minulosti cílil. Od začátku roku 2021 NÚKIB řešil tři kybernetické útoky způsobené tímto ransomwarem.

Útoky na dostupnost

NÚKIB v září neeviduje žádný incident spojený s DoS nebo DDoS útokem. Dva z incidentů sice v nedostupnost služeb vyústily, ale jednalo se o důsledek úspěšného ransomwarového útoku.

Ransomware a DDoS útoky se nicméně stávají propojenými kategoriemi. V posledních měsících se objevil nový trend, kdy útočníci doplňují ransomware o DDoS. Hrozba nedostupnosti služeb klade vedle zašifrování a zveřejnění dat další tlak na oběti, a tak zvyšuje pravděpodobnost, že útočníkům výkupné zaplatí.

[4] Vývoj ilustrovaný šipkou je vyhodnocován ve vztahu k předešlému měsíci.

Nejpoužívanější technika měsíce: Command and Scripting Interpreter - PowerShell

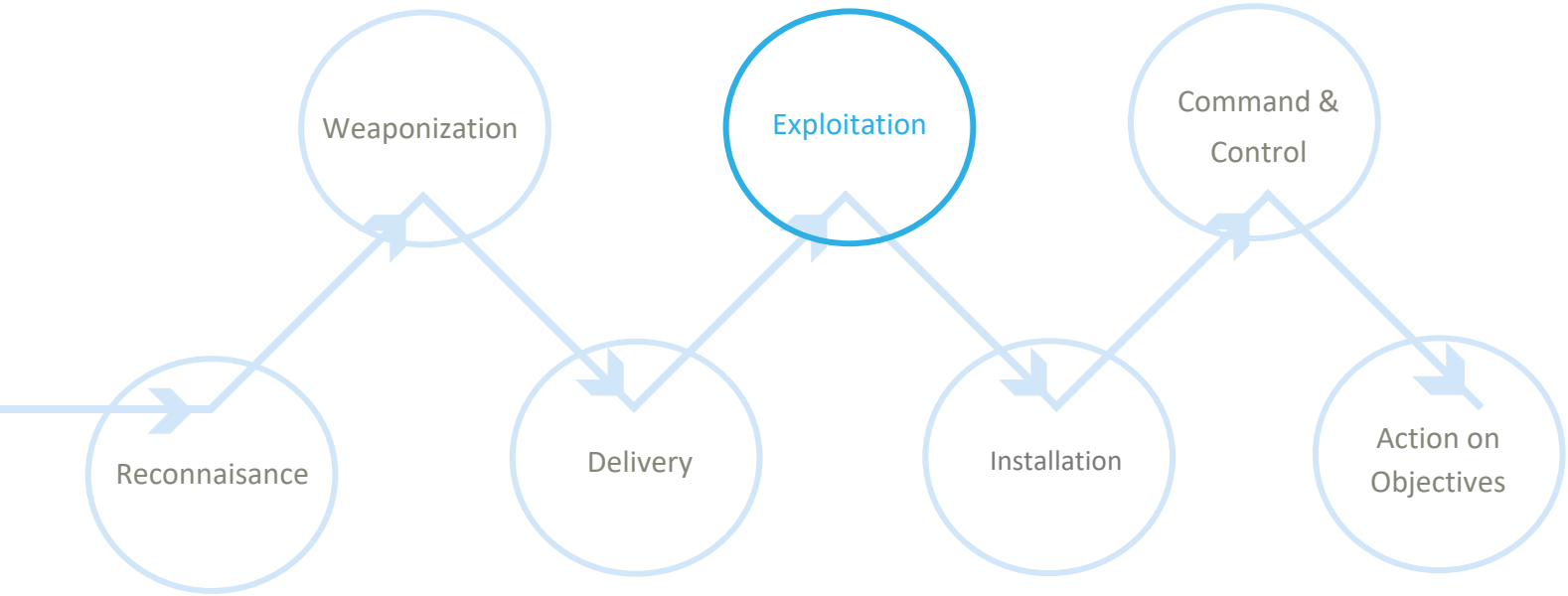
NÚKIB kybernetické incidenty vyhodnocuje také na základě metriky MITRE ATT&CK, která slouží jako přehled všech známých technik a taktik používaných při kybernetických útocích. NÚKIB na jejím základě mimo jiné určuje četnost využívání technik. V zářiových incidentech útočníci nejčastěji používali PowerShell.

PowerShell je skriptovací jazyk a příkazové prostředí sloužící ke správě moderních verzí Windows, v multiplatformní verzi je též k dispozici pro Linux a MacOS. Pro širokou škálu využití a přímou dostupnost v systému bývá často využíván k living-off-the-land útokům, získávání informací o systému obětí a spouštění škodlivých skriptů. S pomocí PowerShellu mohou stahovat payload z internetu, exfiltrovat data, eskalovat oprávnění nebo v případě administrátorského přístupu spouštět skripty na vzdáleně připojených strojích. PowerShellové skripty používají APT i kyberkriminální skupiny napříč celým světem, včetně toho, že si v něm píší své ofenzivní nástroje.

MITRE ID: T1059.001

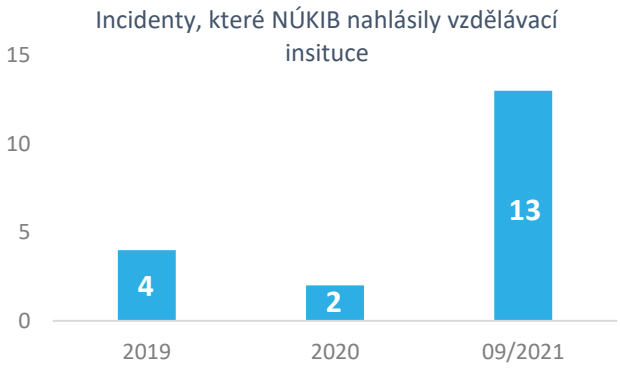
Mitigace: Z hlediska mitigace lze nastavit logování, monitorovat klíčová slova (executionPolicy, iex, hidden, mimikatz etc.), whitelistovat spouštění skriptů pouze na podepsané, nebo uživatelům PowerShell úplně zakázat.

Útočníci mohou PowerShell zneužít v jakékoliv fázi útoku. V zářiových incidentech útočníci nejčastěji spouštěli PowerShell ve fázi „Exploitation“, kdy útočník zneužije příkazové prostředí k získání přístupu nebo stažení dalšího malwaru.



Zaměřeno na sektor: Vzdělávání

Mezi zářiovými kybernetickými incidenty se objevil jeden spojený s českou vysokou školou. Tento rok je to již 13. incident spojený se školským sektorem. V porovnání s předchozími roky se jedná o výrazný nárůst.



Za nárůstem velmi pravděpodobně (75–85 %) stojí i fakt, že si od začátku roku 2021 začaly vysoké školy určovat své informační systémy na základě vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, a nově jsou tak povinny incidenty NÚKIB hlásit. NÚKIB vedle vysokých škol, které spadají pod zákon, eviduje i kybernetické útoky na střední a základní školy. Ty je hlásily dobrovolně, neboť podle zákona o kybernetické bezpečnosti nemají povinnost NÚKIB o podobných útocích informovat.

V hlášeních incidentů se objevuje celá řada typů útoků na vzdělávací instituce nebo pokusů o ně. Nejčastěji je mezi nimi phishing v různorodých podobách – od jednoduchých, plošně rozesílaných vyděračských e-mailů až po sofistikované a specificky cílené podvodné e-maily, v nichž se útočníci vydávali za zaměstnance univerzity. Častým případem jsou i úniky dat, spam, DDoS nebo ransomwarové útoky.

Kybernetické útoky na vzdělávací a výzkumné instituce nelze podceňovat. Na mnoha českých vysokoškolských institucích probíhá výzkum s vysoce hodnotnými výsledky[5], a mohou se proto objevit v hledáčku státem podporovaných aktérů. Jejich hlavní motivací bývají strategicky důležité informace, nebo informace důležité pro získání konkurenční výhody v průmyslové nebo vojenské oblasti. Významnou roli v uchovávání těchto informací hrají vzdělávací a výzkumné instituce, které se podílejí na výzkumu a vývoji nových technologií. V ČR jde hlavně o obory věnující se zdravotnickému výzkumu, dalšímu využití nanotechnologií, vývoji biotechnologií, IT technologií nebo nových energetických zdrojů. Pokud by útočníci v sítích českých univerzit působili nepozorovaně delší dobu, mohlo by to pro Českou republiku ve výsledku znamenat oslabení její konkurenceschopnosti a až miliardové finanční ztráty.

[5] Pod vyhlášku č. 317/2014 Sb., spadají především administrativní systémy vysokých škol, výzkum a vývoj se k nim neřadí.

Použité pravděpodobnostní výrazy

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 %

Podmínky využití informací

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol (dostupná na webových stránkách www.nukib.cz). Informace je označena příznakem, který stanoví podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Barva	Podmínky použití
TLP:RED	Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace.
TLP:AMBER	Informace může být sdílena v rámci organizace, které byla informace poskytnuta. Dále může být poskytnuta pouze těm partnerům, kteří splňují need-to--know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci. Jiným osobám, než výše uvedeným, nesmí být informace poskytnuta. Původce informace může rozsah sdílení dále omezit.
TLP:GREEN	Informace může být sdílená v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace.
TLP:WHITE	Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena.