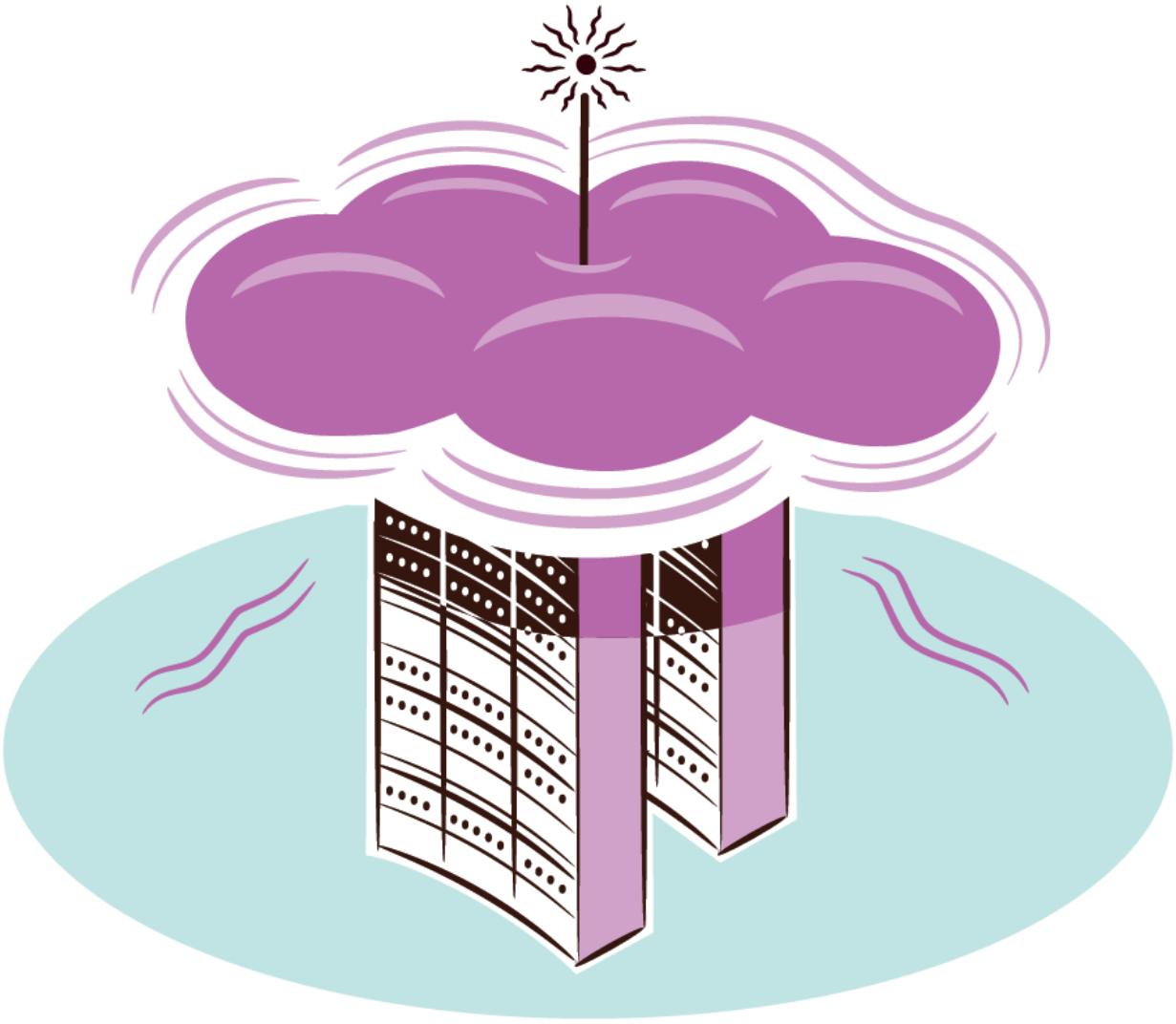
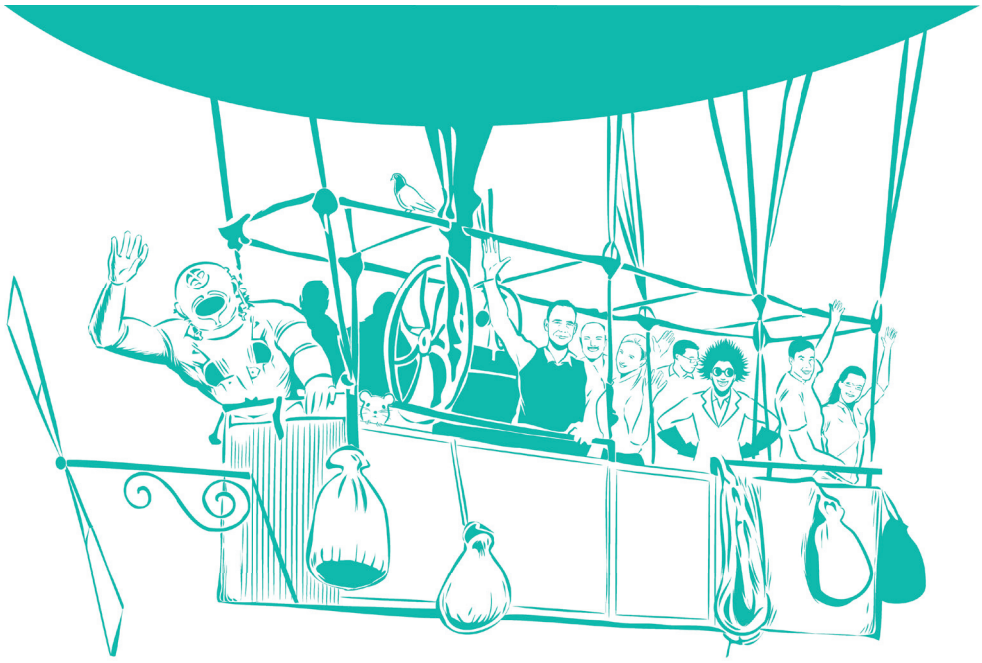
ALEF

Security Report 2021



Trust the Strong
www.alef.com

Obsah



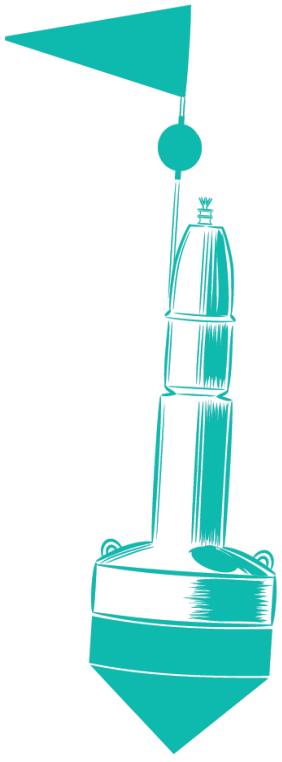
Úvod

S dynamickým rozvojem informačních a komunikačních systémů v posledních letech roste i závislost organizací na těchto systémech. Aktuálně by bylo těžké v rozvinutých ekonomikách nalézt společnost, která je na informačních technologiích naprosto nezávislá. Přestože v mnohých ohledech tento vývoj nesporně přináší výhody v podobě vyšší produktivity práce, jeden potenciálně problematický aspekt není možné vynechat, a tím je informační bezpečnost. Rostoucí význam informačních technologií stále častěji přitahuje pozornost potenciálních útočníků a bezpečnostní rizika spojená s informačními aktivy nabývají bezprecedentních hodnot.

Abychom dokázali alespoň dílčím způsobem predikovat vývoj v oblasti bezpečnostních hrozeb a zranitelností, průběžně sledujeme trendy na poli informační bezpečnosti. Za sběr a vyhodnocování dat je odpovědný bezpečnostní tým ALEF CSIRT, který pro svou analytickou činnost využívá, jak vlastní, tak i relevantní externí zdroje z České republiky a zahraničí. Na této zprávě však participovali i další specialisté z ALEF security týmu tak, abychom Vám byli schopni poskytnout zajímavé výstupy z různých oblastí informační bezpečnosti. Zpráva obsahuje souhrn nejzajímavějších trendů, které jsme identifikovali v roce 2020, spolu s popisem vybraných aktivit našich bezpečnostních týmů a věříme, že Vám naše výstupy umožní se lépe zorientovat v současném nevyzpytatelném prostředí a třeba pomohou s definicí či úpravou bezpečnostních opatření ve Vaší organizaci.

V následujících kapitolách naleznete trendy v oblasti šíření škodlivého kódu nebo vybraných kybernetických útoků, ale můžete se také seznámit s přístupem organizací působících v České republice k bezpečnostnímu monitoringu, penetračním testům nebo vzdělávání uživatelů v problematice kybernetických hrozeb. Součástí zprávy je také několik analýz týkajících se zabezpečení e-mailové komunikace a úrovně šifrování webových aplikací. Rok 2020 byl ve všech ohledech výjimečný zejména v souvislosti s pandemií Covid-19. O to zajímavější je porovnání výstupů s předchozími roky.

Na tomto místě bychom, jako tradičně, rádi poděkovali zejména bezpečnostním týmům CESNET-CERTS a CSIRT.CZ, které nám laskavě poskytly data a statistiky ze svých monitorovacích nástrojů. Zároveň děkujeme všem účastníkům průzkumu, kteří nám zareagovali na naše online dotazníky, neboť dostatečné množství relevantních dat je nutnou podmínkou pro kvalitní výstup.



Útoky, zranitelnosti a šifrování v roce 2020

Jan Kopřiva

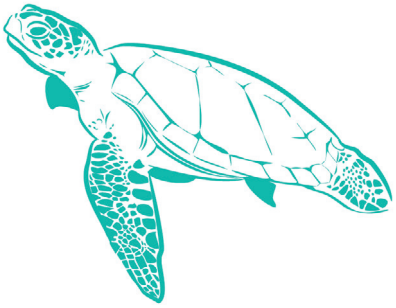
Rok 2020 byl (nejen) pro kybernetickou bezpečnost do jisté míry přelomový. Vedle publikace jednoho z bezpochyby nejvýznamnějších kybernetických útoků poslední dekády – kompromitace systémů společnosti SolarWinds a návazný úspěšný průnik do sítí tisíců dalších organizací – byly v podstatě všechny moderní organizace nuceny vypořádat se také s mnoha citelnými důsledky pandemie Covid-19. Neočekávaný nárůst počtu zaměstnanců pracujících z domova a související potřeba ochránit organizační zařízení v domácích sítích, nebo nezbytné oddělení soukromých zařízení při přístupu do sítí korporátních vedly k mnoha významným změnám v oblasti zabezpečení organizačních IT prostředí.

Paralelně s bezpečnostními specialisty však postupovali také útočníci. I vzhledem k čím dál tím vyšší profesionalizaci v oblasti tvorby a distribuce škodlivého kódu, zejména ransomwaru, jsme byli svědky nespočtu úspěšných kybernetických útoků na kritické, zejména zdravotnické instituce, jejichž dopady budou bezpochyby citelné ještě velmi dlouhou dobu.

Nejen tyto vysoce medializované aktivity útočníků však v roce 2020 způsobovaly významné škody a vedle konkrétních útoků tak stojí za pozornost i vybrané dlouhodobé trendy, a to jak v oblasti působení škodlivých aktérů a obránců, tak z nich vyplývajících změn v síti internet. Právě na tyto oblasti se tak zaměříme v první části letošního reportu.

Data využitá v rámci níže uvedeného textu pochází z bezpečnostních a analytických systémů skupiny Alef, infrastruktur jejích vybraných zákazníků, služby Shodan a ze systémů PROKI a Warden, provozovaných bezpečnostními týmy CSIRT.CZ a CESNET-CERTS. Oběma zmíněným týmům bychom tímto chtěli ještě jednou poděkovat za to, že nám data pro analýzu i v tomto roce poskytnuly.

Pro úplnost je vhodné uvést, že vzhledem k velmi citelným rozdílům mezi počty událostí spojených s vybranými škodlivými aktivitami, které byly detekované v globálním a českém prostředí, jsou v rámci analýz aktivit útočníků a relevantních grafů namísto absolutních hodnot užívána procentuální rozdělení relevantních událostí do jednotlivých měsíců roku 2020.

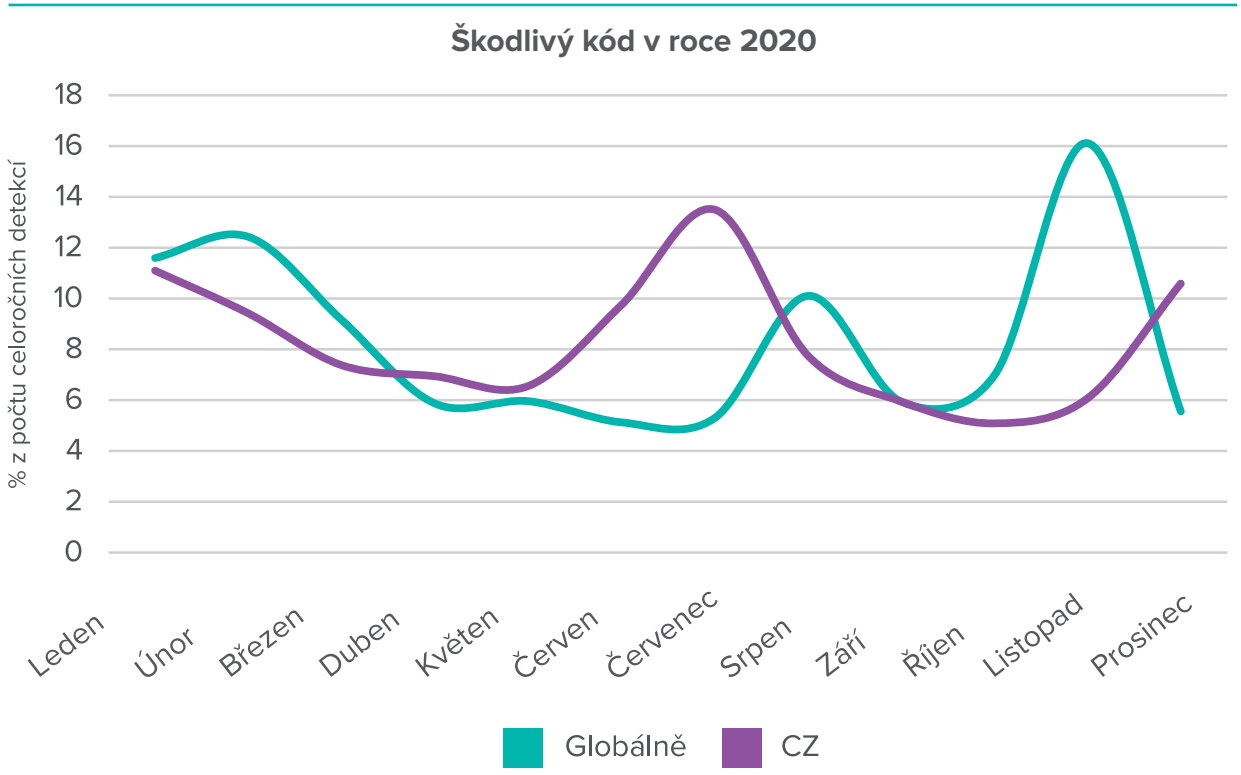


Škodlivý kód

Distribuce ransomwaru zmíněná výše nebyla zdaleka jediným typem útoků, při nichž byl škodlivými aktéry efektivně využíván malware. Ani vlastní ransomwarové infekce se konec konců mnohdy neobešly bez malwaru jiného. V průběhu roku 2020 byl totiž stále významněji patrný jeden z významných trendů posledních let, konkrétně distribuce škodlivého kódu skrz delší řetězec jiných infekcí. Při něm je cílové zařízení nejprve kompromitováno jedním druhem škodlivého kódu, který pak kromě jiných aktivit na dané zařízení stáhne i další malware (mnohdy větší počet variant škodlivého kódu z více než jedné rodiny).

Jedním z nejpodstatnějších typů malware, který byl v rámci těchto řetězců široce využíván, byl bezpochyby trojan Emotet, který kromě jiného distribuoval trojské koně TrickBot a QakBot, ale nezřídka vedl také k infekcím určitými druhy ransomwaru.

Vedle výše uvedených rodin škodlivého kódu jsme v průběhu uplynulých dvanácti měsíců zaznamenali také masivní škodlivé kampaně zaměřené na šíření malwaru z rodin Agent Tesla, AZORult, BazarLoader a mnoha dalších. Stejně jako v předchozích letech při tom bylo možné označit za dominantní vektory pro šíření škodlivého kódu e-mailové zprávy (s odkazy vedoucími ke stažení škodlivého kódu, nebo přílohami, které škodlivý kód přímo nesly) a drive-by downloady, resp. využívání exploit kitů. Zejména u cílených útoků však byl velmi citelný i trend manuální implantace škodlivého kódu do již kompromitovaných systémů.
Jak ukazuje následující graf, v rámci globálního prostředí byl na konci prvního kvartálu patrný relativně silný pokles detekcí, přičemž jejich počty zůstaly na relativně nízké úrovni až do srpna, potažmo listopadu, kdy byl identifikován největší výskyt škodlivého kódu (16,1% ze všech detekcí z celého roku). V prostředí ČR pak počty detekcí stabilně klesaly od počátku roku až do května (od 11,09 až po 6,55%), následně stouply k červencovému maximu (13,5%) a poté až do konce listopadu opět padaly. Jediný další citelný nárůst byl pak v ČR patrný až na konci posledního kvartálu, kdy bylo detekováno 10,59% z veškerého zaznamenaného škodlivého kódu.

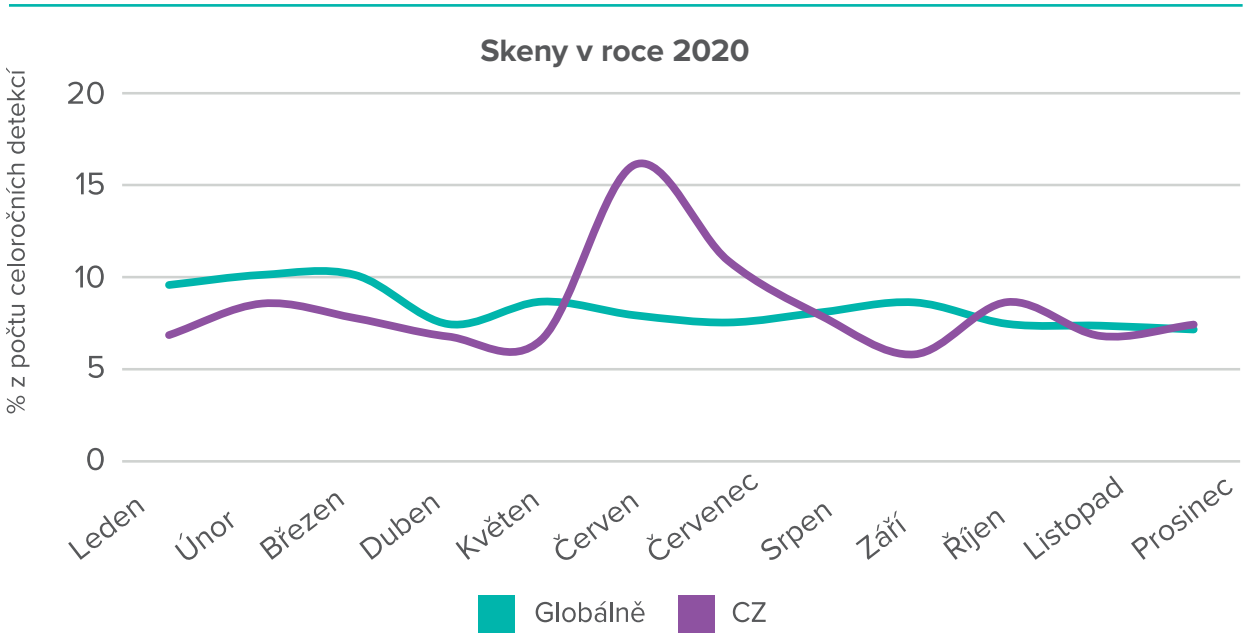


Skeny
Útočníci se v uplynulém roce pochopitelně nesoustředili jen na škodlivý kód. Silně se zaměřovali například i na útoky na služby a systémy dostupné z internetu. Jedním z faktorů, který toto zaměření bezpochyby ovlivnil, byl i vysoký počet systémů nově připojených do internetu. V důsledku zvýšeného počtu zaměstnanců pracujících v důsledku celosvětové pandemie vzdáleně zpřístupnil významný počet organizací s pomocí internetu i systémy a služby, které byly historicky dostupné pouze z interních organizačních sítí. Toto rozhodnutí s sebou v některých případech neslo významná bezpečnostní negativa (viz následující odstavce) a útočníci se tak zcela logicky zaměřili i na odhalování zmíněných systémů a pokusy o identifikaci případných zranitelností v nich. Primárně tak činili s pomocí automatizovaných vzdálených skenů.

Jak ukazuje níže uvedený graf, na němž je vyobrazený rozpad detekovaných síťových skenů do jednotlivých měsíců, v globálním prostředí byl na skeny nejbohatší první kvartál, v němž bylo detekováno téměř 30% jejich celoročního počtu.

V průběhu zbylých devíti měsíců pak byly – zřejmě i v důsledku výše zmíněné pandemie – počty detekovaných skenů i přes drobné výkyvy citelně nižší (mezi 7,12 a 8,67 %).

V rámci ČR vývoj velmi připomínal ten z roku 2019, s tím rozdílem, že k citelným výkyvům došlo v roce 2020 vždy o měsíc dříve, než tomu bylo v roce předchozím. Největší počty skenů tak byly zaznamenány v červnu a červenci (16,14 %, resp. 10,9 %), nejnižší počet detekcí pak patřil září (5,78 %).



Zranitelné systémy

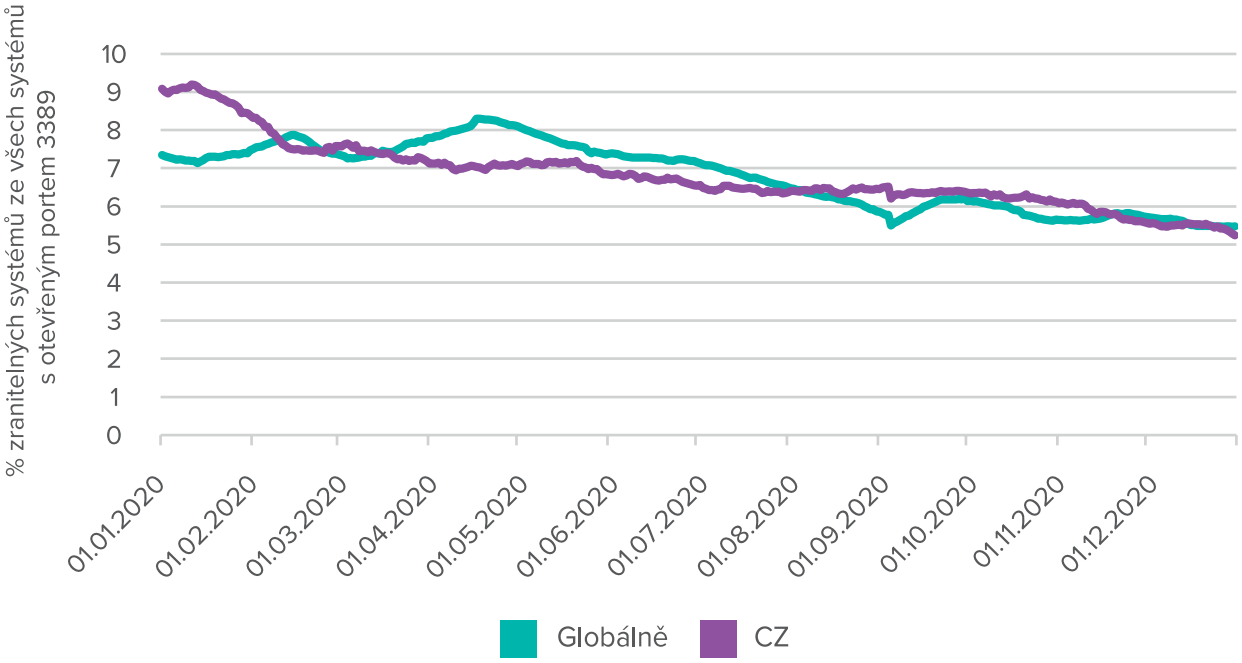
Výše zmíněný trend zpřístupňování dříve výhradně interních systémů z internetu vedl mimo jiné i k povolení příchozí komunikace ke značnému počtu nezáplatovaných či zastaralých systémů.

Tuto skutečnost vhodně dokumentuje například vývoj počtu k internetu připojených systémů nezáplatovaných proti zranitelnosti BlueKeep. Záplata pro tuto zranitelnost, známou též pod identifikátorem CVE-2019–0708, byla publikována již v květnu roku 2019. Přestože jde o zranitelnost vysoce závažnou (umožňuje hypotetickému útočníkovi přes síť spustit na zranitelném zařízení libovolný kód s vysokými oprávněními) a jsou pro ni již velmi dlouho k dispozici veřejně dostupné exploity, na konci roku 2020 bylo stále z internetu přístupných přes 242 000 systémů, které jí byly postiženy. Šlo při tom o číslo relativně nízké v porovnání s téměř 390 000, což byl maximální počet zranitelných systémů, který byl v průběhu loňského roku (konkrétně na počátku května) dostupný z internetu.

Vhodněji než absolutní čísla však mohou v tomto případě vývoj situace dokumentovat procentuální zastoupení zranitelných systémů v počtu všech serverů, které služby vzdáleného sdílení plochy s pomocí protokolu RDP poskytovaly do internetu.

Jak ukazuje následující graf, v prostředí ČR mělo až na drobný pozitivní výkyv v první polovině března procento zranitelných systémů téměř kontinuálně klesající tendenci. V rámci globálního internetu pak byla situace značně rozdílná. Citelné „špičky“ jsou v grafu patrné okolo půlky února, kdy bylo zranitelností BlueKeep postižených 7,87 % ze všech systémů s otevřeným portem TCP 3389 do internetu, a v průběhu dubna, kdy bylo zranitelných celkem 8,3 % těchto systémů.

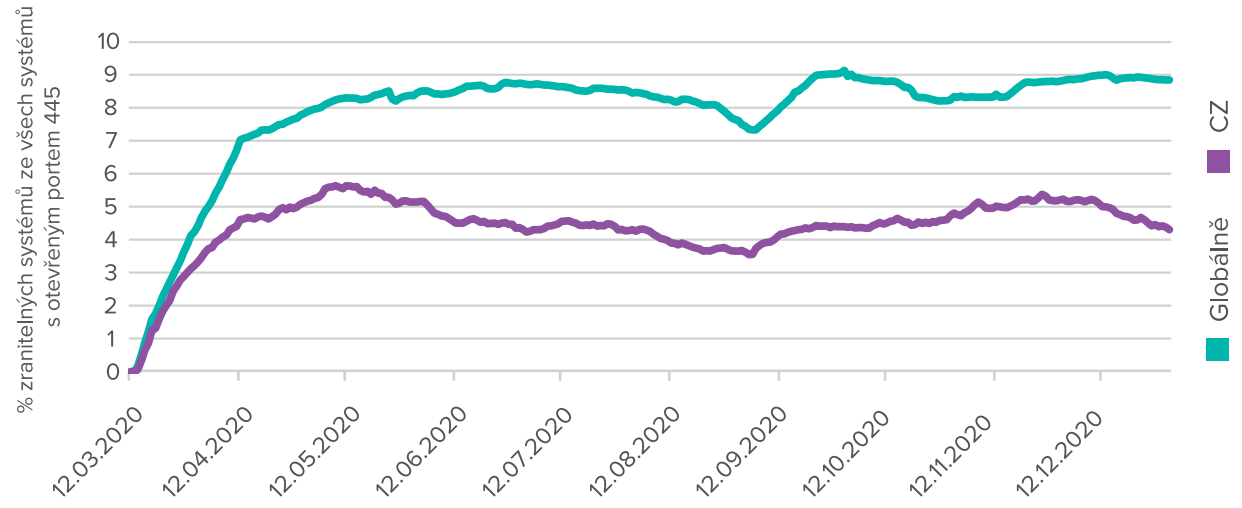
Z internetu dostupné systémy nezáplatované proti zranitelnosti BlueKeep



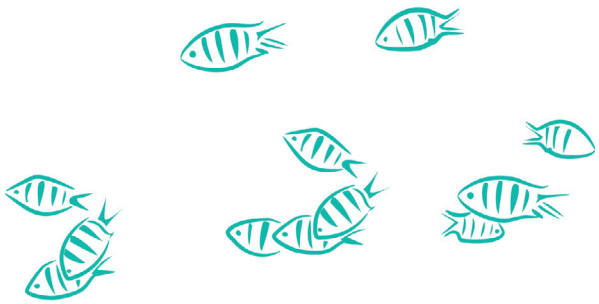
Přestože obecný trend v absolutních počtech i relativním zastoupení zranitelných systémů byl v průběhu uplynulých 12 měsíců klesající, nelze ani stav na konci roku 2020 považovat za uspokojivý.

Stejný závěr je bohužel možné uvést i pro situaci týkající se mnoha novějších zranitelností. Za přehnaně pozitivní totiž nelze označit například ani vývoj počtu zranitelných systémů postižených zranitelností známou jako SMBGhost (CVE-2020–0796). Záplata pro tuto kritickou zranitelnost, která postihuje službu sdílení souborů v moderních operačních systémech Windows, byla publikována v březnu roku 2020. Přesto však – jak demonstruje následující graf – byl na globální úrovni od stabilizace počtů v první polovině května, kdy byl mj. globálně detekován nejvyšší počet zranitelných systémů (přes 136 000), patrný pomalu rostoucí trend poměrného zastoupení zranitelných systémů mezi všemi servery, které službu vzdáleného sdílení souborů do internetu poskytovaly. V prostředí ČR pak měla sledovaná hodnota tendenci v průběhu roku kolísat okolo 4,5 %.

Z internetu dostupné systémy nezáplatované proti zranitelnosti SMBGhost

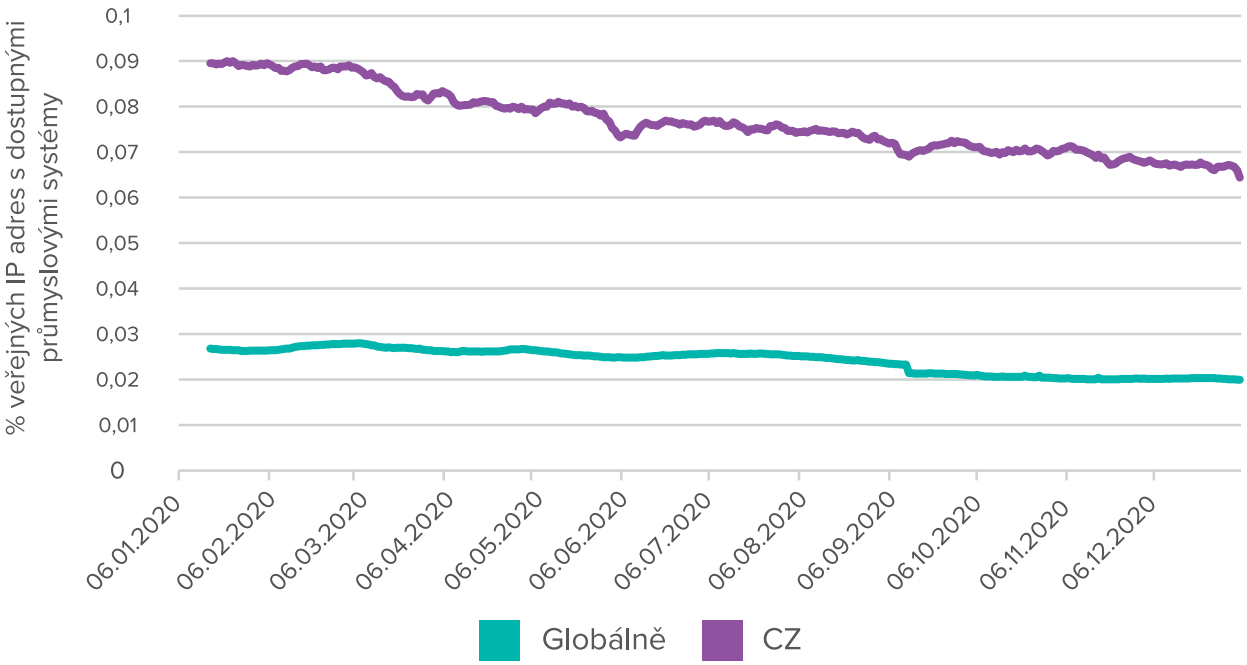


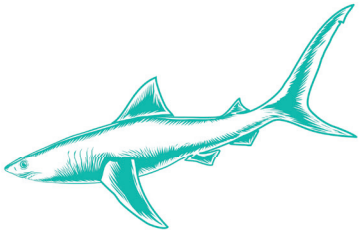
I ponecháme-li stranou, že samotné zpřístupnění služby sdílení souborů do internetu lze ve většině případů považovat za přinejmenším nešťastnou bezpečnostní praxi, jsou uvedené hodnoty velmi znepokojivé.



Průmyslové systémy

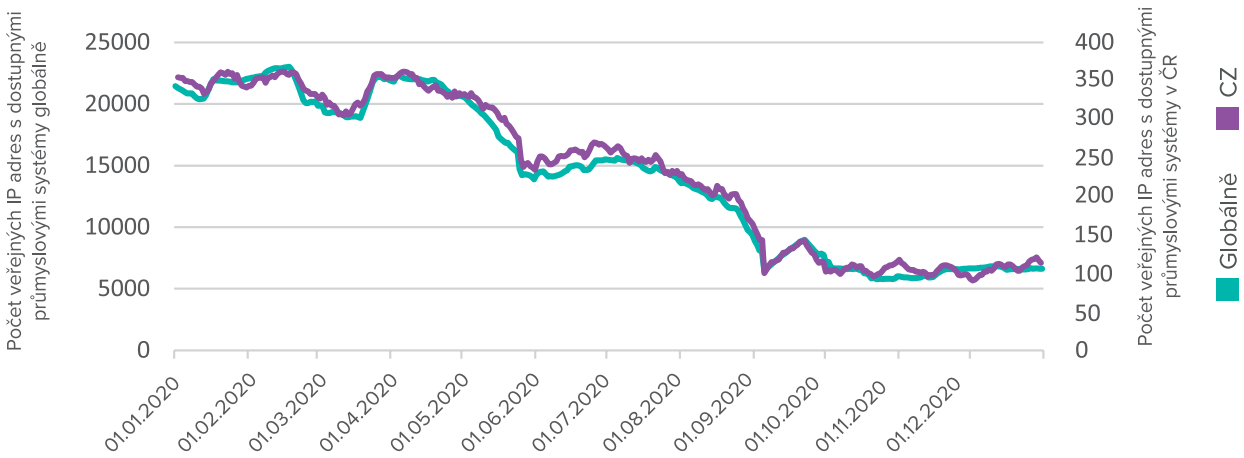
Vývoj, k němuž došlo v průběhu roku 2020 oblasti počtu k internetu připojených průmyslových systémů (ICS) lze naopak označit za převážně pozitivní. Zatímco k 1. 1. 2020 bylo celosvětově detekováno 127 697 takových systémů, přičemž v ČR jejich počet dosáhnul 1 259, k 31. 12. zmíněného roku jich bylo globálně detekováno již jen 96 398 a v ČR 1 020. Jak ukazuje následující graf, citelně se v průběhu roku snížilo i relativní zastoupení průmyslových systémů na českém a celosvětovém internetu.





Primárním důvodem pro zmiňovaný pokles počtu ICS na internetu se zdá být zejména citelné snížení počtu systémů využívajících komunikační protokol Modbus. Množství těchto zařízení na českém i globálním internetu se v průběhu prvních 3 kvartálů roku 2020 významně snižovalo, v důsledku čehož bylo k 31. 12. veřejně dostupných již pouze 6609 (globálně), resp. 119 (CZ) takových systémů, oproti 21 441 (globálně), resp. 353 (CZ), což byly počty ICS komunikujících s pomocí protokolu Modbus detekované na internetu k 1. 1. 2020.

Průmyslové systémy využívající protokol Modbus na internetu



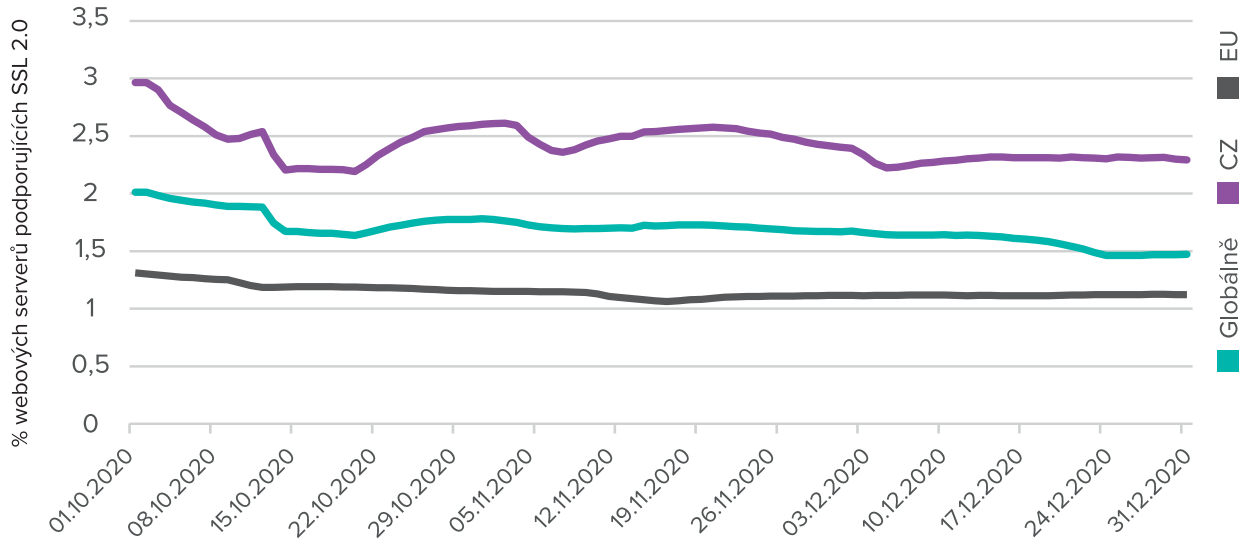
Počty systémů komunikujících s pomocí jiných průmyslových protokolů měly ve většině případů rovněž klesající tendenci, nebo alespoň výrazněji nestoupaly. Jedinou významnější výjimkou byly počty zařízení využívajících průmyslový protokol EIBnet/IP, jejichž počty se z původních 16 087 (globálně), resp. 227 (CZ) zvýšily do konce roku na 18 864 a 259 (tedy o 17,26 % globálně a 14,1 % v rámci českého internetu).

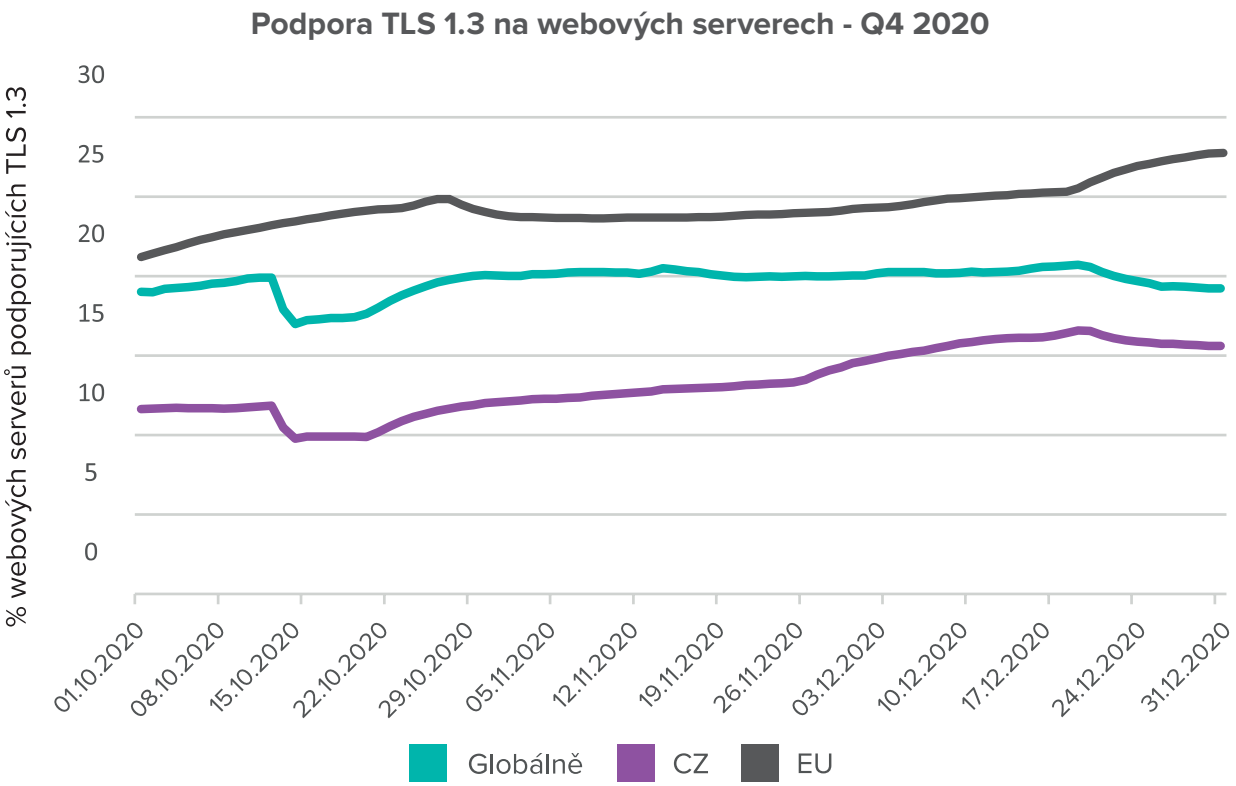
Šifrovaná webová komunikace

Jednou z významných změn v oblasti bezpečnosti internetu, kterou přinesl uplynulý rok, je bezpochyby i relativně citelný posun v oblasti adopce kryptografického protokolu TLS 1.3 a postupné upouštění od používání historického protokolu SSL 2.0.

Přestože jako vhodné pro zabezpečení webového provozu byly již v průběhu roku 2020 považovány pouze kryptografické protokoly TLS 1.2 a TLS 1.3, nemalé počty serverů stále podporují protokoly starší a méně bezpečné. Jak však ukazuje následující graf, v posledním kvartálu roku 2020 od podpory zastaralého a vysoce zranitelného protokolu SSL 2.0 upustilo významné procento provozovatelů webových serverů jak v rámci domácího, tak globálního internetu. Přestože celosvětově bylo na internetu na konci roku stále dostupných přes 873 000 webových serverů, které zmíněný protokol podporovaly, lze současný trend vývoje považovat za vysoce pozitivní.

Podpora SSL 2.0 na webových serverech - Q4 2020





U prozatím poslední iterace protokolu TLS – jeho verze 1.3 – byl naopak v posledním kvartálu jak v prostředí globálního internetu, tak zejména v rámci ČR a EU, patrný citelný nárůst podpory ze strany webových serverů. Tento trend lze rovněž hodnotit jako vysoce pozitivní, mj. i vzhledem k citelně nižší možnosti nevhodné/slabé konfigurace TLS 1.3 na webových serverech nebo bezpečnostní infrastruktuře. Na konci roku 2020 bylo v prostředí ČR evidováno již 26 420 webových serverů podporujících jmenovaný protokol a v rámci globálního internetu bylo takových serverů detekováno celkem 11 416 320.

CSIRT.CZ

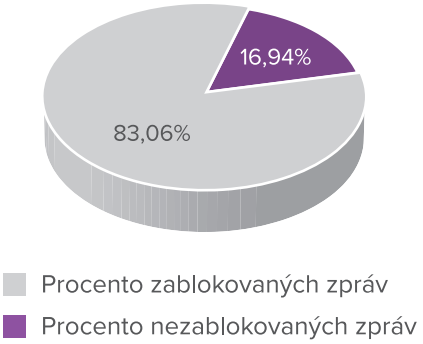
cesnet certs

Analýza dat z e-mailových bran

Milan Habrcetl

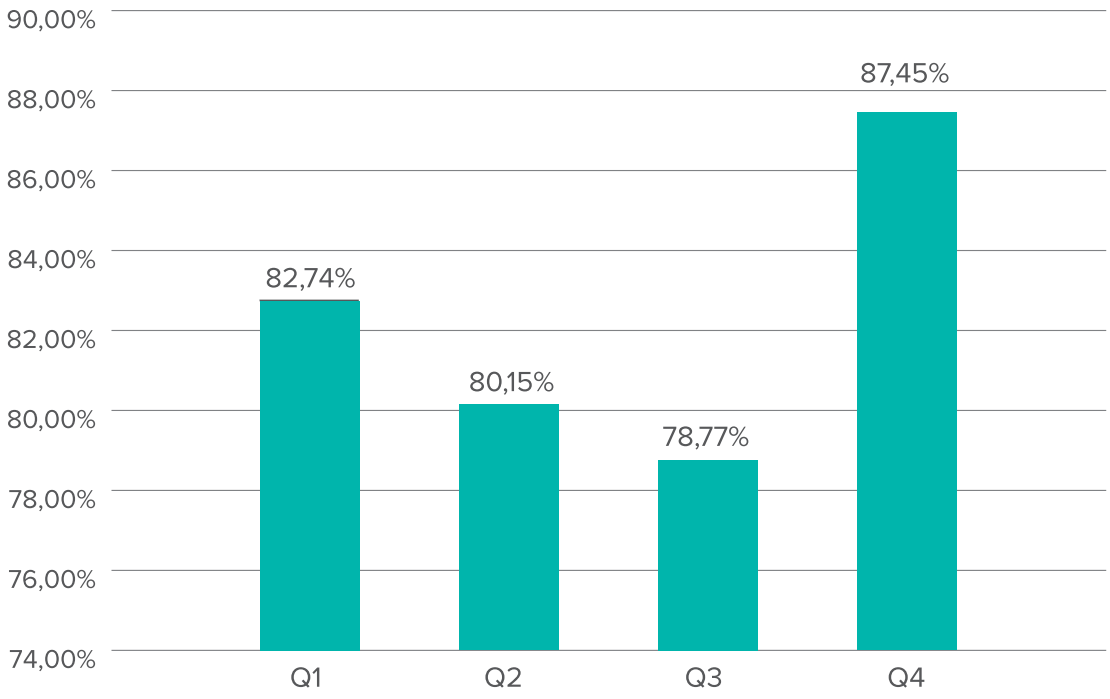
Tato část analýzy probíhala nad daty příchozích e-mailových zpráv, které byly přijaty vybranými e-mailovými branami v roce 2020.
Za celý rok 2020 bylo zablokováno více než 83 procent všech příchozích e-mailových zpráv. Oproti roku předtím se jedná o pokles zablokovaných e-mailových zpráv, což může být následek situace spojené s pandemií a tím, že uživatelé museli převážně používat elektronické zprávy ke komunikaci s kolegy. Tím se tedy zvedl i počet legitimních, nezablokovaných e-mailových zpráv oproti minulému roku.

Zablokované vs. nezablokované e-mailové zprávy



V každém čtvrtletí roku 2020 bylo e-mailovými branami zablokováno průměrně 82,3 procent e-mailových zpráv. Nejvíce e-mailových zpráv bylo blokováno v posledním čtvrtletí (říjen, listopad, prosinec), kdy procento blokovaných zpráv dosáhlo téměř 87,5 % procent.

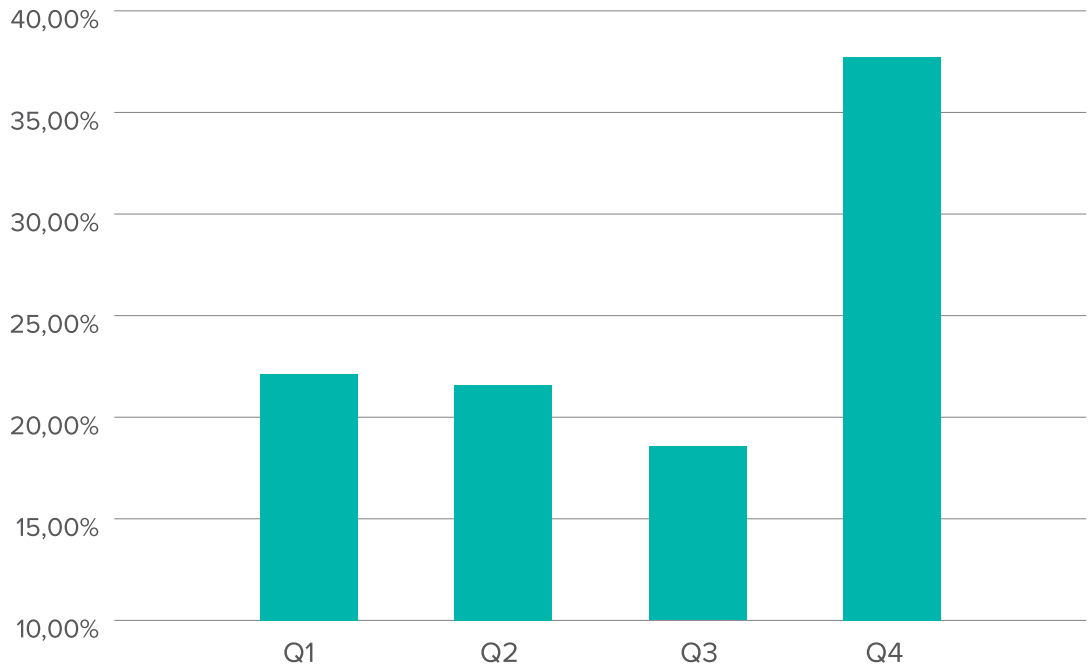
Procento zablokovaných e-mailových zpráv po kvartálech



Po agregaci dat do jednotlivých čtvrtletí lze vypozorovat významný nárůst blokovaných e-mailových zpráv mezi třetím a čtvrtým čtvrtletím roku 2020. Důvodem jsou vánoční svátky a konec roku a všechny přípravy spojené s těmito svátky. V tomto období jsou uživatelé často méně pozorní a také očekávají příchozí balíčky, faktury apod. Útočníci tohoto tedy tradičně využívali tím, že odesílají velké množství škodlivých e-mailových zpráv, aby zvýšili své výdělky. Útočníkům také pomáhala situace spojená s pandemií, protože lidé nemohli nakupovat vánoční dárky v kamenných obchodech, a tak si většinu z nich museli objednávat přes internet.

Níže následuje graf s podílem zablokovaných zpráv v jednotlivých čtvrtletí, kde lze tento rozdíl dobře vidět:

Procentuální zablokování všech zablokovaných e-mailů do jednotlivých kvartálů



Období dovolených a pokles počtu zablokovaných e-mailových zpráv

V třetím čtvrtletí (červenec, srpen, září), ve kterém obvykle bývá větší počet dovolených, lze vypozorovat pokles zablokovaných e-mailových zpráv. S největší pravděpodobností z toho důvodu, že by se útočníkům nevyplatilo odesílat e-mailové zprávy se škodlivým obsahem, protože s nimi uživatelé neinteragují (jsou na dovolené).

Dalším důvodem může být také to, že útočníci jsou také na dovolených, a tedy neodesílají spam, phishing a jiné e-mailové zprávy se škodlivým obsahem.

Analýza důvodu blokace e-mailových zpráv

Při analýze důvodů blokace e-mailových zpráv na e-mailových branách jsme zjistili, že téměř všechny (přes 97 procent) zablokované e-mailové zprávy byly zablokovány na základě informací z reputační databáze o serveru, ze kterého e-mailová zpráva přišla. V reputační databázi je serverům přiděleno skóre – pokud je serveru přiděleno nízké nebo negativní skóre, pak je komunikace z tohoto serveru zablokována. Necelá 2 procenta zablokovaných e-mailových zpráv byla zablokována kvůli tomu, že e-mailové adresy příjemců těchto zpráv neexistují, často se v tomto případě jedná o překlep v zadávání e-mailových adres. Také se může jednat o e-mailovou adresu, která v minulosti existovala, ale byla smazána, a útočníci ji mají stále uloženou v seznamech, případně je již neexistující adresa stále k dispozici na webových stránkách.

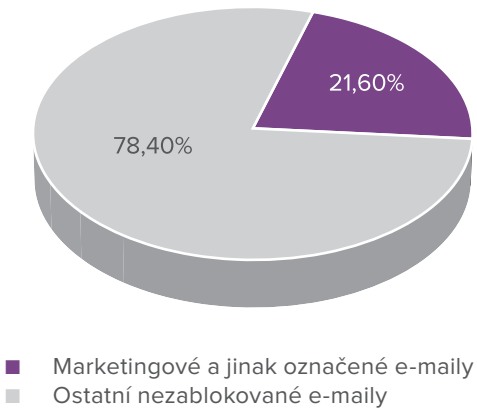
Téměř 1 procento zablokovaných e-mailových zpráv bylo zablokováno kvůli tomu, že zprávy byly klasifikovány jako spam, nebo byl jejich součástí škodlivý obsah. Většina zablokovaných e-mailových zpráv se škodlivým obsahem obsahovala URL adresu, která odkazovala na škodlivé webové stránky. Zbytek zablokovaných zpráv se škodlivým obsahem měl přílohu, která obsahovala škodlivý software.

Více než čtvrt procenta zablokovaných e-mailových zpráv bylo blokováno kvůli porušení DMARC politiky, která byla nastavena u doménového jména v adrese odesílatele (legitimní i podvržený) e-mailové zprávy. Což značí adopci bezpečnostních mechanismů SPF, DKIM a DMARC, které umožňují organizacím zamezit podvrhování jejich doménového jména v e-mailových zprávách.

Marketingové a jinak označené e-mailové zprávy (Graymail)

E-mailové brány jsou obvykle také schopny identifikovat a označovat e-mailové zprávy s marketingovým obsahem či zprávy ze sociálních sítí. Často jsou tyto typy e-mailových zpráv nazývané jako „Graymail“, protože někteří uživatelé považují tyto zprávy za nevyžádanou poštu, někteří si ale naopak tuto poštu vyžádali. Tyto zprávy se tedy pohybují v „šedé zóně“ mezi spamem a legitimním e-mailem. Proto se nedá jednoznačně určit, jestli se jedná o nevyžádanou poštu. Tyto e-mailové zprávy se tak automaticky neblokují, ale jen nějakým způsobem označují, například vložením textu „[Marketing]“ do předmětu e-mailové zprávy. Takto označených e-mailových zpráv bylo v námi získaném vzorku dat z e-mailových bran více než 18 procent z celkového počtu nezablokovaných e-mailových zpráv.

Podíl marketingových a jinak označených e-mailů na celkovém počtu nezablokovaných e-mailů



Zabezpečení e-mailové komunikace

Jan Kopřiva

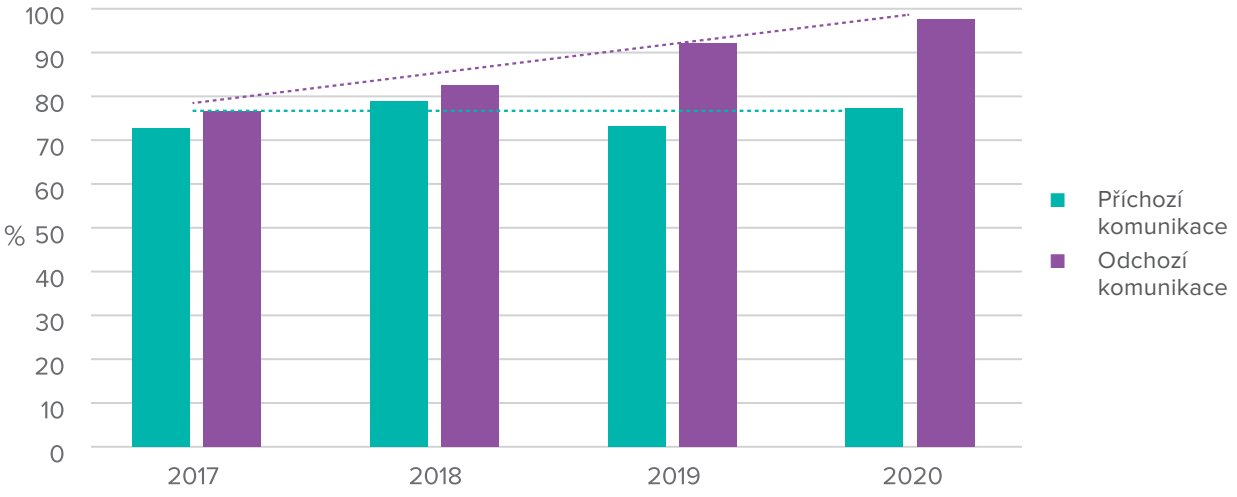
Tak jako každý rok, i letos se krátce pozastavíme také u dat týkajících se zabezpečení e-mailové komunikace na úrovni protokolu užívaného pro vlastní přenos zpráv. Aplikační protokol SMTP, který je pro komunikaci mezi e-mailovými servery odesilatelů a příjemců užíván, je standardně nešifrovaný, v důsledku čehož může hypotetický škodlivý aktér, který dokáže proniknout mezi komunikující servery, potenciálně odposlechnout obsah vyměňovaných zpráv.

Efektivní ochranu před únikem citlivých informací v podobných případech samozřejmě poskytuje zašifrování e-mailu jeho odesilatelem, žádná z technologií, které jsou k tomuto účelu užívány (S/MIME, PGP, ani proprietární řešení různých výrobců), však v současnosti není bez předchozí specifické konfigurace infrastruktury nebo výměny klíčů jednoduše plošně použitelná. Převážná většina e-mailové komunikace tak aktuálně není svými odesilateli šifrována.

K ochraně přenášených e-mailů však nemusí docházet pouze jejich zašifrováním na straně autora. Zabezpečení zpráv proti přečtení neoprávněnou třetí stranou při jejich přenosu po síti může poskytnout také zašifrování samotné komunikace mezi SMTP servery. Šifrování je v takových případech zajištěno pomyslným zabalením nešifrované SMTP komunikace do kryptografického tunelu zajišťovaného protokolem TLS (případně SSL). K sestavení zmíněného tunelu dochází automaticky (případně s pomocí mechanismu STARTTLS) v případech, kdy server odesilatele i server příjemce tuto možnost podporují. Aplikace kryptografické ochrany s pomocí popsaných mechanismů je tak z pohledu uživatelů e-mailových služeb zcela transparentní.

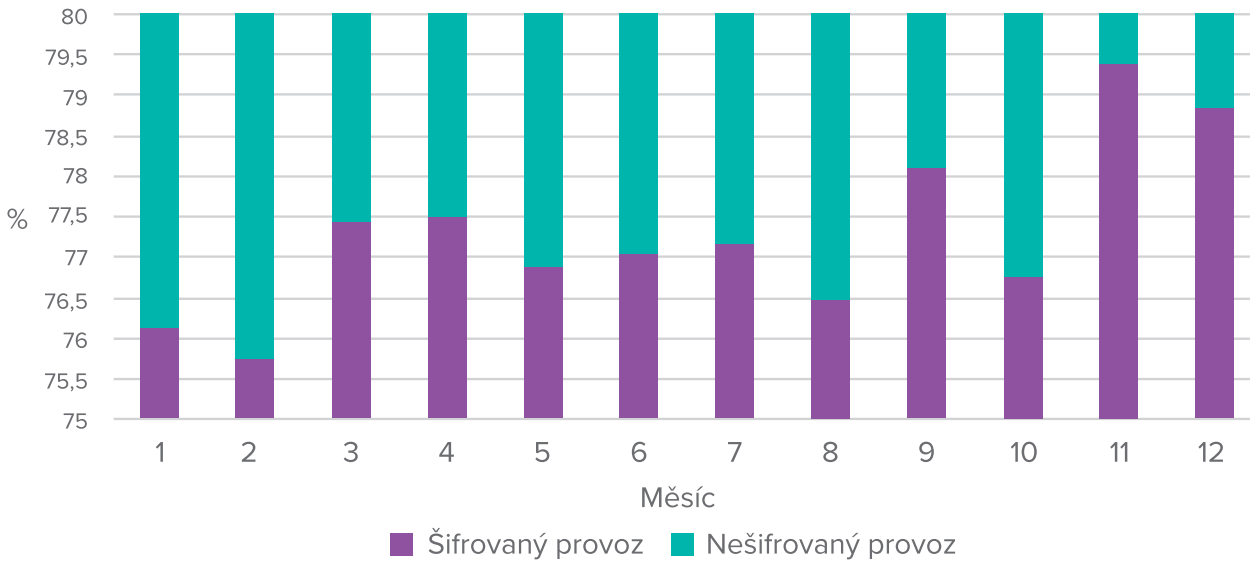
Počty poštovních serverů, které transparentní TLS šifrování provozu podporují, se kontinuálně zvyšují a stejně tak stoupají i počty zpráv, které jsou zmíněným mechanismem chráněny. Následující graf ukazuje vývoj procentuálního zastoupení chráněné komunikace u příchozích a odchozích zpráv v posledních 4 letech. Tak jako v předchozích letech, i letos byla data získána ze systémů ALEF Group a vybraných zákaznických infrastruktur v ČR, přičemž za rok 2020 jsou založena na téměř 98,5 milionech vyměněných zpráv. V rámci tohoto vzorku komunikace bylo v roce 2020 šifrováno 77,27 % příchozí komunikace a 97,55 % komunikace odchozí, což znamenalo použití šifrování u 94,15 % e-mailové komunikace celkem.

E-mailová komunikace šifrovaná s pomocí TLS

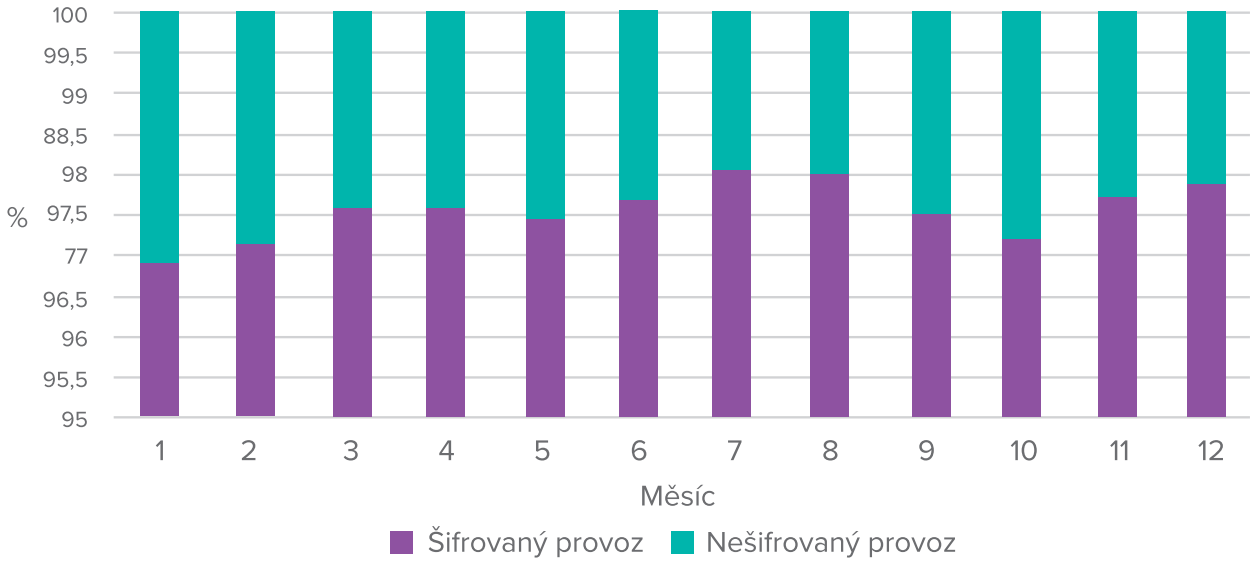


Následující grafy ukazují procentuální zastoupení šifrované a nešifrované komunikace v jednotlivých měsících roku 2020.

Šifrování příchozího e-mailového provozu s pomocí SSL/TLS v roce 2020



Šifrování odchozího e-mailového provozu s pomocí SSL/TLS v roce 2020



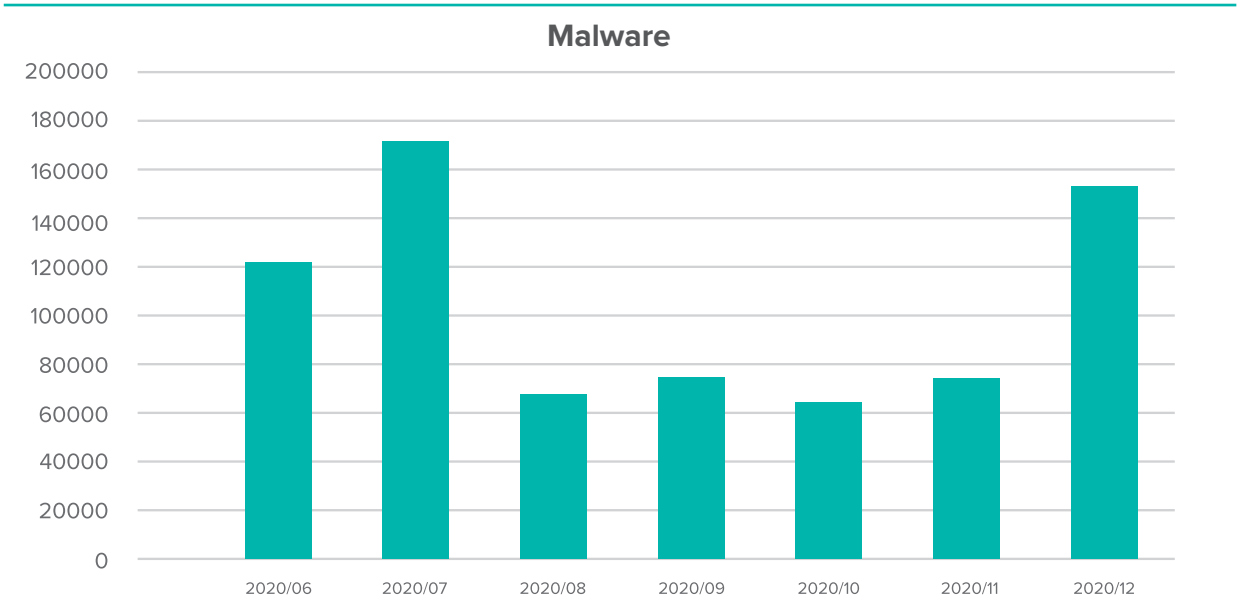
I přes občasné propady je z obou předchozích grafů relativně dobře patrný dlouhodobý trend růstu šifrovaného provozu na úkor provozu nešifrovaného a lze se domnívat, že tento trend bude i v nadcházejících letech stále pokračovat.

Analýza událostí zachycených IPS sondami

Stanislav Techlovský

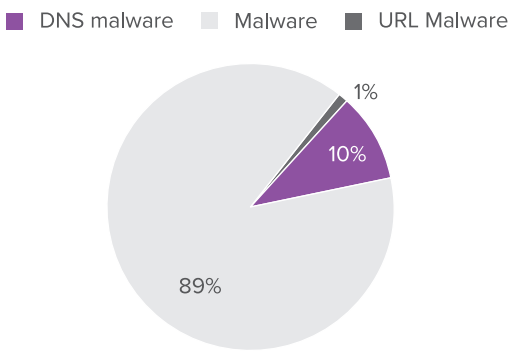
Následující část reportu se zabývá analýzou dat z IPS (Intrusion Prevention System) sond pod správou společnosti ALEF Nula a.s. Analýza se zaměřuje na data z období posledních dvou kvartálů roku 2020.

V první části analýzy se nejprve podíváme na phishing. IPS sondy detekovaly incident vždy, když se uživatel pokusil navštívit blokované phishingové stránky. Nejvíce incidentů z minulého roku bylo detekováno v měsíci říjnu v množství 12731 incidentů, což je bezmála 120x násobné zvýšení oproti předchozímu roku za stejný měsíc. Ke konci roku 2020 došlo k poklesu počtu phishingových útoků na celkové množství 3814. Jedná opět o 7x násobné zvýšení oproti předešlému roku za totožné období.



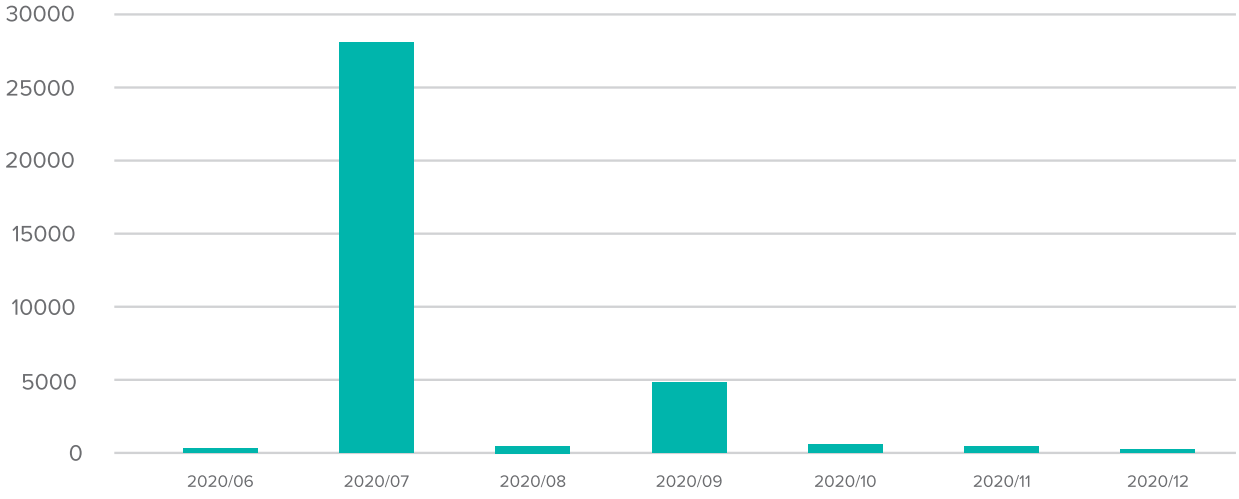
Za poslední dva kvartály roku 2020 bylo největší množství incidentů spojených s malwarem zachyceno IPS systémy v měsíci červenec – šlo přes 171 tisíc událostí. Jedná se téměř o 5x násobné zvýšení oproti předchozímu roku za totožné období. V prosinci bylo detekováno bezmála 153 tisíc incidentů, oproti předchozímu měsíci listopadu jde o 333 % nárůst. Vyšší četnost těchto útoků je dána vyšší uživatelskou aktivitou na internetu spojenou s koncem roku, k obdobnému nárůstu incidentů v tomto období dochází pravidelně, jak ukazují mimo jiné i data z předešlých let.

Malware struktura



Detekce spojené se škodlivým kódem člení sledované IPS systémy do tří základní kategorií. V kategorii malware se nacházejí události, při kterých byla identifikována shoda s reputační databází IPS, která obsahuje IP adresy, na nichž se vyskytuje nebo vyskytoval malware. Porovnává se při tom jak zdrojová, tak cílová IP adresa. Kategorie URL malware obsahuje pouze adresy, na nichž byl zaznamenán výskyt malwaru. Samotnou detekci provádí sondy na základě analýzy webového provozu s pomocí kontroly URL. Poslední kategorií je DNS malware, reputační databáze v tomto případě obsahuje seznam domén, u kterých byl detekován malware. Událostmi jsou v takovém případě detekované DNS dotazy na škodlivé domény, o jejichž překlad se pokusil malware nacházející se uvnitř chráněných sítí. Za sledované období posledních dvou kvartálů roku 2020 byla struktura detekcí malwaru následující: z 89 % byly detekce výskytu malware realizovány s pomocí reputační databáze, pouze z 10 % se jednalo o detekce s pomocí kontroly DNS a zbylé 1% malwaru bylo odhaleno s využitím URL kontroly (viz. graf Detekce škodlivého kódu).

Cryptomining



Jednotlivé „Cryptomining“ události jsou detekovány pomocí reputační databáze IP adres, u nichž byly v minulosti a současnosti vedeny pokusy o těžbu kryptoměn. Detekce se dále zaměřuje na stahování a analyzování binárních dat, webových klientů, těžebních protokolů, blacklist domén a SSL certifikátů. V červenci 2020 byl zachycen nejvyšší počet pokusů o těžbu kryptoměn o celkovém množství přes 28 tisíc pokusů. Oproti předchozímu měsíci červnu se jednalo o 880 % nárůst. V posledním kvartálu loňského roku došlu k pozvolnému poklesu, přičemž nejmenší množství pokusů bylo zaznamenáno v měsíci prosinec a to pouze 253 pokusů o těžbu kryptoměn.

Analýza dostupnosti šifrovaného DNS v roce 2020

Jan Šimůnek

Protokol DNS byl od roku 1983 přenášen v prostředí internetu výhradně v otevřené textové podobě. Jednotlivé dotazy směřující na veřejné rekurzivní DNS resolvery tak bylo snadné zneužít pro monitorování (DNS eavesdropping) a přesměrování (DNS hijacking) uživatelského provozu.

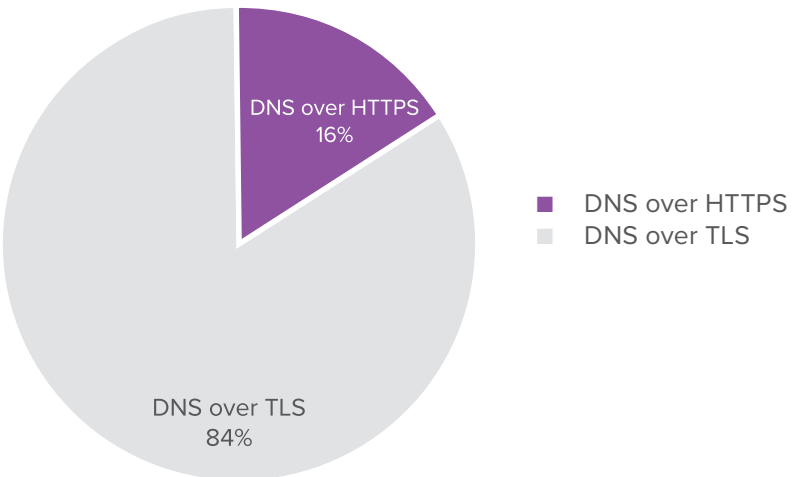
Tento ne zcela ideální stav vedl k vytvoření šifrovaných variant protokolu DNS, ze kterých následně vznikly dvě standardizované varianty RFC 8484 a RFC 7858, známé pod zkratkou DoH (DNS over HTTPS) a DoT (DNS over TLS). Účel těchto protokolů je prostý – skrýt komunikaci na úrovni DNS před pozorováním třetích stran. Tento krok vede z pohledu uživatelů k ochraně jejich soukromí a zachování integrity jednotlivých dotazů. Z pohledu zachování bezpečnosti ve firemním prostředí jsou však tyto protokoly více než problematické. Velká množina bezpečnostních prvků je založena právě na sledování DNS provozu a díky tomu je schopna včas zachytit pokusy o přístup na phishingové domény, pokus o exfiltraci dat nebo komunikaci s command & control servery z infikovaných stanic. S použitím šifrované alternativy pohled do DNS provozu vymizí a případné blokování DNS dotazů tak není možné.

Porovnání veřejně dostupných DNS resolverů v roce 2020

Jak to bylo s dostupností veřejných DNS serverů, které nabízí šifrované DNS, v roce 2020 se podíváme v následujících části.

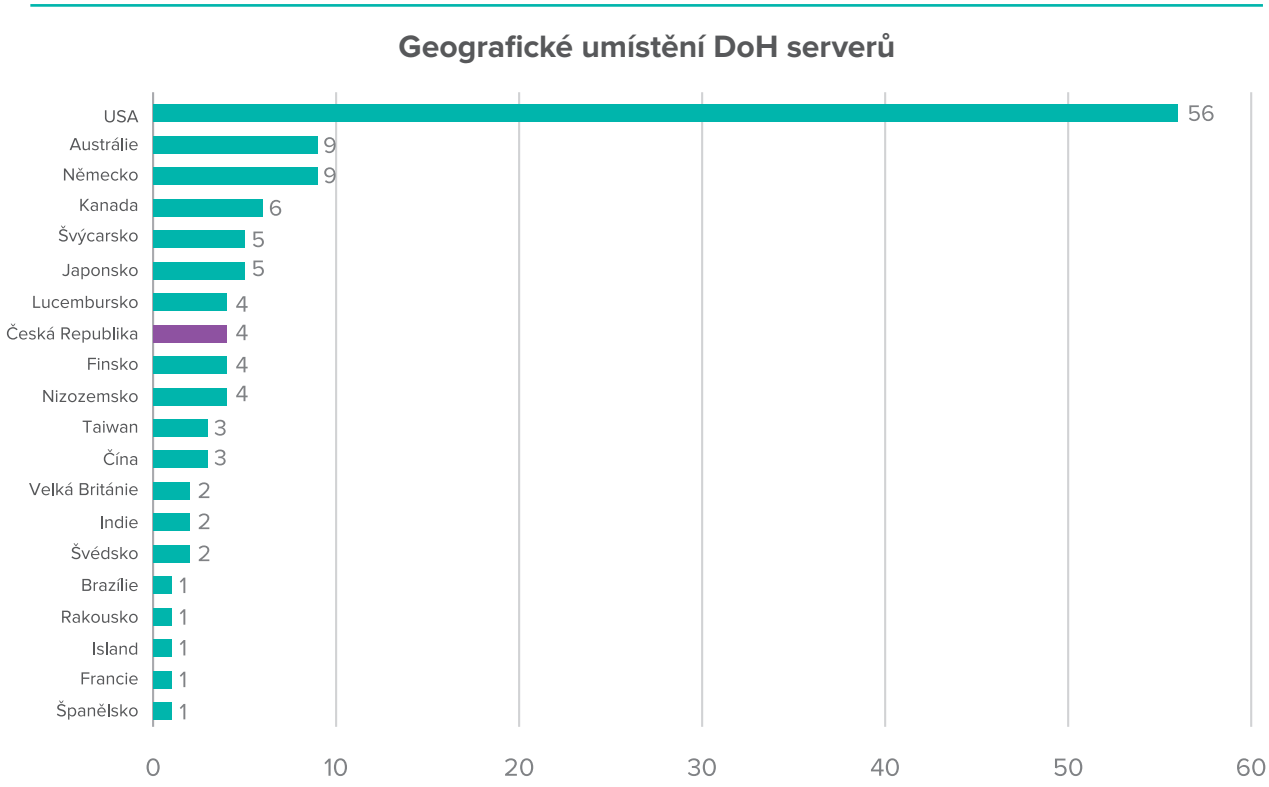
Pro vytvoření přehledu byly použity nástroje Shodan a Zmap, pomocí nichž byl procházen IP adresní rozsah internetu. Získaná data byla následně filtrována tak, aby odpovídala implementaci dle RFC (specifikace portu, URI a odpověď na dotaz). Podíl dostupnosti hovoří jednoznačně ve prospěch DoT, jehož zastoupení tvořilo 84 % oproti zbylým 16 % tvořených DoH.

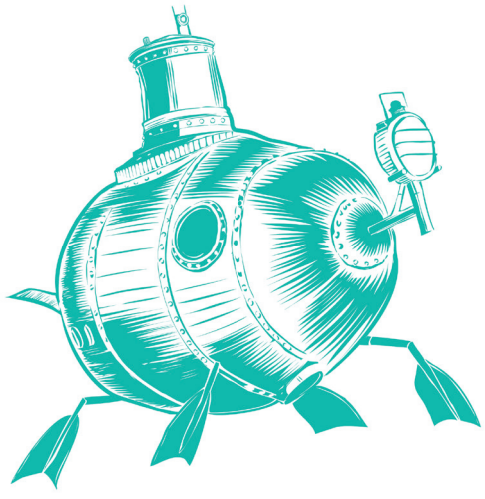
Porovnání veřejně dostupných DNS resolverů podporujících DoH nebo DoT



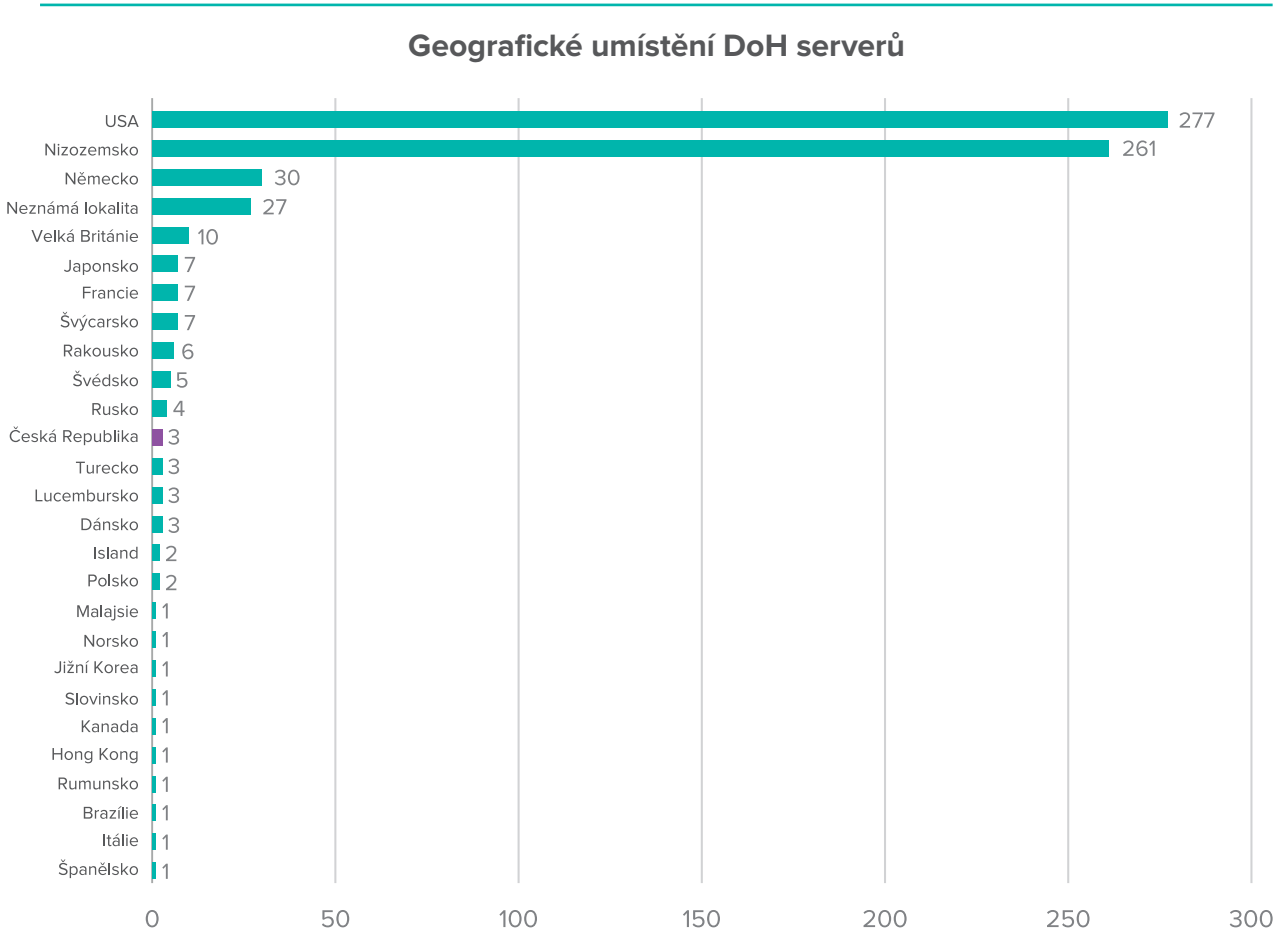
Celkově bylo identifikováno 667 veřejných DoT resolverů a 123 DoH resolverů. Oproti běžným DNS resolverům dle RFC 1035, kterých bylo objeveno 2 559 031, je počet nasazení šifrovaných variant prozatím minimální. Je nicméně vhodné poznamenat, že mezi počtem „šifrujících“ DNS serverů a množstvím jimi zodpovězených dotazů neexistuje žádný lineární vztah a je tak pravděpodobné, že i přes rozdíl mnoha řádů mezi klasickými DNS servery a DoH a DoT servery odbavovaly v loňském roce „šifrující“ DNS překladače již značnou část celosvětového provozu.

Geografickému zastoupení DoH serverů odpovídá následující graf. Největší zastoupení bylo nalezeno v USA, v České republice byly identifikovány 4 veřejné resolvery.





V případě dostupnosti DoT serverů je opět nejvíce zastoupena lokalita USA a následuje Nizozemsko. V České republice byly identifikovány 3 DoT resolvery.



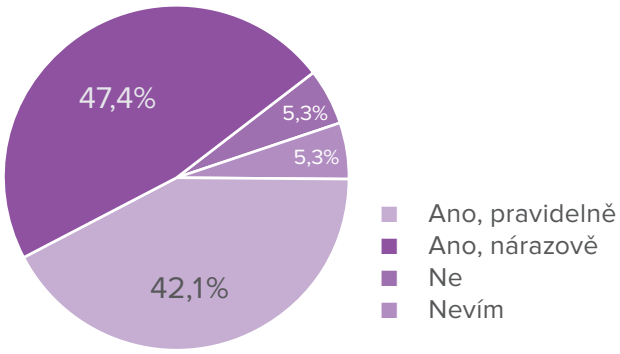
Zdroje:
[1] C. Lu et al., “An End-to-End, Large-Scale Measurement of DNS-over-Encryption: How Far Have We Come? CCS CONCEPTS • Networks ➔ Application layer protocols; Network measurement; Naming and addressing. KEYWORDS Domane Name System, DNS Privacy, DNS-over-TLS, DNS-over- HTTPS, DNS Measurement ACM Reference Format,” 2019, doi: 10.1145/3355369.3355580.
[2] “The ZMap Project,” Zmap.io, 2020. https://zmap.io/ (accessed Feb. 15, 2021).
[3] “Shodan,” Shodan.io, 2013. https://www.shodan.io/ (accessed Feb. 15, 2021).
[4] “dnspython | dnspython,” Dnspython.org, Jan. 07, 2021. https://www.dnspython.org/ (accessed Feb. 16, 2021).

Bezpečnostní testování v roce 2020 a výhled na rok 2021

Jana Little

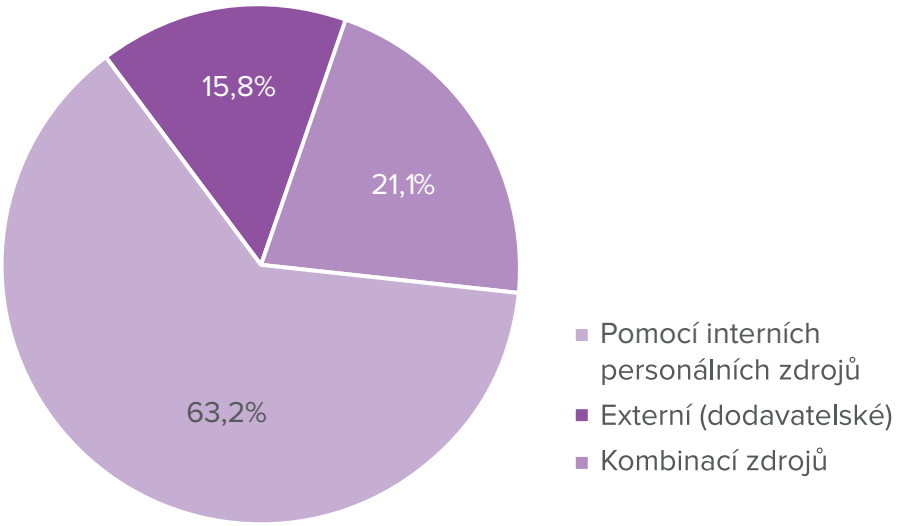
Jako v minulém Security reportu se budeme v tomto článku věnovat bezpečnostnímu testování. Rádi byste věděli, jaké jsou dle dotázaných organizací plány na rok 2021 a jak si stál rok 2020 z pohledu bezpečnostního testování? Pokud si vzpomínáte na minulý článek, zajímalo nás, jak se dotázané organizace staví k vulnerability testům / testům zranitelností a k penetračnímu testování. V tomto článku to nebude jinak. Pojďme se dozvědět jakým směrem uchylují pozornost organizace v rámci bezpečnostního testování a jaké jiné zajímavé typy bezpečnostního testování organizaci využívají?

Prováděla Vaše organizace v roce 2020 vulnerability testy / testy zranitelnosti?



V minulém reportu jsme se zajímali, zda dotazované organizace budou věnovat pozornost vulnerability testům v roce 2020. V plánu to mělo 90% z nich. A realita? Oproti roku 2019 došlo v roce 2020 skokově k navýšení na 89,5%. Tedy plán odpovídá skutečnosti. Tyto testy byly prováděny pravidelně i nárazově. V celkovém souhrnu vyšlo najevo, že pouze 5,3% dotázaných organizací tyto testy vůbec neprovádělo.

Jak jste v roce 2020 realizovali vulnerability assessment scany?



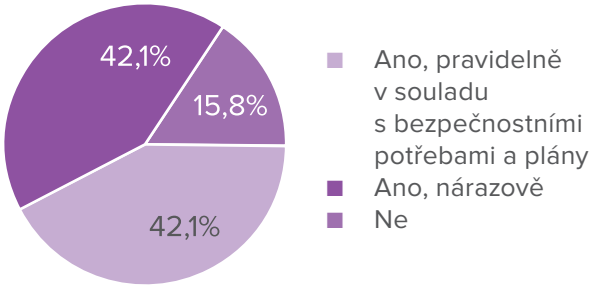
Velká část dotázaných organizací uvedla, že se vulnerability testy / testy zranitelností v roce 2020 zabývala. Zajímalo nás, jakým způsobem testy realizovali. V roce 2019 dali organizace přednost realizaci pomocí interních personálních zdrojů. V roce 2020 tomu nebylo jinak. Nejvíce docházelo k realizaci vulnerability assessment scanů interními zdroji. Kombinaci zdrojů (tedy dodavatelské řešení a zapojení svých interních zdrojů) využilo 21,1 % dotázaných organizací. Žádná dotázaná organizace v roce 2019 nepřenechala realizaci testů pouze na externího dodavatele. V roce 2020 tomu bylo jinak. Jak je z grafu patrné, 15,8 % organizací realizovalo scany pomocí dodavatelského řešení.

Penetrační testování v roce 2020

V této části se podíváme na to, jak to bylo v případě penetračního testování. Oproti roku 2019, kdy 65 % dotázaných organizací uvedlo, že se penetračnímu testování věnuje, v roce 2020 můžeme radostně oznámit, že se tento počet zvýšil. Penetračnímu testování se v loňském roce věnovalo necelých 85 % dotázaných organizací. Je to skvělá zpráva, jelikož tento typ bezpečnostních testů představuje způsob, jak nejen identifikovat přítomnost zranitelností v systémech organizace, ale také prokázat, že jejich zneužití je reálně možné, a demonstrovat míru rizika, kterou skutečně představují pro organizaci.

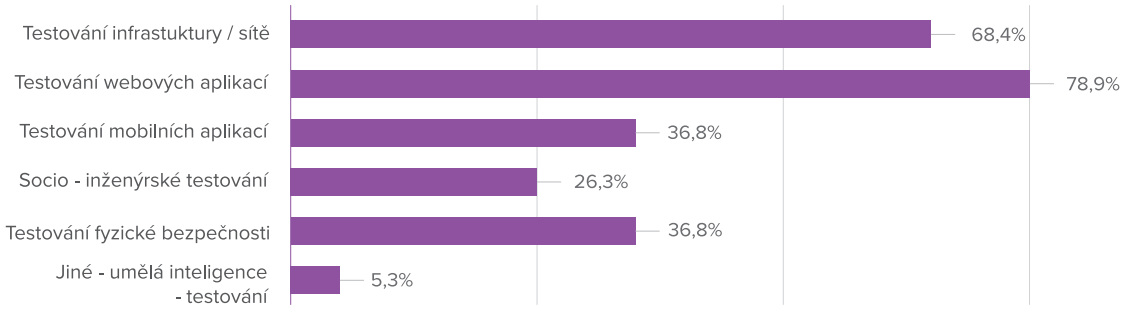
Jak z dotazníku vyplynulo, polovina dotázaných organizací se penetračnímu testování v roce 2020 věnovala pravidelně. V roce 2019 bylo nejvíce penetračních testů uskutečněno pomocí externí dodávky. V roce 2020 tomu bylo naopak. Nejvíce organizací (44,4 %) realizovalo penetrační testy pomocí interních personálních zdrojů. Lze se domnívat, že tento trend ovlivnila světová pandemie a také zvyšující se kvalifikace odborníků na v oblasti Cybersecurity.

Prováděla Vaše organizace v roce 2020 penetrační testování?



O jaké typy penetračního testování šlo? Nejvíce organizací testovalo v roce 2020 webové aplikace, infrastrukturu a mobilní aplikace. Vysoký zájem byl také o testování fyzické bezpečnosti. Zajímavostí je, že 5% dotázaných uvedlo, že v roce 2020 realizovaly penetrační testování pomocí umělé inteligence.

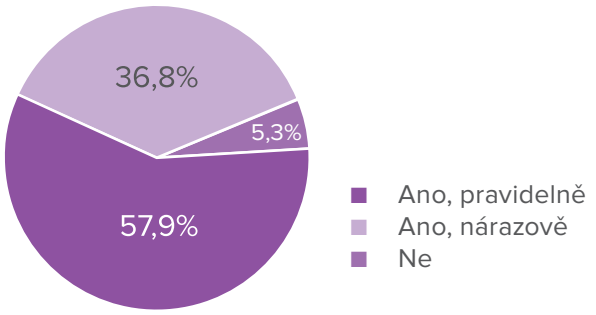
Jaký typ penetračního testování jste v roce 2020 prováděli?
Vyberte jednu nebo více z nabízených možností:



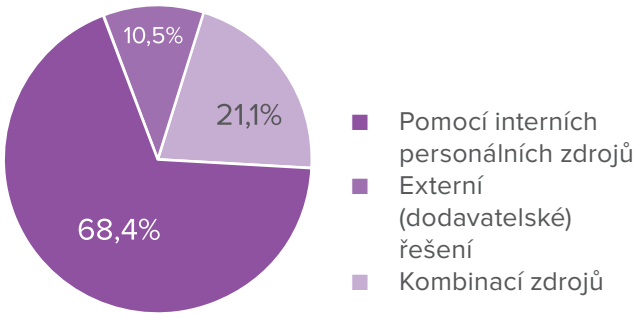
Bezpečnostní testování v roce 2021

A jak je to s výhledem na další rok? Necelých 60 % organizací má na rok 2021 v plánu věnovat se vulnerability testům / testům zranitelnosti pravidelně. Největší procento organizací má v plánu testování zranitelností realizovat s pomocí interních personálních zdrojů či využití interních zdrojů spolu s externí dodavatelskou firmou. Pouze malá část dotázaných (10,5 %) plánuje realizovat testy jen prostřednictvím dodavatelského řešení.

Máte v roce 2021 v plánu realizovat vulnerability testy/testy zranitelnosti?



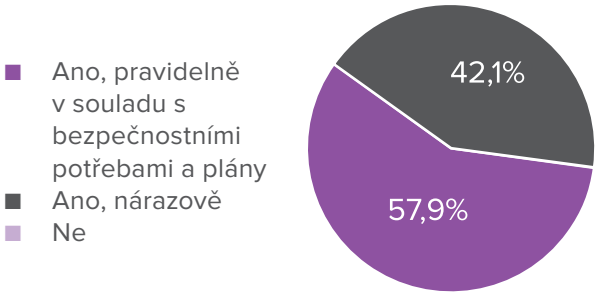
Jak budete v roce 2021 realizovat vulnerability assessment scany?



Penetrační testování v roce 2021

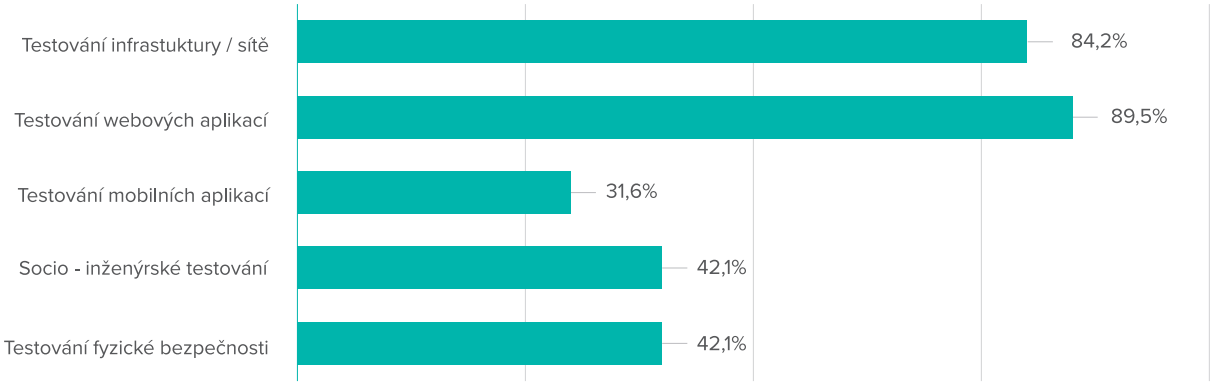
Jak z dotazníku vyplynulo, všechny dotázané organizace mají v plánu se v roce 2021 věnovat penetračnímu testování. Je to dobrá zpráva oproti roku 2019, kdy necelých 10 % dotázaných organizací uvažovalo se těmto testům vůbec nevěnovat. Nejvíce se organizace mají v plánu věnovat pravidelnému testování v souladu s bezpečnostními potřebami a plány, případně hodlají využívat nárazové penetrační testy.

Máte v roce 2021 v plánu realizovat penetrační testování?

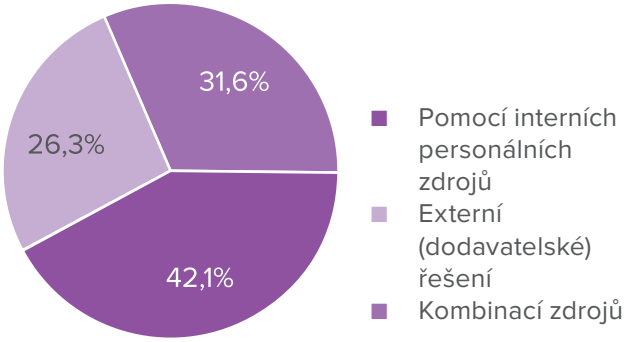


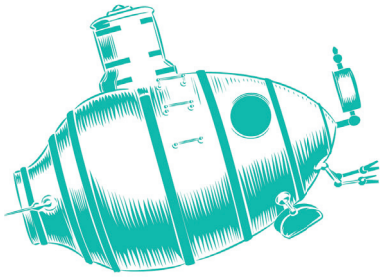
Jak je z níže uvedeného grafu patrné, zaměření testů bude mít obdobný charakter jako v roce 2020. Největší zájem mají organizace o testování webových aplikací, testování infrastruktury / sítí, testování fyzické bezpečnosti a v neposlední řadě provádění socioinženýrských testů. 42,1% dotázaných organizací má v plánu využít k tomu interní personální zdroje. 26, 3 % dotázaných bude realizovat penetrační testy pouze pomocí dodavatelského řešení a zbylých 31, 6 % využije interní zdroje s využitím dodavatelského řešení.

Jaký typ penetračního testování budete v roce 2021 provádět? Vyberte prosím jednu nebo více z nabízených možností:

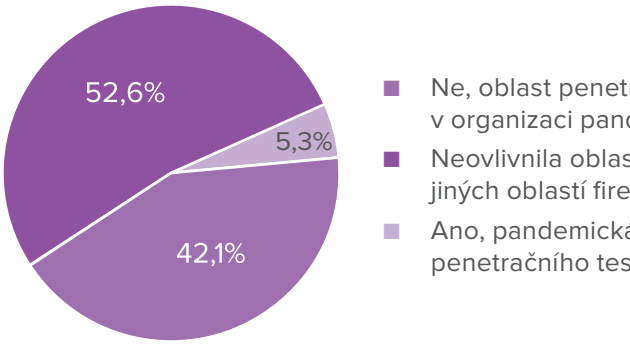


Jak budete v roce 2021 realizovat penetrační testování?





Ovlivnila pandemie týkající se COVID-19 nějakým způsobem oblast penetračního testování ve Vaší organizaci?



Zajímalo nás, jakým způsobem ovlivnila světová pandemie COVID-19 penetrační testování. Nejvíce dotázaných organizací (52,6 %) uvedlo, že pandemie konkrétně penetrační testování neovlivnila, ale promítla se ovšem do jiných oblastí firemního IT. Zajímavé a pozitivní je také zjištění, že ve 42,1% případech pandemie oblast penetračního testování ani v jinou oblast IT neovlivnila.

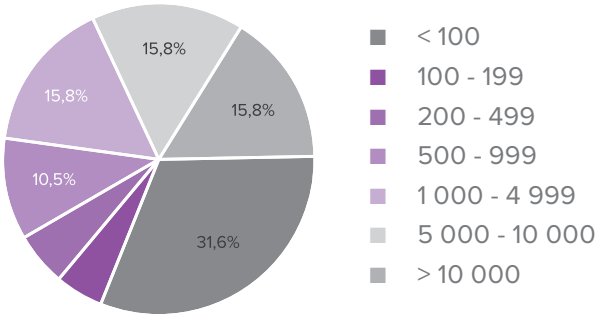
Bezpečnostní dohled a stav Security Operations v roce 2020

Daniel Neumann

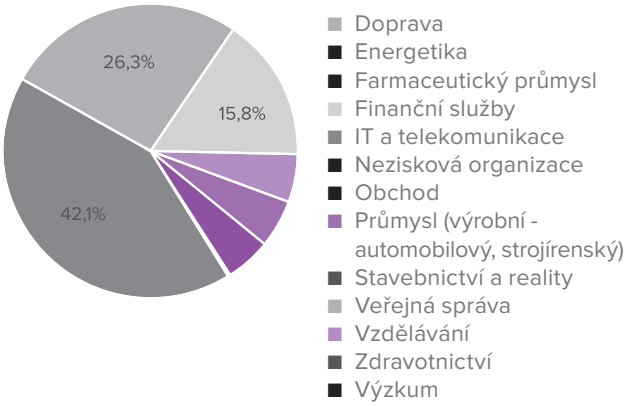
Bezpečnostní dohled je v oblasti IT pojem zavedený, často probíraný a v každé organizaci ne vždy správně podchycený. Toto tvrzení potvrdí i data získaná prostřednictvím dotazníkového šetření mezi klienty Alef Group, kterým tímto velice děkujeme za spolupráci.

Velikost konkrétní organizace představuje podstatný faktor, jak k otázce bezpečnostního dohledu přistupovat. Přibližně třetina dotázaných spadá do kategorie organizací s méně jak 100 zaměstnanci, 10,5% má mezi 500–999 zaměstnanci a dále se stejným procentuálním zastoupením 15,8% pracujeme s intervaly 1.000–4.999/5.000–10.000/10.000+ zaměstnanců.

Kolik zaměstnanců má Vaše organizace?



V jakém sektoru Vaše organizace působí?

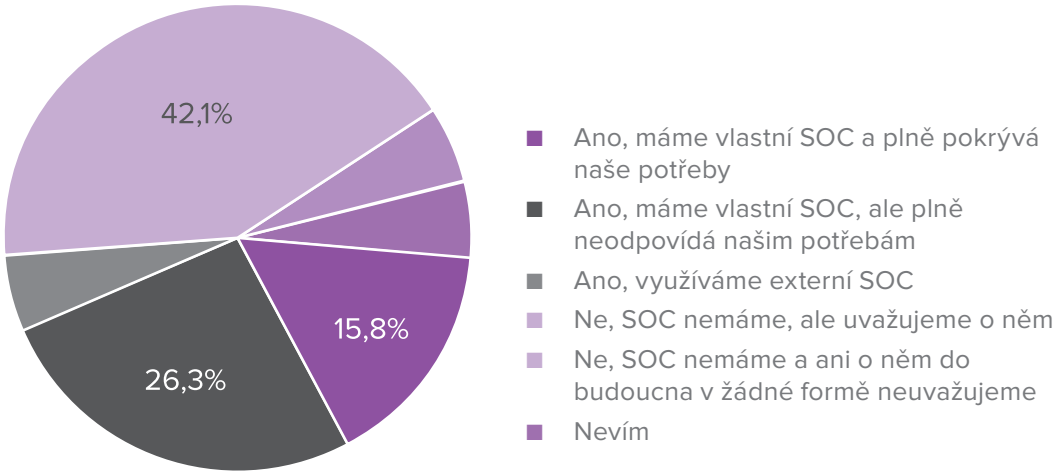


Pro lepší vypovídací hodnotu jsme dotazované požádali o zařazení své organizace do konkrétního sektoru. Silnou převahu oproti ostatním sektorům, se zastoupením více jak 40%, vychází pro IT a telekomunikace. Zhruba čtvrtinový podíl připadá na státní správu, za níž následuje s 15,8% obor finančních služeb. Minoritní zastoupení vykazuje doprava, výzkum a vzdělávání.

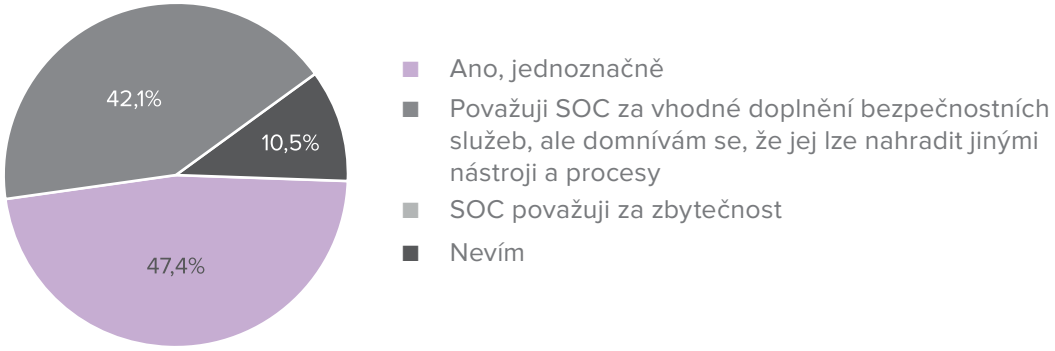
Nyní již přistupme k samotnému dotazníkovému šetření. Z odpovědí první otázky si dokážeme udělat dobrý přehled o tom, kdo a jakým způsobem využívá služeb SOC. Privátní a plně vyhovující SOC vykázalo 15,8% respondentů. V porovnání s předchozím rokem se jedná o 10% pokles, neboť v roce 2019 tímto způsobem odpověděla přesně čtvrtina dotázaných. Tento podíl aktuálně vykázali ti, kteří sice mají vlastní SOC, ten ale plně neodpovídá potřebám konkrétní organizace. Nejsilnější zastoupení již tradičně představují organizace, které vlastní SOC nemají, ale uvažují o něm. Prakticky obdobný výsledek jsme pozorovali v roce minulém. Externí dohled využívá pouze 5% dotazovaných. Stejné zastoupení SOC nemá a ani o něm do budoucna neuvažuje. Je zajímavé sečíst odpovědi ze dvou nejčastěji zastoupených skupin a zjistit tak, že přibližně dvě třetiny organizací buď SOC vůbec nemá (i když o něm uvažuje) nebo jej má, ovšem nikoli ve vyhovující podobě.

Při schůzkách s klienty se tématu bezpečnostního dohledu samozřejmě věnujeme velmi často. Mohu konstatovat, že většinou opravdu o vlastním SOC uvažují (bavíme se nyní o větších zákaznících, kteří mají vždy alespon několik stovek uživatelů). Méně potěšující je ovšem skutečnost, že „fáze uvažování“ trvá několik let a během nich se téma bezpečnostního dohledu interně nikam neposune, resp. někdy možná ano, a to do daleké budoucnosti. Důvodů, proč tomu tak je, může být spousta a nemám v plánu je zde všechny vyjmenovávat. Podíval bych se na věc raději z jiného úhlu. Nemáte možnost SOC zastřešit interními kapacitami? Nejste si vlastně jisti, zda by pro Vás vůbec měl SOC smysl a představoval dostatečnou přidanou hodnotu? Řešení je nasnadě. SOC zajišťovaný externím subjektem, a to v režimu, který by Vám umožnil reálně ověřit, zda má vůbec SOC pro Vaše prostředí smysl. Režimem mám na mysli takový rozsah, který nebude představovat přílišnou finanční zátěž, ovšem výstupy z něj budou dostatečně relevantní. Nebavíme se tedy s největší pravděpodobností o režimu 24x7, či 8x5, ale o jiné flexibilní formě. Více se k tomu dostaneme v článku níže.

Využíváte služeb SOC (Security Operations Center)?



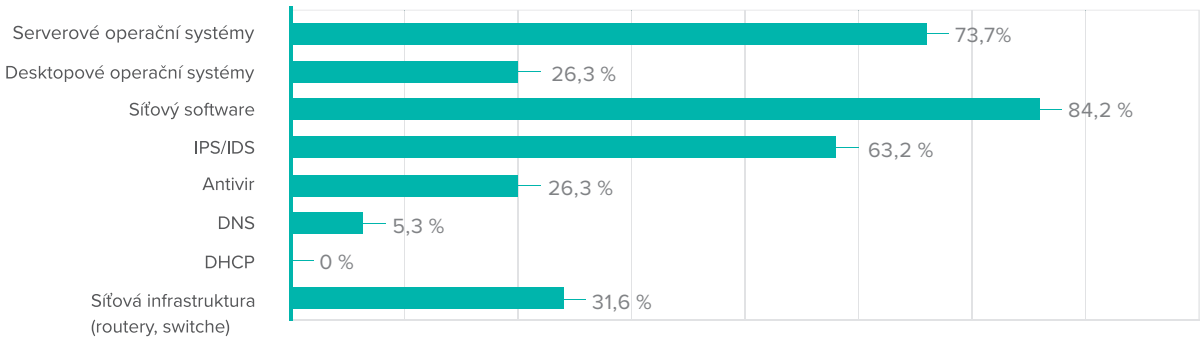
Považujete SOC za nutnost?



Považujete SOC za nutnost? Téměř polovina odpovědí zněla „ano, jednoznačně“. O něco méně odpovědí se přiklánělo k názoru, že SOC může být sice vhodným doplněním bezpečnostních služeb, nicméně jej lze nahradit jinými nástroji a procesy. Deset procent tazatelů si odpovědí není jisto.

Mezi základní činnosti nezbytné k ověření zabezpečení IT prostředí organizace patří zaznamenávání dat za účelem jejich analýzy (logování). Celkem jednoznačně obsadil pomyslný stupeň vítězů síťový firewall následovaný serverovými operačními systémy a IPS/IDS. Obdobný význam je přikládán prvkům síťové infrastruktury, desktopovým operačním systémům a antiviru. V porovnání s minulým rokem nedošlo k výrazným změnám v odpovědích, za zmínku stojí pouze snad jen mírný pokles důležitosti přisuzované IPS/IDS a síťové infrastruktuře.

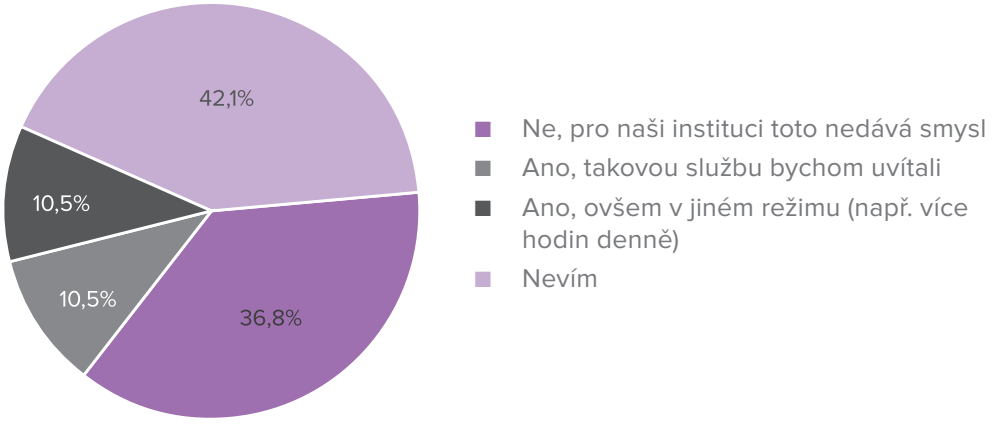
Logy z jakých tří typů systémů považujete za nejpodstatnější z pohledu použití v rámci bezpečnostní analýzy? (Vyberte maximálně 3 odpovědi)



Bezpečnostní dohled ve „flexibilním“ režimu vycházejícím z potřeb zákazníka jsem zmínil v předchozí části článku. Ne vždy zákazník potřebuje real-time dohled – jeho prostředí nespadá do kategorie, v němž je třeba vědět o každém kybernetickém bezpečnostním incidentu a neprodleně jej řešit. Plně by postačovalo tyto incidenty monitorovat s určitým časovým odstupem a řešily by se pouze ty události, které jsou opravdu kritické.

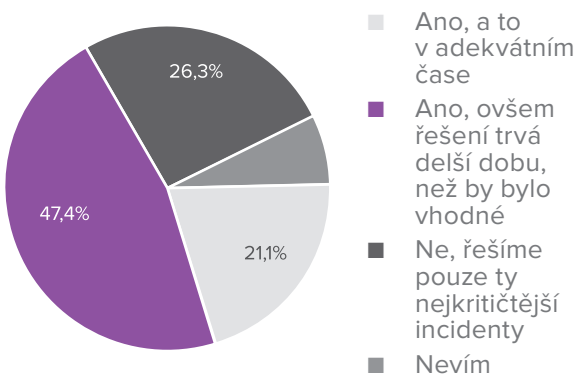
Důvod ale může být mnohem prozaičtější – finanční náklady. SOC v režimu 24x7 (ale i 8x5) je finančně velice nákladný, a ne každá instituce si může tuto formu dohledu dovolit. Nebo jednoduše nechce, protože jsou jiné položky, do kterých je třeba investovat. Řešením by mohl být bezpečnostní dohled v režimu např. 1 hodinu každý pracovní den. Více jak 40 % tazatelů bohužel neví, zda právě tato forma dohledu by byla tou pravou, třetina respondentů si myslí, že pro jejich organizaci SOC v této podobě nedává smysl. Pouze 10,5 % by naopak tuto formu dohledu uvítala, případně upravila její rozsah.

Byla by pro Vás zajímavá služba SOC v režimu 1 hod/pracovní den na vyhodnocování detekovaných incidentů za předchozí den?



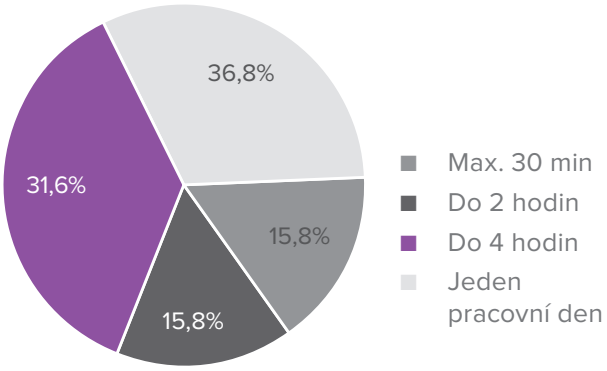
Navzdory tomu, kolik finančních prostředků investujeme do bezpečnostních opatření, dojde v určité časové periodě k bezpečnostnímu incidentu. Ten je potřeba řešit, a to jak reaktivně, tak proaktivně. Aby však bylo možné bezpečnostní incident řešit, musí být v prvé řadě co nejdříve zjištěn. Řešit incident v adekvátním čase zvládá zhruba pětina oslovených, čtvrtina řeší pouze ty nejkritičtější incidenty a necelá polovina se sice věnuje každému odhalenému bezpečnostnímu incidentu, ovšem jeho řešení trvá delší dobu, než považuje za vhodné.

Zvládáte řešit každý odhalený bezpečnostní incident?



Uvedli jsme, že reakční doba je při řešení bezpečnostních incidentů klíčová. Jeden pracovní den připadá více jak třetině dotázaných dostatečná, necelá třetina se ztotožňuje s polovinou pracovního dne, tedy časem 4 hodin. Zastoupení ve výši 15,8 % má skupina, pro níž je dostatečnou dobou pro řešení nekritického bezpečnostního incidentu čas max. dvou hodin, stejný podíl tazatelů preferuje vyřízení incidentu za méně než 30 minut.

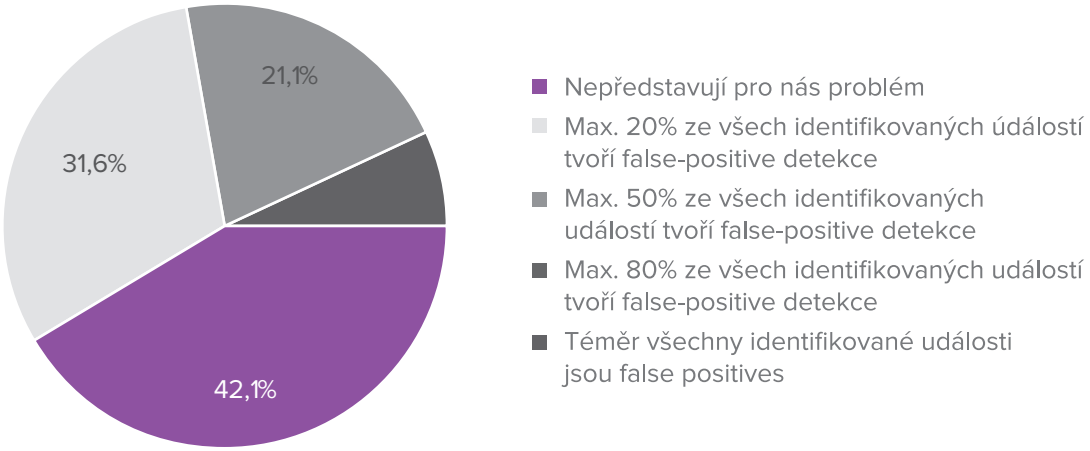
Jakou reakční dobu na bezpečnostní (nekritický) incident považujete za dostatečnou?



Výstupy z automatizovaných skenů sítě, IPS, SIEM a dalších nástrojů nemusí vždy přinášet validní data. Může se jednat o chybné detekce zranitelností a bezpečnostních incidentů, tzv. „false-positive“ detekce. Pokud se musí pracovníci IT zabývat vysokým počtem takovýchto detekcí, představuje to plýtvání jejich časem, resp. plýtvání zdroji celé organizace.

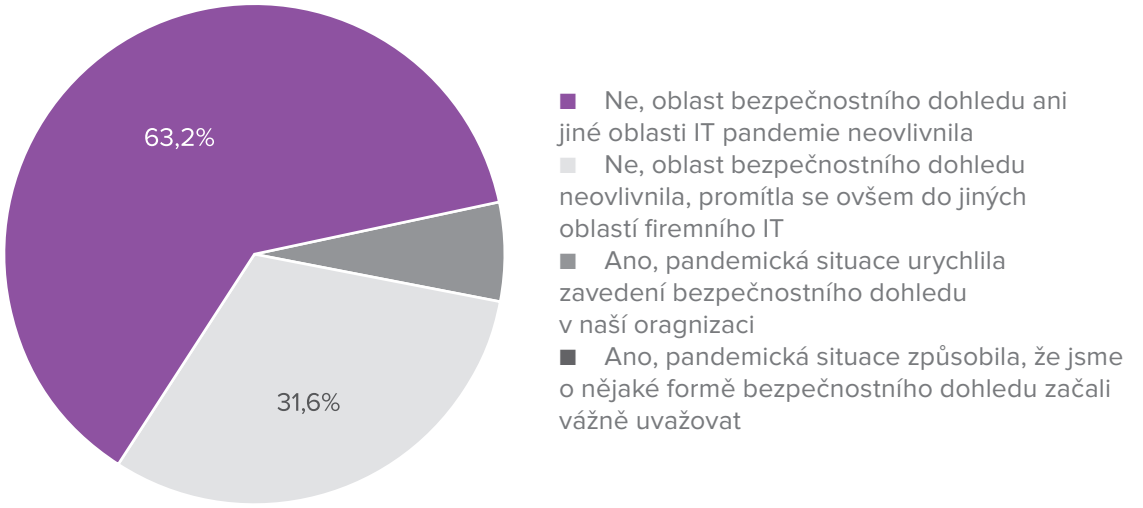
Jsou tedy „false-positive“ detekce problémem, se kterým se v praxi setkáváme? Získaná data ukazují, že více jak 40 % tazatelů nemá s uvedeným typem detekcí problém. V cca třetině případů tvoří méně jak pětinu všech identifikovaných událostí. Pětina organizací uvedla, že max. 50 % ze všech identifikovaných událostí tvoří právě „false-positive“ detekce.

Jsou false-positive detekce problém, který Vás nadmíru zatěžuje? Pokud ano, kolik % z celkového počtu identifikovaných bezpečnostních událostí představují právě false positives?



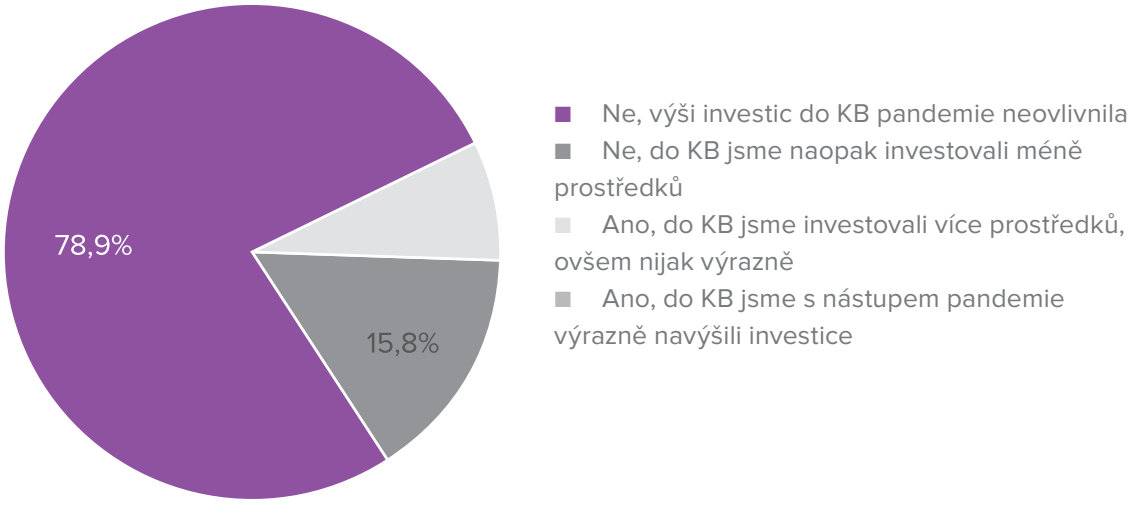
Rok 2020 byl v jistém směru unikátní. Bohužel nikoli v pozitivním slova smyslu. Je tím myšlena pandemie týkající se COVID – 19. Předmětem tohoto článku není řešit počty infikovaných, hodnotit přístup naší vlády k řešení situace, ani odhadovat, jak účinná bude vakcinace. Vyvstala otázka, zda pandemie nějakým způsobem ovlivnila oblast bezpečnostního dohledu. Zhruba dvě třetiny respondentů odpověděly, že pandemie oblast bezpečnostního dohledu neovlivnila, ale promítla se do jiných oblastí firemního IT. U třetiny organizací pandemie oblast IT neovlivnila žádným způsobem. Nejmenší zastoupení, tedy 5,3 %, vykázaly organizace, v nichž naopak pandemie zavedení bezpečnostního dohledu urychlila.

Ovlivnila pandemie týkající se COVID-19 nějakým způsobem oblast bezpečnostního dohledu ve Vaší organizaci?



Závěr průzkumu se věnoval výši investic do kybernetické bezpečnosti v návaznosti na pandemickou situaci. Téměř 80 % účastníků průzkumu uvedlo, že výši investic do kybernetické bezpečnosti pandemie neovlivnila. V případě 15,8 % respondentů došlo k omezení investic do oblasti KB.

Změnila se s nástupem pandemie COVID-19 výše investic do oblasti kybernetické bezpečnosti (KB) ve Vaší organizaci?



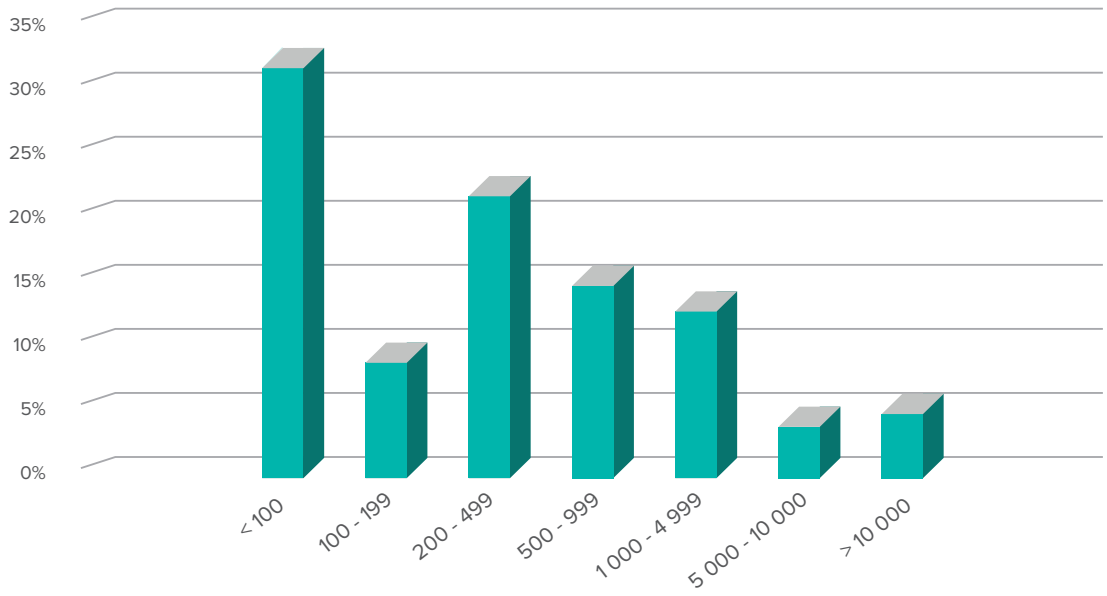
Trendy v oblasti bezpečnostního vzdělávání

Radek Švadlenka

Obecně přijímané pravidlo praví, že systém je tak silný jako jeho nejslabší článek. A v oblasti bezpečnosti to platí dvojnásobně. Přestože organizace nainvestuje množství zdrojů do technických bezpečnostních opatření, snadno se může ukázat, že největší zranitelností jsou pro systémy samotní uživatelé. Dynamický vývoj ICT technologií v posledních letech s sebou přináší stále nové a sofistikovanější metody útočníků a orientace na poli kybernetické bezpečnosti pro běžně uživatele je stále složitější. Na tato úskalí pamatuje i zákon o kybernetické bezpečnosti, resp. jeho prováděcí dokumentace, která povinným subjektům definuje pravidla pro realizaci funkčního modelu plánu rozvoje bezpečnostního povědomí uživatelů, administrátorů a osob zastávajících bezpečnostní role. Nicméně podobná opatření by měla být samozřejmostí v každé organizaci, kde to s bezpečností myslí alespoň trochu vážně.

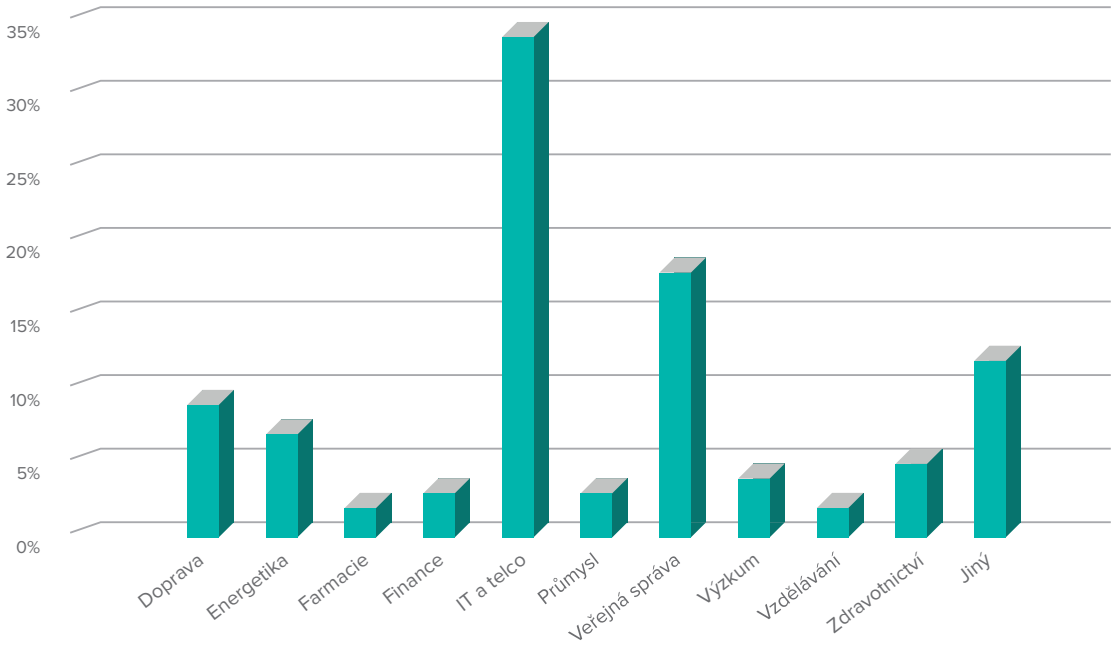
Každoročně uveřejňujeme výsledky průzkumu zaměřeného na realizované a plánované vzdělávací programy a aktivity organizací a ani tento rok není výjimkou. Abychom byli schopni sledovat trendy ve vývoji těchto aktivit, připravili jsme pro Vás nový průzkum za rok 2020 s ohledem na plánovaná opatření pro rok 2021. Do většiny aktivit organizací v loňském roce výrazně zasáhla pandemie Covid-19. O to zajímavější je meziroční srovnání plánovaných a realizovaných aktivit v oblasti vzdělávání v kybernetické bezpečnosti. Průzkumu se zúčastnilo bezmála sto organizací různých zaměření a velikostí, jak je vidět z grafů níže. Výzkumný vzorek je velmi podobný tomu z loňského roku, a to jak s ohledem na počet respondentů, tak i v poměru zastoupení organizací dle oboru a velikosti. Interpretace výstupů v porovnání hodnot s předchozím rokem je tedy relevantní a neměla by být příliš zkreslena rozdíly ve výzkumném vzorku.

Procentuální zastoupení organizací dle velikosti



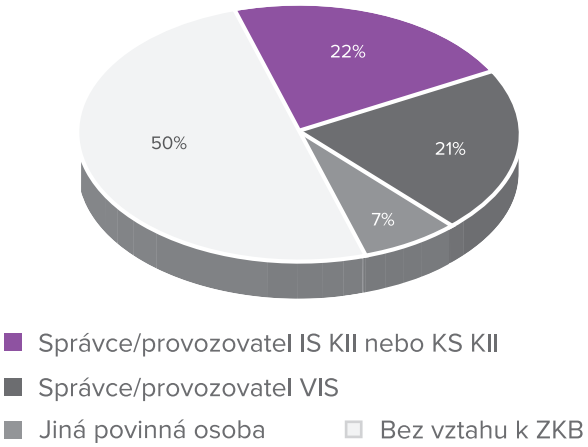
Počet zaměstnanců organizace

Procentuální zastoupení organizací dle oboru



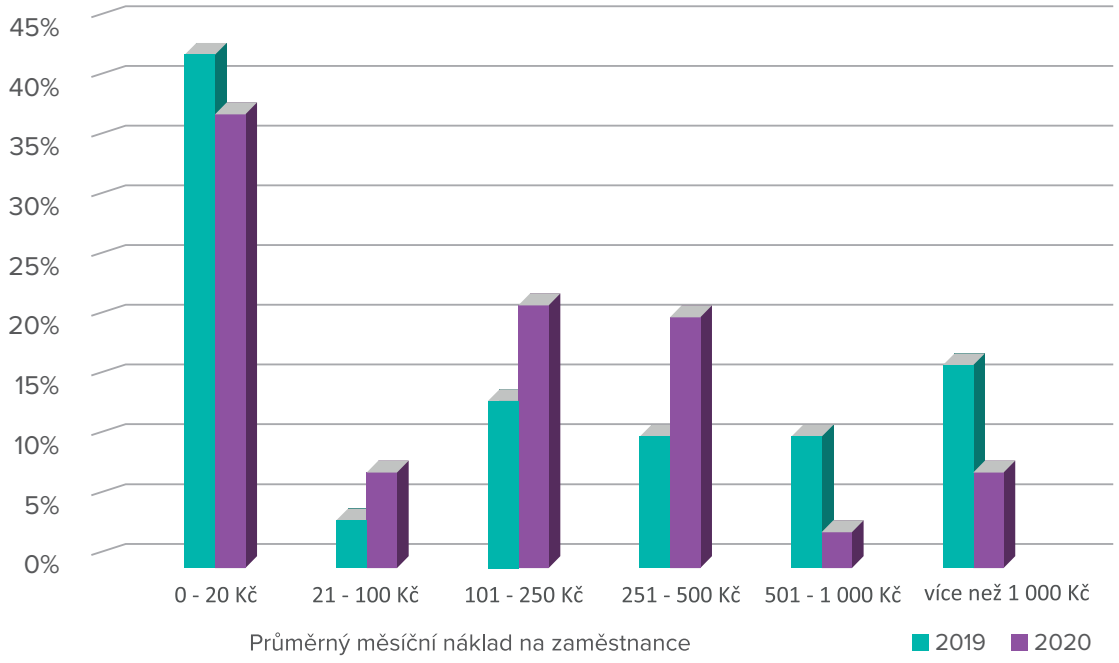
Pro úplnost je třeba upřesnit, že polovina respondentů průzkumu se řadí mezi povinné subjekty podle zákona o kybernetické bezpečnosti, jak ilustruje následující obrázek.

Vztah organizací k ZKB



Realizaci vzdělávacích aktivit v oblasti kybernetické bezpečnosti je možné zajistit za pomoci jak interních, tak i externích zdrojů v podobě prezenčních školení či e-learningových nástrojů. Vzhledem k omezením souvisejících s pandemií musela být zejména prezenční školení nahrazena jinou formou např. virtuálních školení pomocí online platforem. V grafu níže je možné sledovat porovnání investovaných prostředků do vzdělávání v letech 2019 a 2020. Jako pozitivní trend je možné označit meziroční pokles počtu organizací, které investují do vzdělávacích aktivit minimum prostředků. Celkem logicky také roste počet firem investujících do vzdělávání mezi 100 až 500 Kč na zaměstnance. Na druhou stranu je vidět, že ochota investovat větší částky než 500 Kč na zaměstnance byla v roce 2020 pro některé firmy neudržitelná.

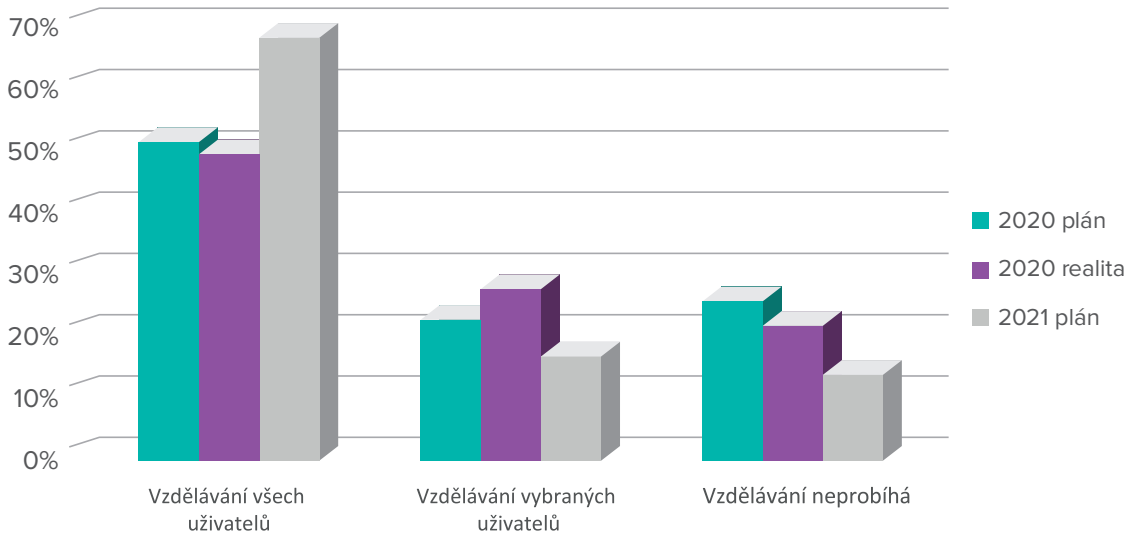
Zastoupení organizací dle výdajů na vzdělávání v kybernetické bezpečnosti



Vzdělávání uživatelů – realita versus plán

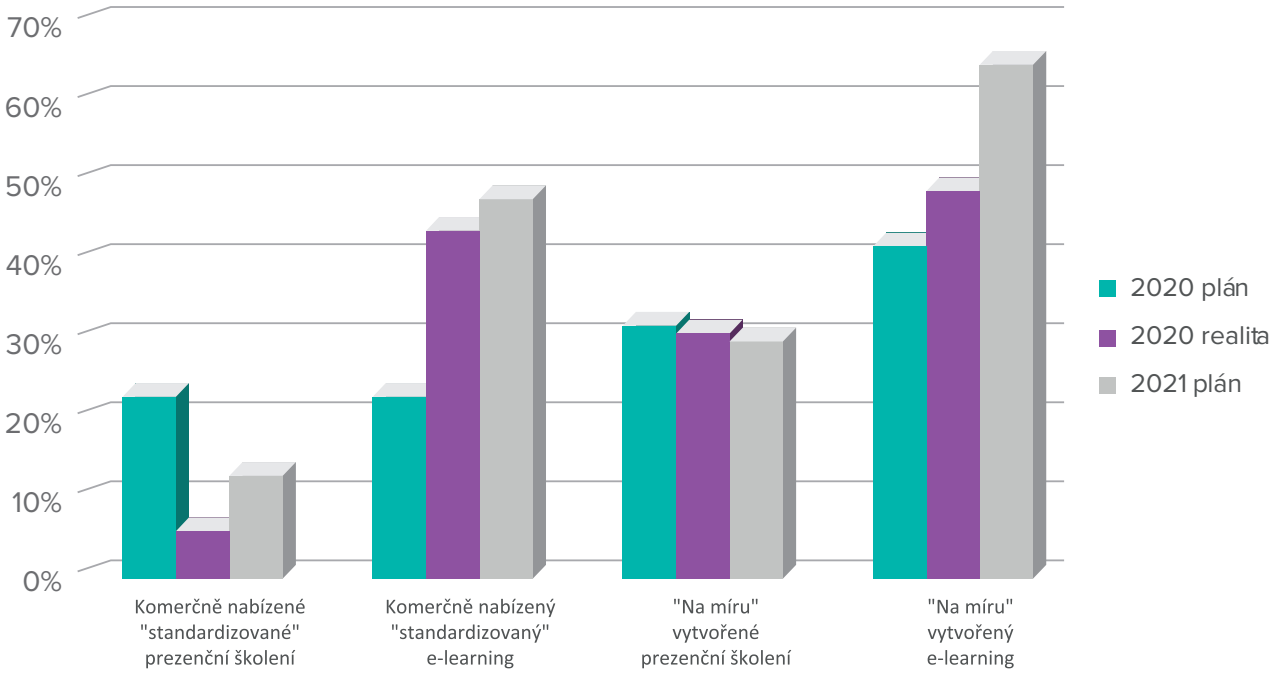
Součástí našeho průzkumu v loňském roce byla oblast věnovaná dotazům na plánované aktivity v oblasti vzdělávání uživatelů pro rok 2020. V té době však ještě nikdo nemohl predikovat opatření spojená s pandemií. O to zajímavější je porovnání plánovaných vzdělávacích aktivit s reálně provedenými v roce 2020. Graf níže naznačuje, že dopady pandemie prozatím neměly na realizované aktivity v oblasti vzdělávání uživatelů zas až tak velký vliv. Polovina respondentů aplikovala vzdělávání pro všechny uživatele, a co je ještě mnohem optimističtější, alespoň nějaké vzdělávací aktivity v roce 2020 proběhly i u části organizací, které s tím předem nepočítaly. Pozitivní trend je také možné pozorovat ve výhledu na rok 2021, kde téměř 70 % respondentů odpovědělo, že počítá se vzděláváním všech uživatelů v tomto kalendářním roce.

Vzdělávání uživatelů v organizacích

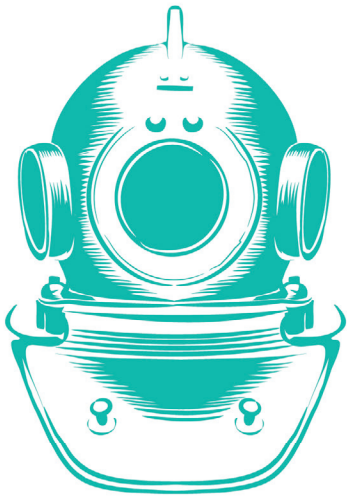


Zatímco na vzdělávání uživatelů obecně neměla pandemie výrazný dopad, jak jsme demonstrovali na předchozím obrázku, jinak je tomu zákonitě s ohledem na plánované a realizované formy vzdělávání uživatelů. Jak je patrné z grafu níže, celkem logicky došlo v roce 2020 k omezení prezenčních standardizovaných školení ve prospěch e-learningových řešení oproti plánu stanoveném na konci roku 2019. Naproti tomu na míru vytvořená prezenční školení byla často realizována pomocí online platformy a zde se realita nijak zvlášť neodchýlila od plánu. Z odpovědí týkajících se plánu na rok 2021 je možné predikovat pokračující trend migrace k e-learningovým nástrojům a realizace standardizovaných prezenčních kurzů bude přímo úměrná protiepidemickým opatřením vlády a potenciálnímu riziku nákazy zaměstnanců.

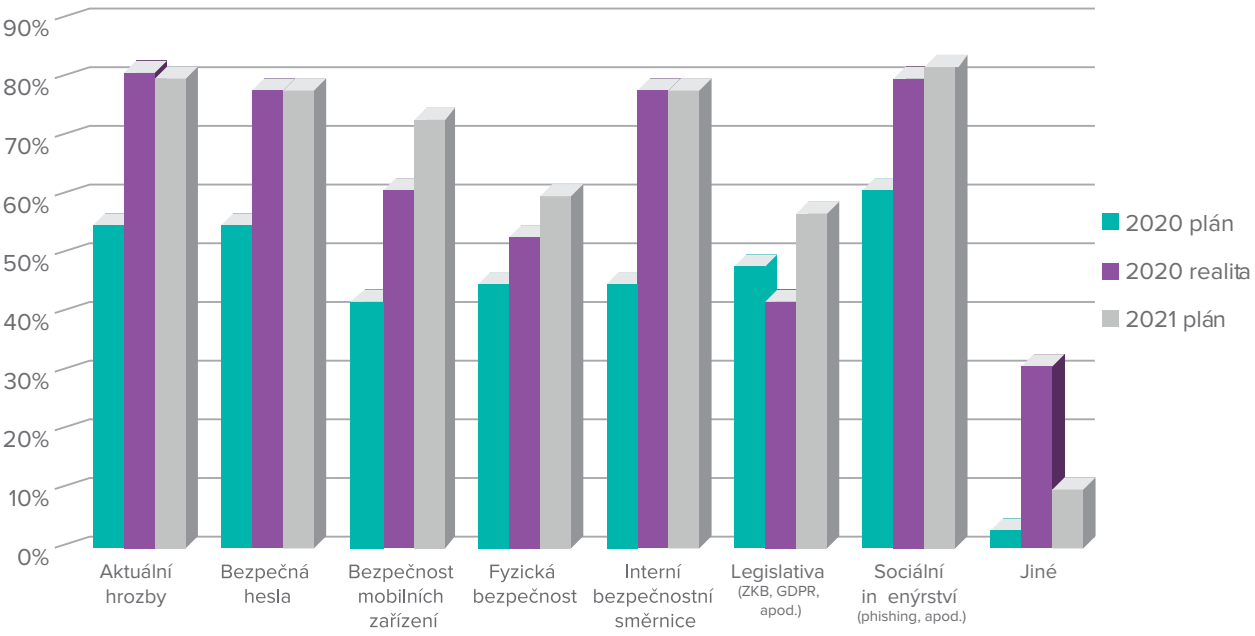
Realizované / plánované formy vzdělávání uživatelů



Za velmi optimistický je možné pokládat vývoj v oblasti zaměření vzdělávání pro uživatele. Oproti plánovaným aktivitám hned v pěti kategoriích došlo významnému nárůstu v počtu firem zaměřujících se na danou oblast. Největší zájem byl spojen s problematikou aktuálních hrozeb, bezpečných hesel, bezpečnosti mobilních zařízení, interními bezpečnostními směrnicemi a sociálním inženýrstvím. Naopak méně organizací oproti plánu se soustředilo na oblast legislativy, ale pravdou je, že připravované novely vyhlášky o významných informačních systémech a tzv. cloudové vyhlášky byly časově odsunuty až do tohoto roku a žádná další významná norma týkající se bezpečnosti nebyla v roce 2020 vydána. Plán zaměření vzdělávacích aktivit pro uživatele na rok 2021 se příliš neliší od reality z roku 2020, snad s výjimkou již zmíněné legislativy.

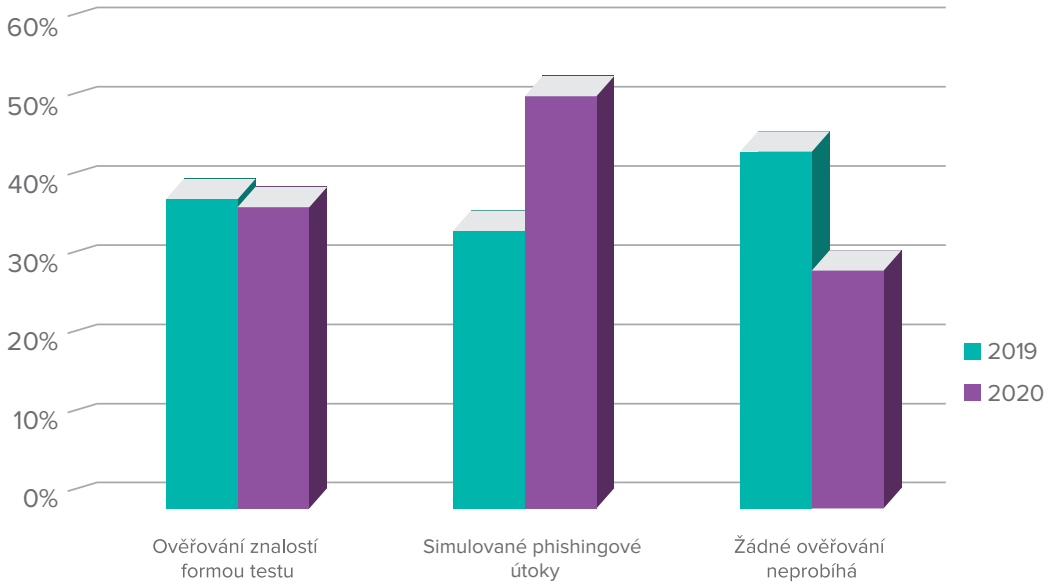


Zaměření vzdělávacích aktivit pro uživatele



Mezi zaměstnanci málo oblíbené, ale také velmi efektivní, mohou být aktivity spojené s ověřováním znalostí a ostražitosti uživatelů v oblasti kybernetické bezpečnosti. Velmi pozitivní trend je možné pozorovat v grafu níže, kde v meziročním porovnání o 15 % více organizací provádělo alespoň nějakou formu ověřování uživatelských znalostí nebo ostražitosti. Toto zvýšení reflektuje vysoký procentuální nárůst organizací, které realizovaly simulované phishingové útoky. Plánované aktivity spojené s ověřováním uživatelských znalostí a ostražitosti v roce 2021 korespondují s realitou z loňského roku, kde 30 % organizací neplánuje žádná taková opatření.

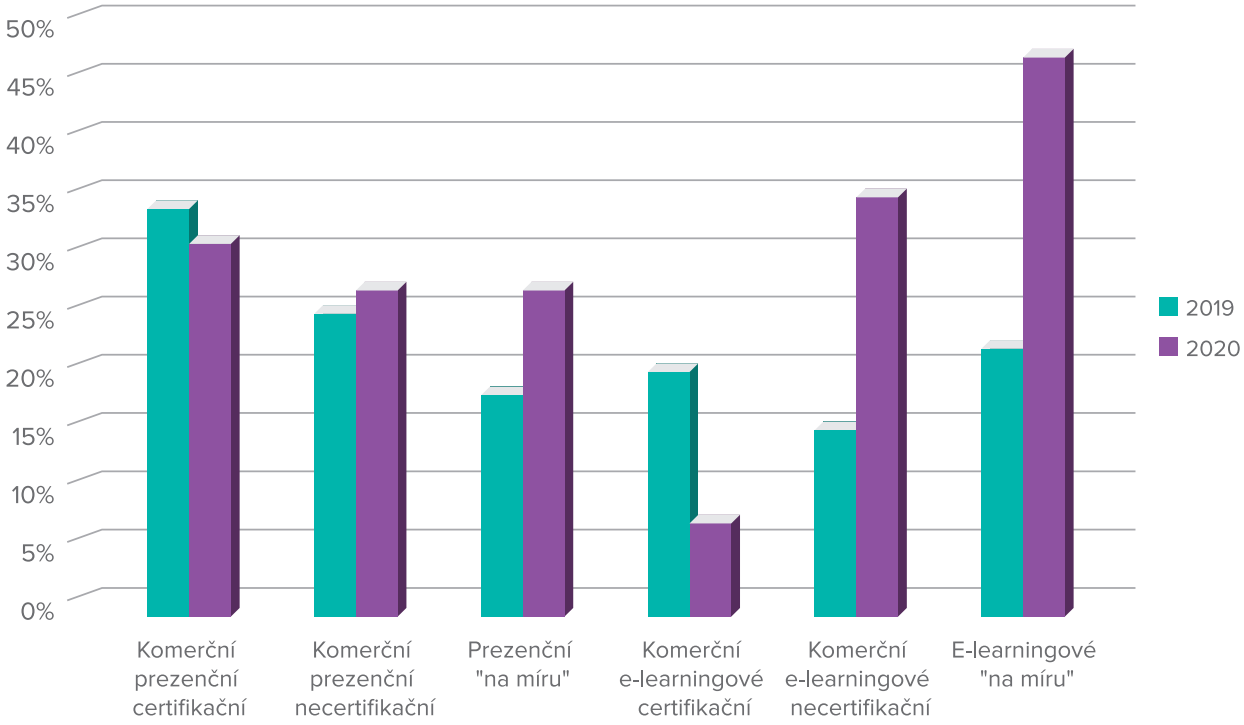
Ověřování znalostí a ostražitosti uživatelů



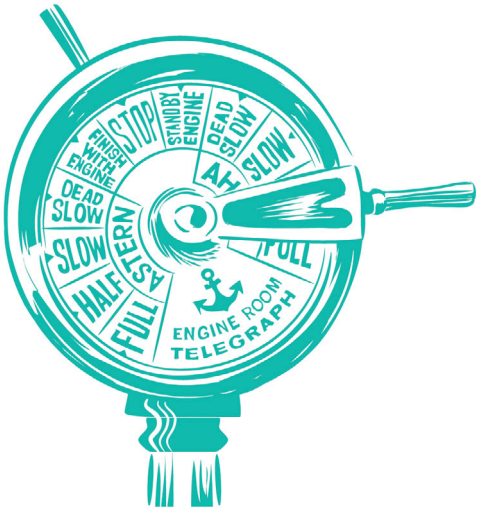
Vzdělávání odborných rolí

Zaměstnanci na pozicích administrátorů a bezpečnostních expertů jsou klíčoví pro plánování, realizaci a udržitelnost bezpečnostních pravidel v organizaci. Jejich znalosti a dovednosti mohou mít významný dopad na efektivitu zvládání bezpečnostních incidentů. Na grafu níže je zobrazeno meziroční porovnání realizovaných forem vzdělávání bezpečnostních rolí v organizacích. Na první pohled je patrný růst v oblasti e-learningových kursů v kategoriích necertifikační a na míru. Paradoxně certifikační e-learningové kursy nebyly v porovnání s předchozím rokem tolik populární. Podobně je tomu i u prezenčních školení, kde s nižší intenzitou také vzrostla poptávka po necertifikovaných školeních a školeních na míru. Omezení zájmu po certifikovaných formách vzdělávání může souviset s jejich vyšší cenou, která v současné době nemá opodstatnění.

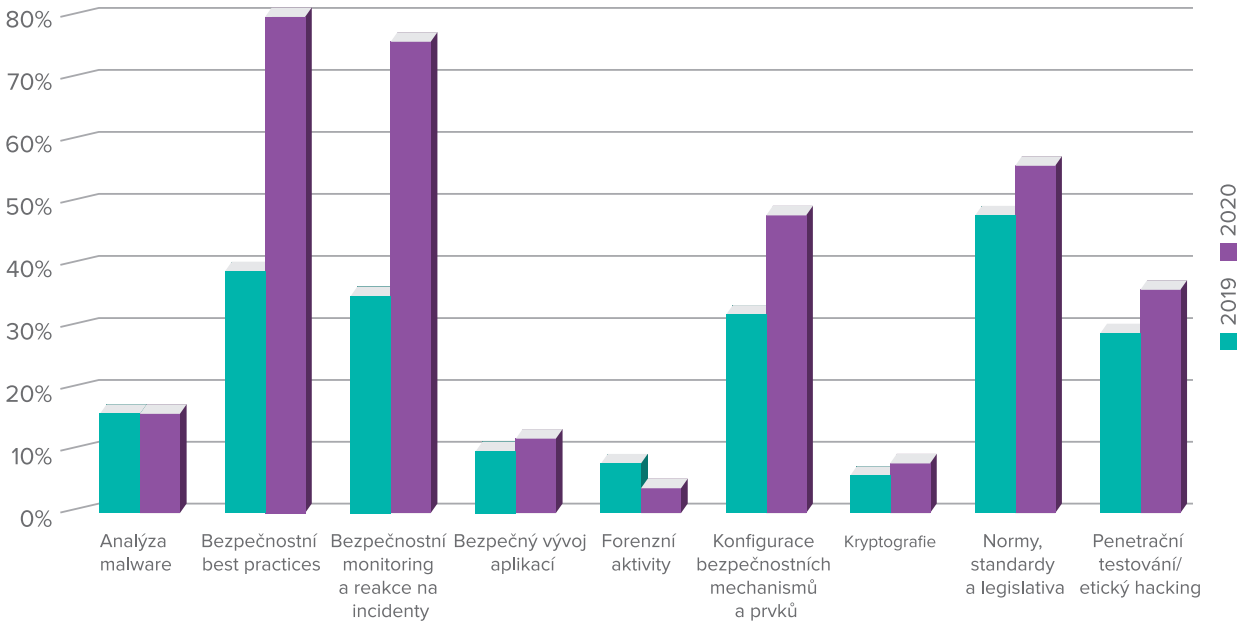
Realizované formy vzdělávání bezpečnostních rolí



Vzdělávání odborných rolí vyžaduje v porovnání s uživateli mnohem hlubší znalosti a výběr ze specifických oblastí kybernetické bezpečnosti. Jak je patrné z obrázku níže v roce 2020, v porovnání s rokem předešlým, rezonovala mezi bezpečnostními experty zejména dvě témata, a to bezpečnostní best practices a bezpečnostní monitoring a reakce na incidenty. Zvýšený zájem byl i o oblasti konfigurace bezpečnostních mechanismů a penetračního testování a etického hackingu. Naopak menší poptávka byla v roce 2020 spojena se vzděláváním v oblasti forenzních aktivit. Obecně panuje v komunitě odborných rolí nižší zájem o kurzy zaměřené na bezpečný vývoj aplikací, kryptografie a již zmíněné forenzní aktivity.



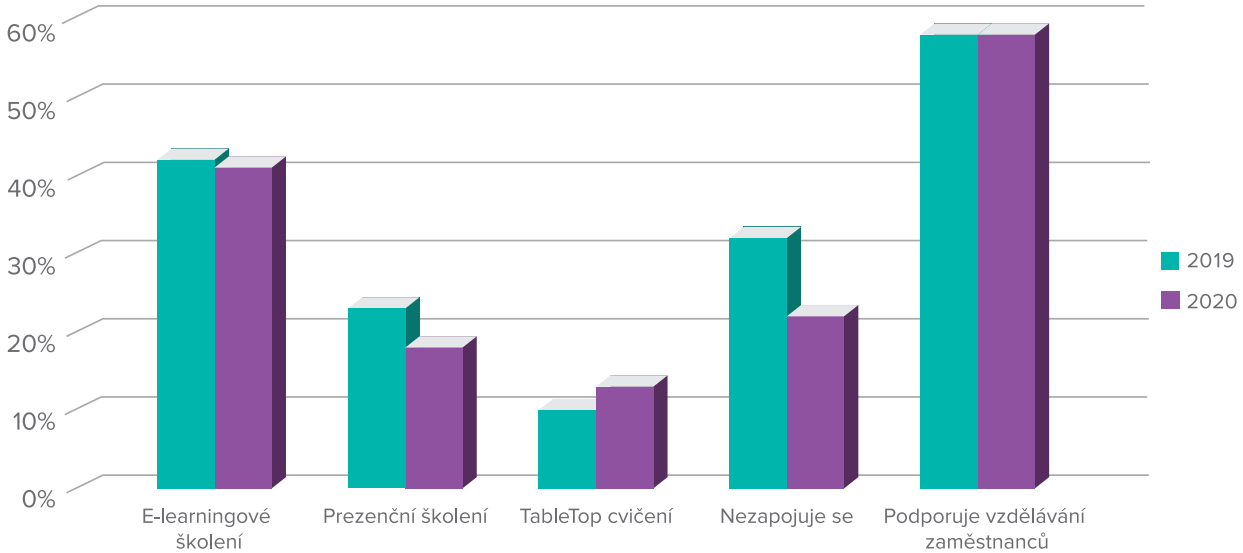
Zaměření vzdělávacích aktivit pro bezpečnostní role



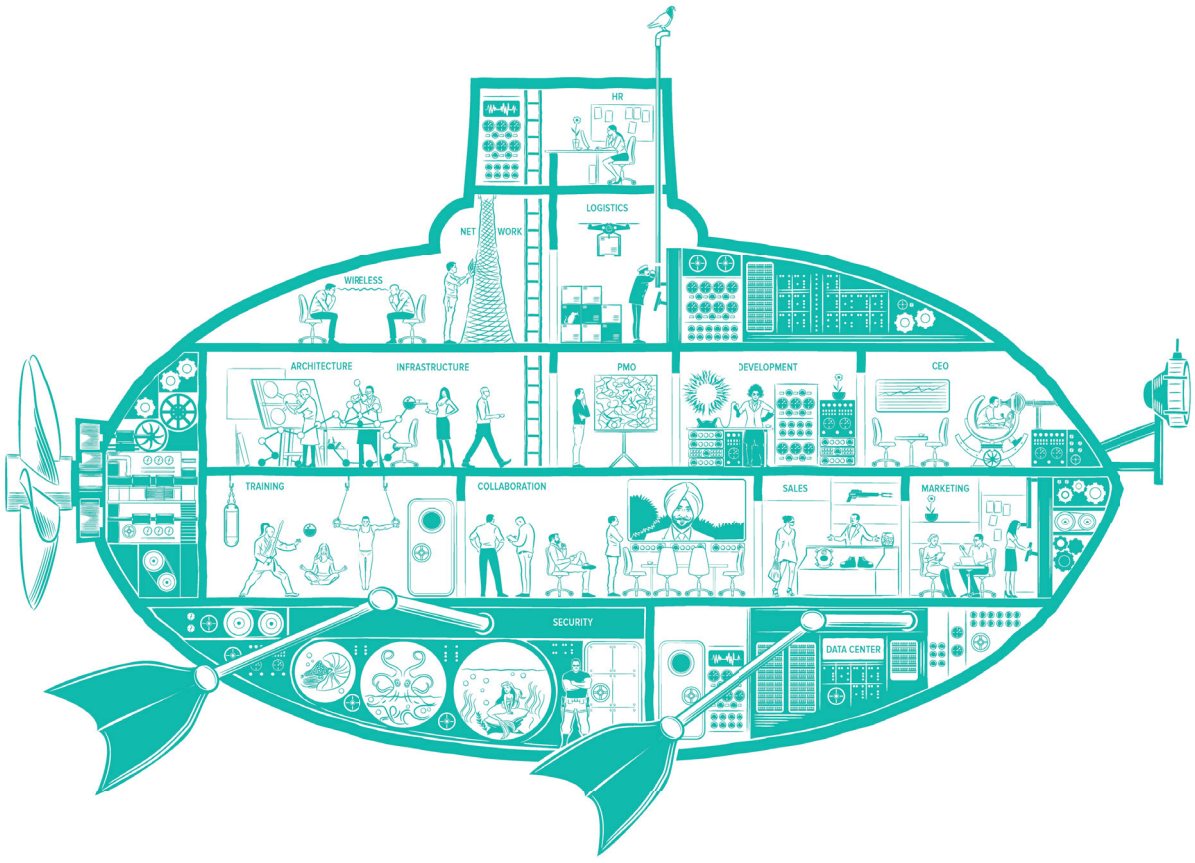
Zapojení top managementu do vzdělávacích aktivit

Vrcholový management organizace má zásadní vliv na realizaci bezpečnostních opatření prostřednictvím schvalování investic do bezpečnosti, ale také v podobě podpory do vzdělání zaměstnanců. Je však třeba připomenout, že i vrcholový manažer je uživatelem informačních systémů a v případě jeho slabší orientace v oblasti kybernetické bezpečnosti je celá organizace mnohem zranitelnější vůči externím, ale i interním hrozbám. Níže zobrazený graf ukazuje meziroční trend v oblasti vzdělávání top managementu v kybernetické bezpečnosti. Pozitivním bodem je bezesporu celkový pokles v počtu organizací, jejichž manažeři se do vzdělávacích aktivit vůbec nezapojují. Na druhou stranu došlo k poklesu zájmu o prezenční formu školení, což je možné spojit s protiepidemickými opatřeními. Naopak mírně vzrostla poptávka po tabletop cvičeních. Z hlediska podpory vzdělávání zaměstnanců ze strany top managementu se stav od loňského roku nijak nezměnil a drží se na úrovni 58 % z oslovených organizací.

Zapojení top managementu do vzdělávacích aktivit v oblasti kybernetické bezpečnosti



Závěr tohoto příspěvku je obohacen o zajímavé odpovědi z řad respondentů, týkající se top managementu a jeho orientace v kybernetické bezpečnosti a také vlivu epidemie na organizace. Celkem 89 % respondentů je přesvědčeno, že vyšší vzdělanost vrcholového managementu v kybernetické bezpečnosti má pozitivní vliv na rozvoj security v organizaci. 51 % účastníků průzkumu souhlasí s názorem, že hlavním faktorem pro ochotu managementu investovat zdroje do kybernetické bezpečnosti jsou medializované kybernetické incidenty, případně interní incidenty. Zároveň 38 % dotázaných odpovědělo, že hybnou silou pro investice do kybernetické vzdělanosti je právě úroveň orientace top managementu na poli kybernetické bezpečnosti. Většina respondentů jako důsledek epidemie vyzdvihuje přesun aktivit do online režimu. Přibližně třetina organizací vsadila na e-learningové nástroje pro vzdělávání zaměstnanců, což potvrzují závěry interpretované v předchozí kapitole. Více než 20 % respondentů uvádí omezení zdrojů do kybernetické bezpečnosti a přibližně stejné procento organizací prozatím nezavedlo změny oproti stavu před epidemií.



Dostupnost phishing kitů na indexované části internetu

Jan Kopřiva a Ina Rumlová

Tak jako každý rok, i letos je závěrečná část našeho reportu věnována vybrané analýze nebo výzkumu, kterému se v uplynulém roce věnoval bezpečnostní tým ALEF CSIRT. Tentokrát se zaměříme na výzkum dostupnosti tzv. phishing kitů, tedy standardizovaný šablon podvodných webových stránek, které si mohou útočníci zakoupit či volně stáhnout a následně využívat pro realizaci phishingových kampaní.

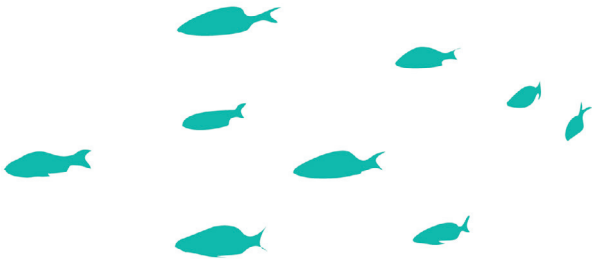
Phishing kity, označované mezi útočníky také jako “scam pages” nebo zkráceně “scamas”, umožňují i technicky méně schopným kybernetickým zločincům používat při podvodných kampaních falešné stránky, které působí na první pohled realistickým dojmem.

V rámci těchto balíků jsou totiž standardně předpřipraveny důvěryhodně působící přihlašovací stránky vybrané služby, u nichž pro zajištění korektní funkcionality zpravidla stačí jejich nahrání na určitý webový server.

Každý útočník, který si dokáže zajistit prostor na webovém serveru (ať už na vlastním, nebo kompromitovaném serveru třetí strany) má tak možnost velmi rychle získat přístup k dobře působícímu falešnému přihlašovacímu portálu, nebo oficiálně vyhlížejícím stránkám, které vyžadují například zadání platebních údajů.

Balíky s podvodnými stránkami jsou standardně nabízeny jako komerční produkt na vybraných Dark webových fórech, avšak v některých případech jsou dostupné i v rámci tzv. indexovaného nebo také „surface“ či „clear“ webu, tedy té části internetu, která je běžně procházena a indexována standardními vyhledávači obsahu.

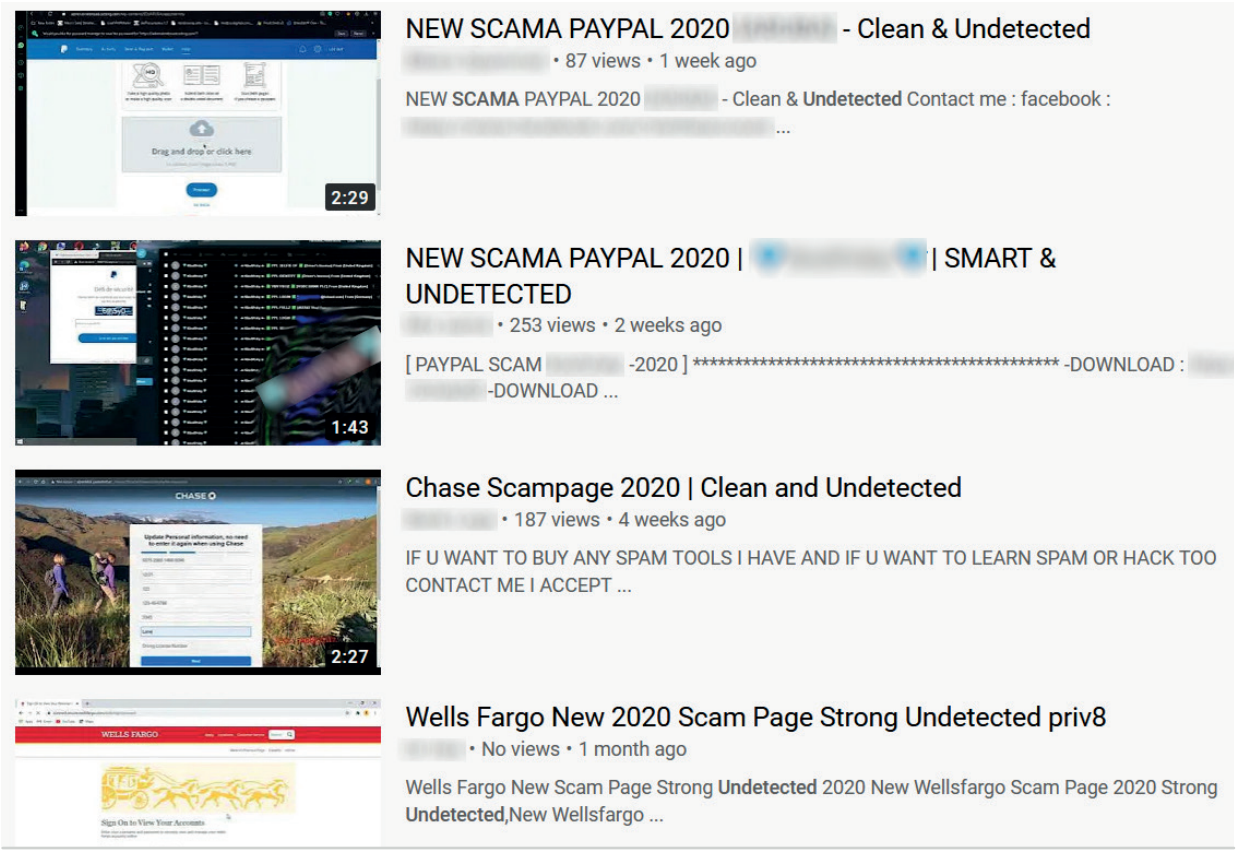
Pro úplnost je vhodné uvést, že vybrané balíky nejen v rámci clear webu jsou svými tvůrci distribuovány zcela zdarma. V takových případech je však často součástí sady phishingových stránek i nějaký škodlivý kód, například takový, který umožňuje jejich původnímu autorovi získat přístup k datům, která byla s pomocí daného phishing kitu získána jinými škodlivými aktéry.



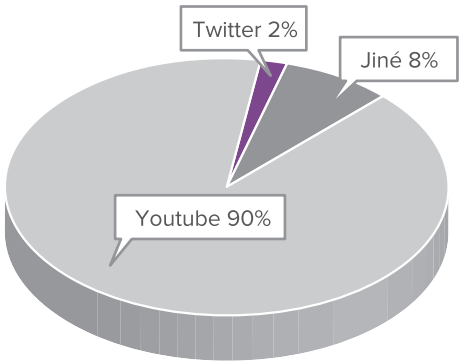
V posledním kvartálu uplynulého roku provedli členové bezpečnostního týmu ALEF CSIRT několik analýz nabídek phishing kitů, které jejich autoři publikovali v prostředí indexované části internetu v průběhu roku 2020. Na různých platformách (Youtube, Twitter apod.) se jim při tom podařilo identifikovat celkem 300 různých komerčních nebo zdarma nabízených kitů.

Vedle „scamas“ balíků byly na stejných platformách nabízeny také seznamy vhodných cílů pro phishingové kampaně (například seznamy e-mailových kontaktů zákazníků vybraných bank), související šablony e-mailových zpráv (tzv. “letters”) nebo vybrané technické nástroje určené pro usnadnění phishingových kampaní (například validátory e-mailových adres).

Jak se ukázalo, zejména YouTube byl v roce 2020 autory phishing kitů užíván pro nabízení jimi vytvářených produktů velmi silně. Nabídky na tomto portálu byly zpravidla realizovány formou demonstračních videí, které předváděly schopnosti nabízeného zboží a byly obvykle doplněny o informace o ceně a případně o odkaz na stažení nebo koupi daného kitu.



Platformy používané pro distribuci phishing kitů



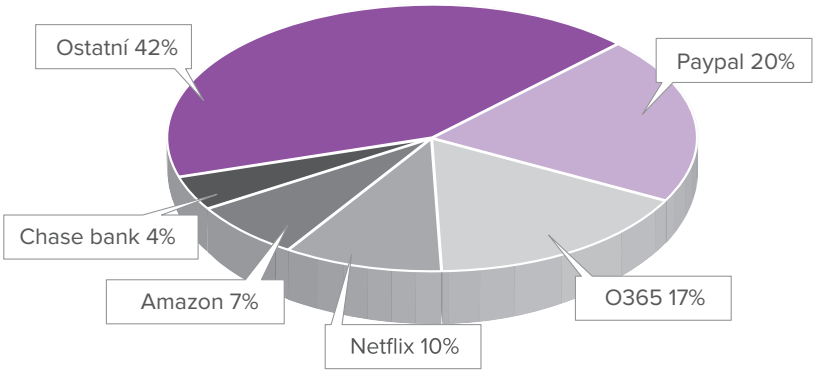
Přestože YouTube byl autory phishing kitů využíván dominantně, nešlo o jedinou platformu, s pomocí níž byly v rámci clear webu jejich produkty nabízeny.

Celkem se podařilo identifikovat 185 různých účtů, které phishing kity v prostředí indexovaného webu nabízely. Pouze 26 z nich nabízelo 2 či více balíků a pouze tři z identifikovaných účtů/skupin nabízely více než 10 kitů (konkrétně 11, 15 a 22).

Zmínku zaslouží velmi zajímavé rozložení cen u komerčních balíků. Ty se nejčastěji pohybovaly v částkách od pěti do několika desítek amerických dolarů nebo EUR. V určitých případech však byly phishing kity nabízeny i za zcela nesmyslné ceny okolo 100 BTC. Balíků poskytovaných zdarma pak bylo identifikováno celkem 36.

Mezi celkem 87 službami, na jejich uživatele byly podvodné stránky cíleny, byly mj. různé banky streamovací služby, e-mailové portály nebo e-shopy. Jak ukazuje následující graf, nadpoloviční většina (174) phishing kitů přitom cílila na zákazníky/uživatele pouze pěti vybraných služeb – Paypal, Office 365, Netflix, Amazon a banky Chase.

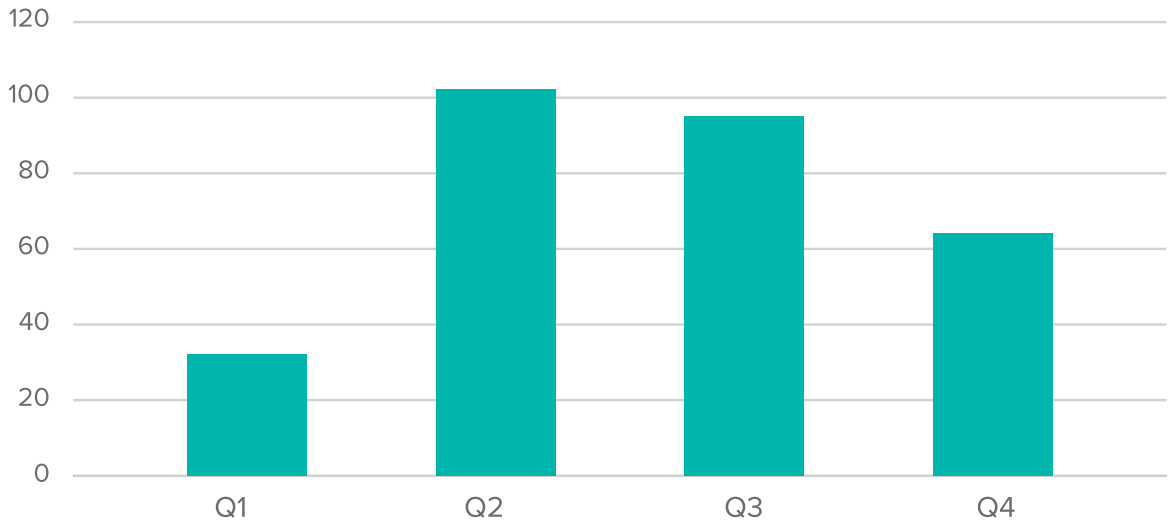
Cílení phishing kitů

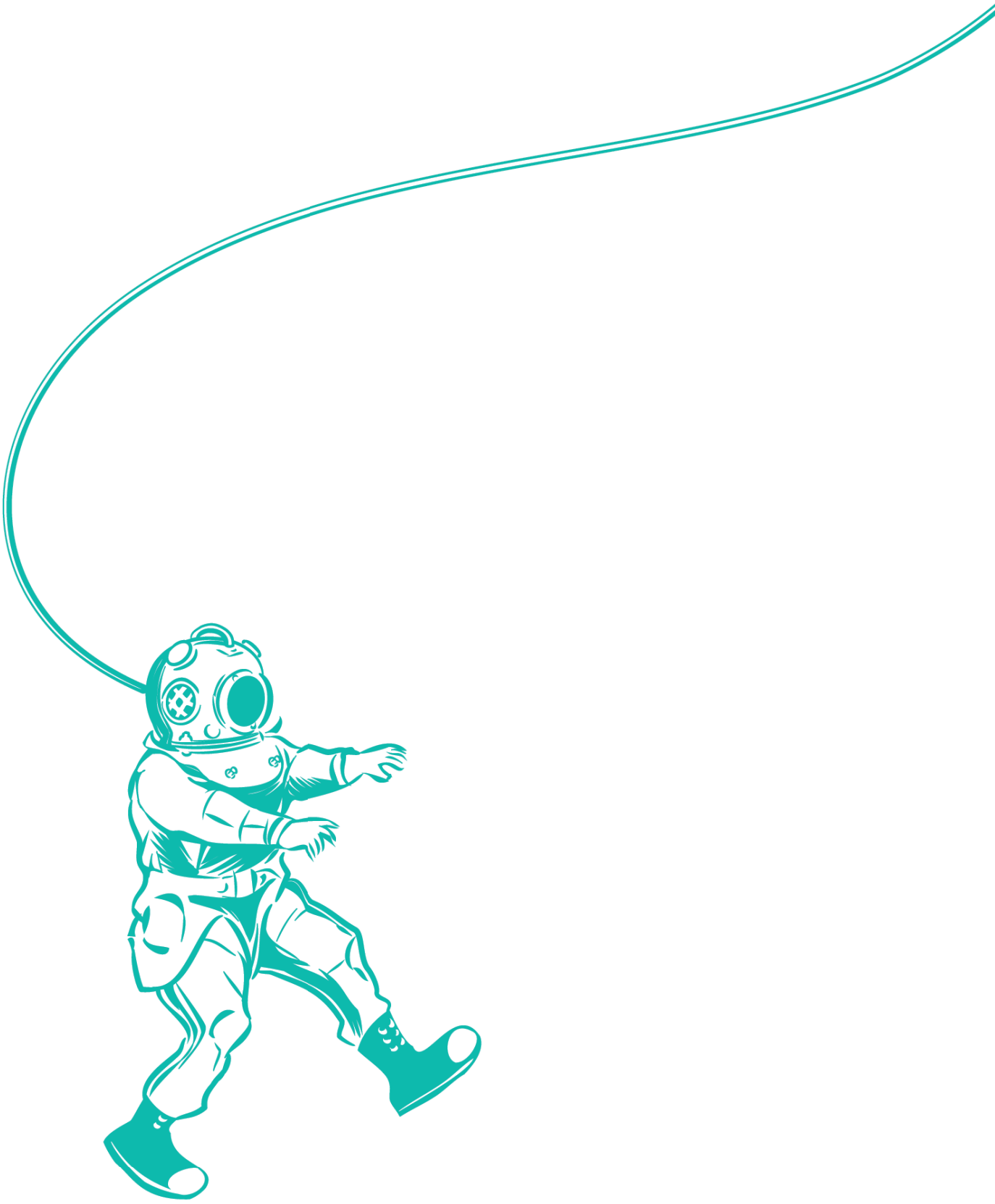


Prostředí indexovaného webu není za běžných okolností obvyklým místem pro nabízení podvodných stránek. Důvod je nasnadě. Policejní orgány i další organizace bojující s kybernetickým zločinem mají podstatně širší možnosti monitorování tohoto prostředí, než je tomu například u Dark webových tržišť. Výše zmiňované počty nalezených phishing kitů se tak zdají být až výjimečně vysoké.

Přestože z dostupných dat není možné jednoznačně určit důvod tak širokého používání otevřeného webu pro nabízení phishing kitů v roce 2020, z rozložení datumů publikace nabídek lze usuzovat, že širší používání volně dostupných internetových komunikačních kanálů ze strany autorů podvodných stránek bylo do jisté míry zapříčiněno pandemií Covid-19. V průběhu prvního kvartálu totiž byly na clear webu publikovány nabídky pouze necelých jedenácti procent ze všech identifikovaných phishing kitů a zejména ve druhém kvartálu byl viditelný citelný nárůst počtů nabídek. Je tedy pravděpodobné, že v důsledku omezení vybraných jiných aktivit v důsledku pandemie se i někteří škodliví aktéři, kteří by běžně „scamas“ nenabízeli, rozhodli s tímto typem kyberzločinu začít a učinili tak prostřednictvím otevřených internetových komunikačních kanálů.

Počet nově nabídnutých phishing kitů





Pro více informací kontaktujte cz-sales@alef.com nebo @ALEFSecurity