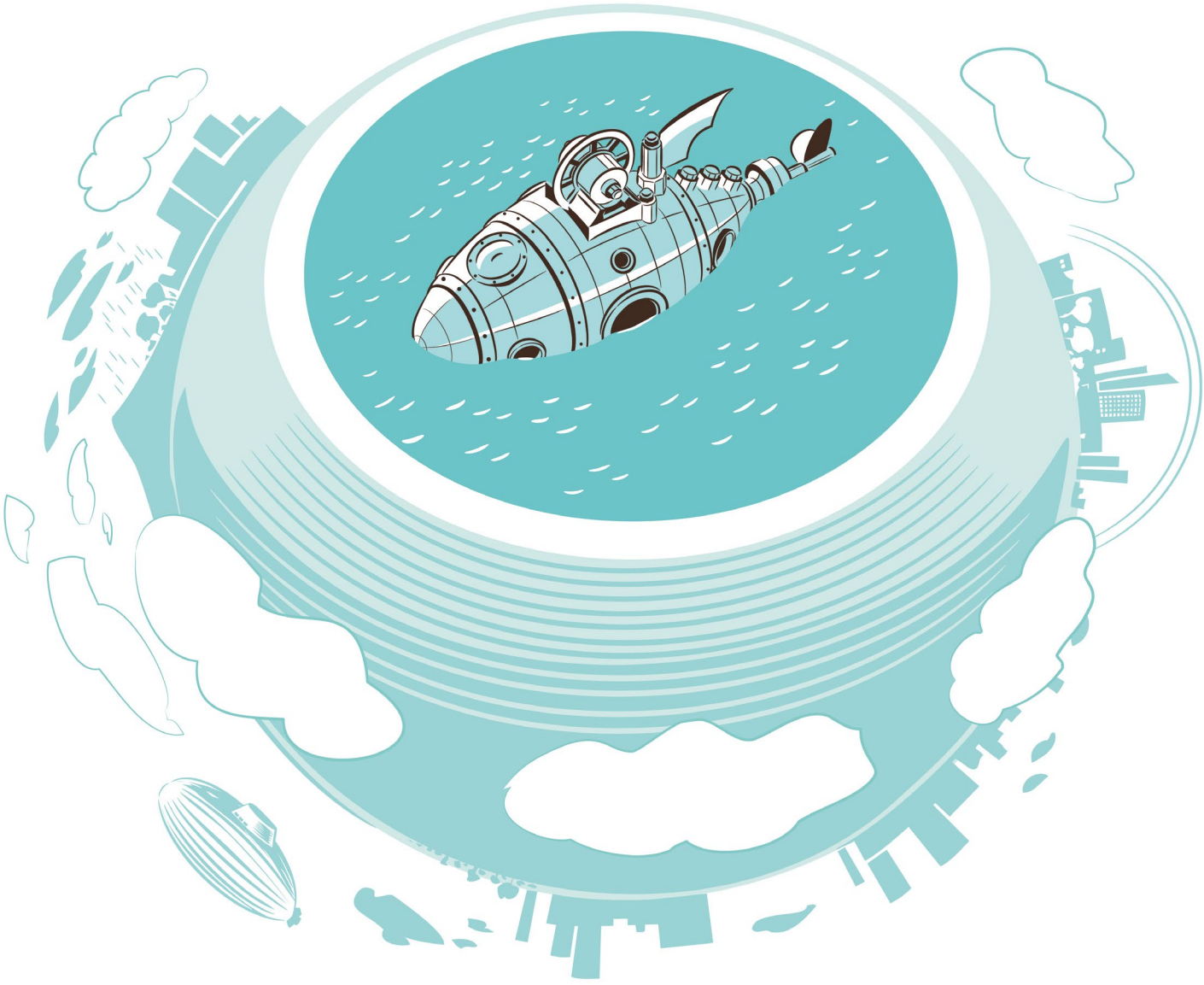
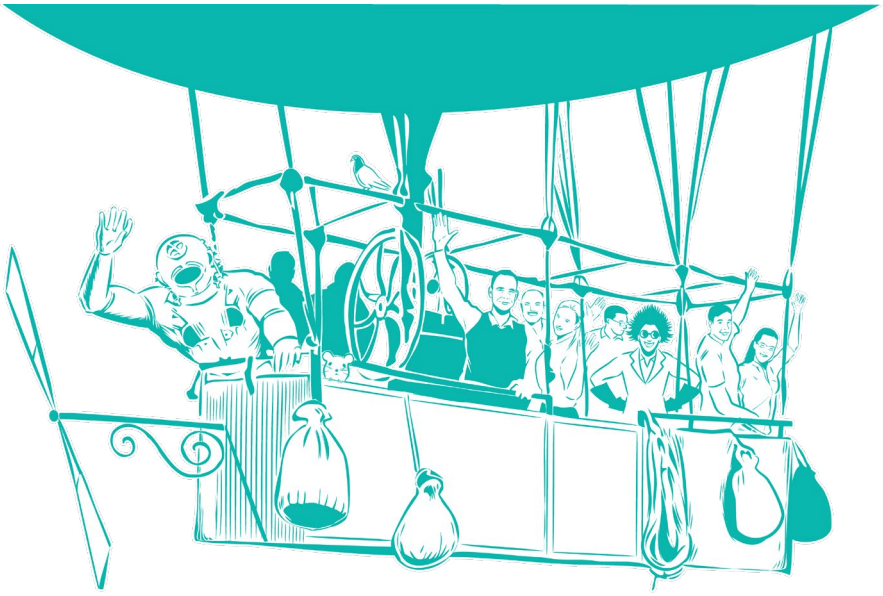
ALEF

Security Report 2023



Trust the Strong
www.alef.com

Obsah



Úvod

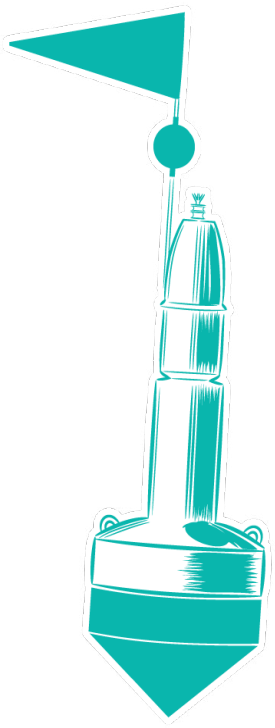
Poslední roky na poli IT a kybernetické bezpečnosti jsou poznamenány bezprecedentní dynamikou, která pramení z množství významných globálních událostí. Svět se ještě nestačil vzpamatovat z pandemie Covid-19 a už se rozhořel válečný konflikt na Ukrajině. Přestože je Rusko v demokratických zemích dlouhodobě považováno za potenciální bezpečnostní hrozbu, únorová invaze ještě více polarizovala svět a zkomplikovala řízení bezpečnosti. Dalším významným milníkem v roce 2022 bylo schválení a publikování finální podoby směrnice NIS2 v Úředním věstníku Evropské unie. Ta přináší mnoho změn v oblasti zajišťování kybernetické bezpečnosti a týká se nejen organizací, které jsou již dnes ze zákona o kybernetické bezpečnosti povinny své systémy zabezpečovat, ale i velkého množství organizací, které budou do regulace spadat nově a do dnešního dne žádné povinnosti plnit nemusely.

Hlavním cílem předložené publikace je poskytnout čtenáři přehled o aktuálních trendech u vybraných oblastí na poli kybernetické bezpečnosti a pomoci tak organizacím i jednotlivcům při výše zmíněné obraně obstát.

Majoritním zpracovatelem bezpečnostních dat využitých v rámci této publikace byl tým ALEF CSIRT, který kontinuálně analyzuje výstupy z vlastních technických a dalších zdrojů, i relevantní data z České republiky a zahraničí poskytovaná třetími stranami. Předložený report je však obohacen i o příspěvky dalších specialistů z týmu ALEF Security, kteří pro Vás zpracovali zajímavá témata z různých domén kybernetické bezpečnosti. Věříme, že pro Vás obsah tohoto reportu může být inspirativní například pro řešení problematiky kybernetické bezpečnosti ve Vaší organizaci.

Pokud nahlédnete dále do těla publikace, můžete se těšit mimo jiné na článek týkající se nejvýznamnějších světových událostí v oblasti kybernetické bezpečnosti, příspěvek řešící problematiku bezpečné emailové komunikace, aktuální trendy v oblasti bezpečnostního vzdělávání, analýzu dat z emailových bran a událostí zachycených IPS sondami, ale třeba také informace o stavu adopce bezpečnostních mechanismů SPF, DKIM a DMARC v ČR. Součástí této publikace je také několik analýz týkajících se mj. bezpečnostního dohledu. Vzhledem k výše zmíněným mezinárodním událostem, které mají významný dopad na řízení bezpečnosti, může být rovněž zajímavé porovnání dat s výstupy z předchozího roku, který byl ovlivněn zejména pandemií Covid-19. Trendy patrné z tohoto porovnání mohou poodhalit, jak byly organizace schopné se adaptovat na nové podmínky a přizpůsobit své procesy probíhajícím globálním změnám.

Na tomto místě bychom, jako tradičně, rádi poděkovali zejména bezpečnostnímu týmu CSIRT.CZ, který nám laskavě poskytl data a statistiky ze svých monitorovacích nástrojů. Zároveň děkujeme všem respondentům, kteří vyplnili naše online dotazníky, neboť dostatečné množství relevantních dat bylo nutnou podmínkou pro zajištění kvalitního zpracování obsahu následujících příspěvků.



Zabezpečení obsahu e-mailové komunikace

Martin Šišmiš

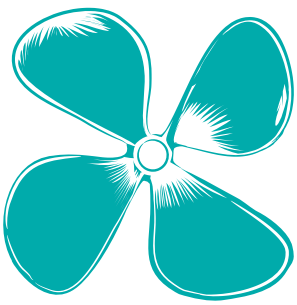
Stejně jako předchozí rok, pojďme se podívat na situaci a data ohledně zabezpečení emailové komunikace. Pro rekapitulaci si pojďme připomenout vlastnosti protokolu SMTP, který je sám o sobě nešifrovaný, umožňuje útočníkovi provádět on-path útoky a ten je tím pádem schopen si obsah e-mailové komunikace přečíst, nebo zprávy modifikovat. Pro ochranu dat při přenosu se dá využít kombinace dvou přístupů.

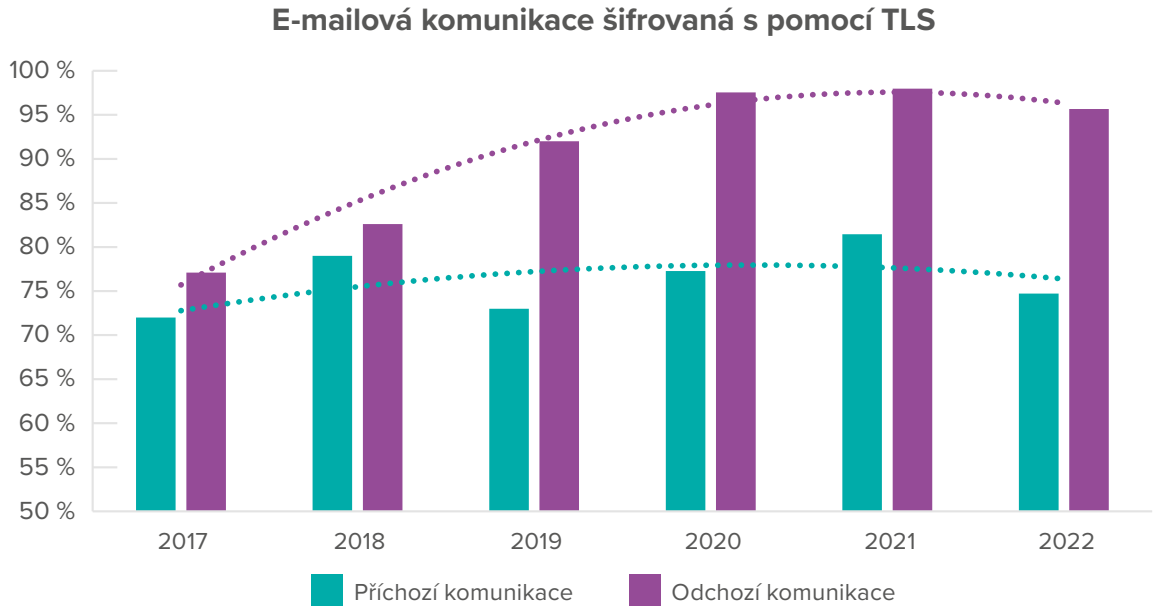
End-to-End šifrování: zašifrování zprávy probíhá na straně klienta, a to primárně za pomoci asymetrických kryptografických metod, jako například RSA, či ELGammal, při možnosti využívání Public Key Ifrastructure (PKI), key vaultů a jiných alternativ pro zprostředkování a správu používaných klíčů. Specifika lze najít ve standardech PGP, GPG, S/MIME a jiných. Díky nutnosti správy a výměny veřejných klíčů mezi korespondenty, není jednoduché zavést End-to-End šifrování plošně a je tedy uplatněno tam, kde je infrastruktura schopna distribuci a ověření klíčů zprostředkovat, či korespondenti si mezi sebou výměnu klíčů v rámci standardu vykomunikují. Jednou z nevýhod End-to-End šifrování je, že SMTP hlavičky jsou stále čitelné a také, že bezpečnostní prvky, jako třeba kontrola obsahu na emailovém serveru, či Intrusion Prevention System (IPS), nejsou schopné číst samotné tělo emailu a najít například škodlivé odkazy, nebo analyzovat přílohy.

Šifrování na transportní vrstvě: v tomto případě je nešifrovaná SMTP komunikace zabalena do šifrovaného tunelu. Takovýto tunel standardně využívá protokolu TLS (Transport Layer Security), a je vytvořený zvlášť pro každou komunikaci mezi jednotlivými servery po cestě. Pro vyjednávání o sestavení tunelu se používá příkazu STARTTLS, který dle nastavení obou serverů tunel sestaví, a to pouze pokud oba servery mají TLS povolené a podporují stejnou verzi TLS šifrování. Je nutné podotknout, že moderní e-mailoví klienti taktéž podporují šifrování mezi koncovou stanicí a jejím e-mailovým serverem. Tudíž, pokud je vše správně nastaveno a existuje podpora TLS na serverech po celé trase přenosu dat, pak by měla být zajištěna bezpečnost a důvěryhodnost zprávy při přenosu. Bohužel, vzhledem k tomu, že nejsme schopni zaručit, že nastavení a správa dalších serverů podílejících se na komunikaci je bezpečná, nelze on-path útoky zcela vyloučit (a to i přesto, že TLS a specifické verze lze vynucovat na vlastních serverech).

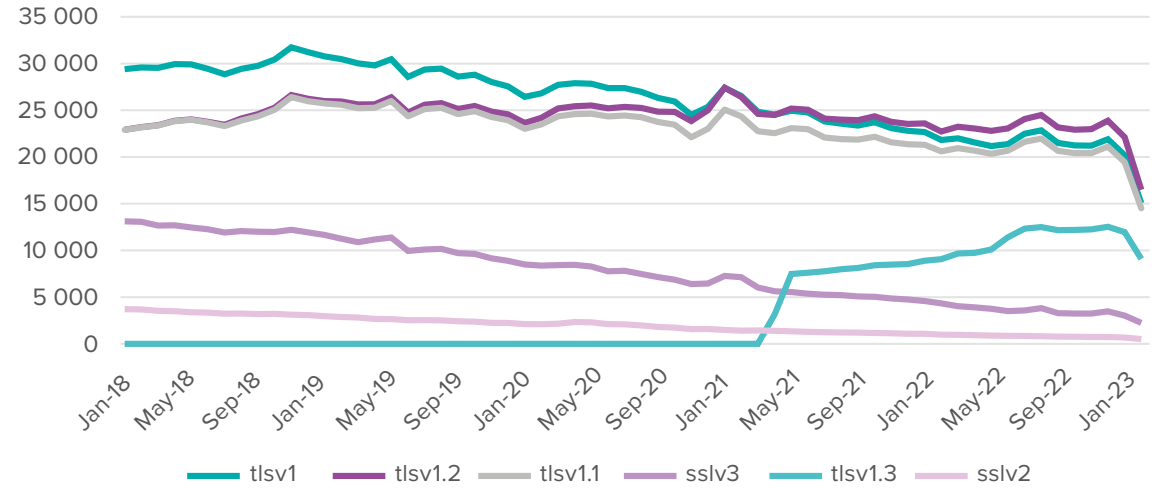
Pokud bychom se chtěli podívat na množství TLS šifrované komunikace u některého z globálních poskytovatelů, může nám pomoci například společnost Google. Ta na svých stránkách se statistickými údaji uvádí procentuální hodnoty šifrovaní příchozích a odchozích zpráv. Pro rok 2022 je, dle dat společnosti Google, z celkového počtu e-mailů šifrováno 89 procent, z toho 92 procent příchozí a 86 procent odchozí e-mailové komunikace. Tyto hodnoty se za posledních několik let nijak výrazně nemění.

Pojďme se také podívat na to, jaká je situace u nás v Česku. Pro tento účel můžeme využít našich interních dat získaných ze serverů ALEF GROUP, ale také našich vybraných zákazníků, přes které za rok 2022 prošlo více jak 50 miliónů zpráv. Následující graf ukazuje, že v rámci použitého vzorku bylo v roce 2022 šifrováno přibližně 87 procent z celkového počtu e-mailové komunikace. Z dat také vyplývá, že přibližně 75 procent příchozí a 96 procent odchozí komunikace je šifrováno. Změna oproti minulému roku může být z důvodu zahrnutí jiných či jinak nastavených serverů.





Zajímavá jsou i data z platformy Shodan ohledně viditelných SMTP služeb poskytovaných na portu 25 v České republice. Dle platformy je viditelných lehce přes 31 tisíc otevřených portů, z toho 19 tisíc portů má povolenou šifrovanou SMTP komunikaci alespoň v jedné z verzí SSL/TLS kryptografických protokolů. Z dat a přiloženého grafu, který se týká povolení konkrétních SSL/TLS verzí na SMTP serverech, lze vidět několik zajímavých trendů. Šifrování za pomoci zastaralých a zranitelných SSL verzí 1 a 2 je dlouhodobě na ústupu, což je samozřejmě pozitivní indikátor společně s nástupem a stoupající tendencí používat TLSv1.3. Bohužel, stejně jako v případě SSLv1 a SSLv2, tak i TLSv1 a TLSv1.1 obsahují zranitelnosti (například BEAST, či downgrade útoky), ale množství portů, které tyto verze protokolů mají povolené je stále poměrně značné. Pokud se podíváme na nastavení SMTP serverů, které mají povolenou pouze a jenom komunikaci přes prozatím bezpečné verze TLSv1.2 a TLSv1.3, dostaneme se na číslo okolo 2200 serverů, což je méně jak 10 procent z celkového počtu.



Je důležité si tedy uvědomit, že se nelze spoléhat pouze na šifrování na transportní vrstvě, obzvláště, pokud nemáme kontrolu nad servery na trase, po které SMTP provoz putuje. Proto bychom měli pro zasílání citlivých informací zvolit end-to-end šifrování, či jiný způsob bezpečné komunikace.

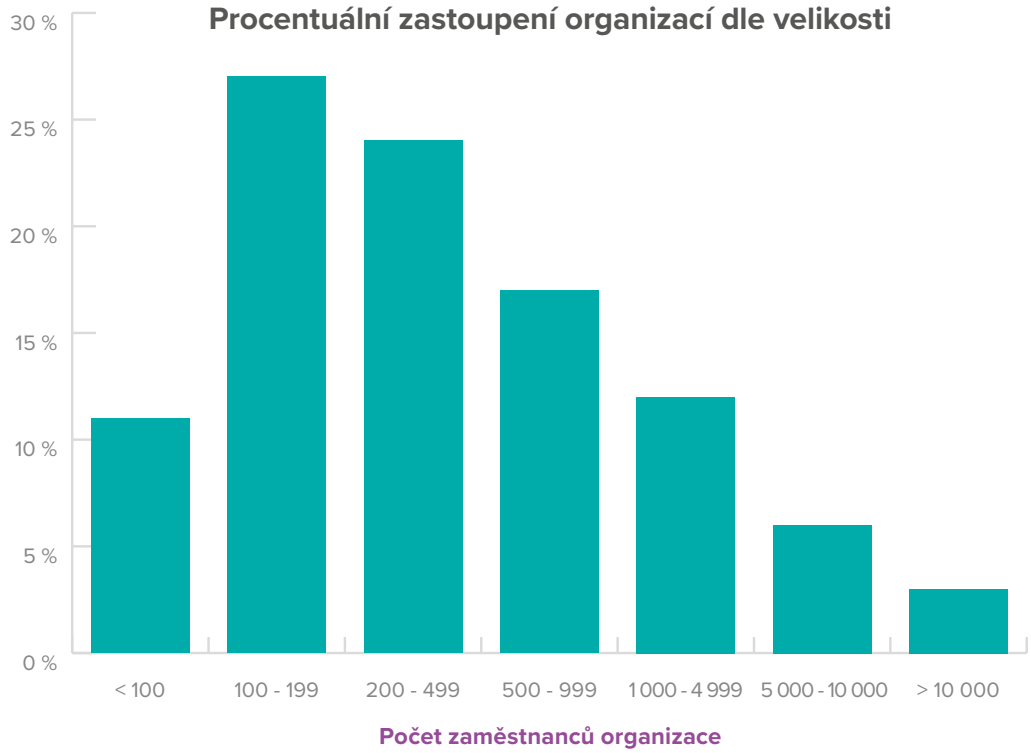
Zdroje: 1: https://transparencyreport.google.com/safer-email/overview
2: https://www.shodan.io/

Trendy v oblasti bezpečnostního vzdělávání

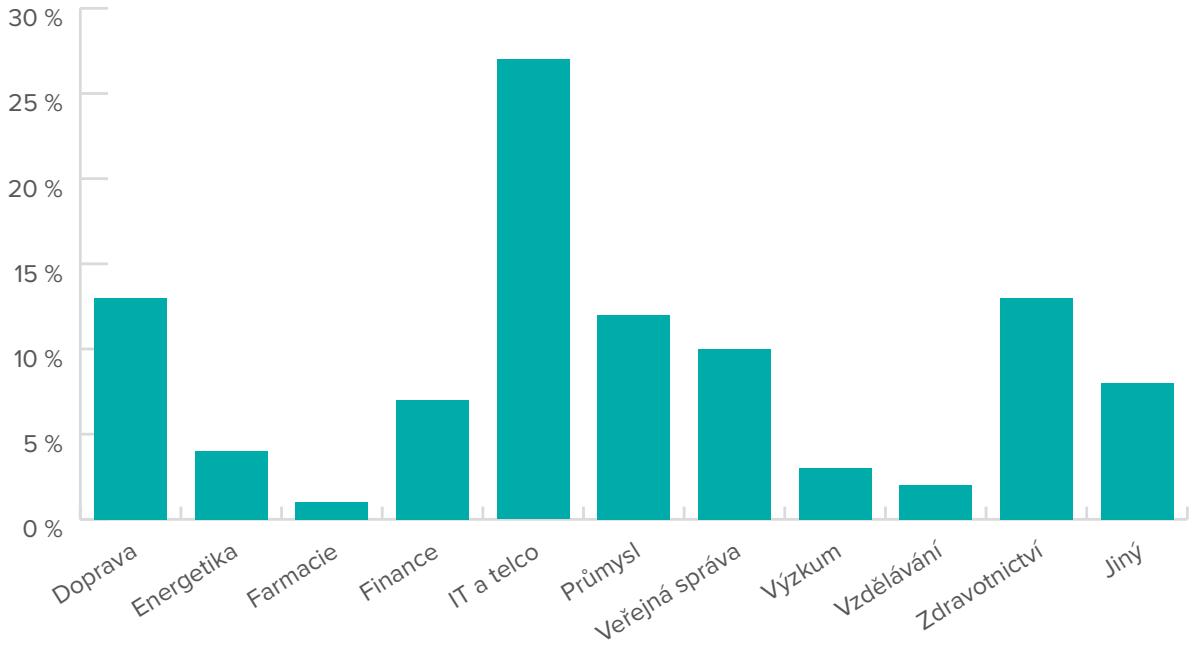
Radek Švadlenka

Obecně přijímané pravidlo praví, že systém je tak silný jako jeho nejslabší článek. A v oblasti bezpečnosti to platí dvojnásobně. Přestože organizace investují 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 běžné 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. Nově schválená a uveřejněná směrnice Evropské unie NIS2 po její transpozici do české legislativy bude mít vliv na dalších několik tisíc nových subjektů, nicméně na reálné dopady si musíme ještě nějaký čas počkat.

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 2022 s ohledem na plánovaná opatření pro rok 2023. Do většiny aktivit organizací v loňském roce stále ještě zasáhla slábnoucí pandemie Covid-19. Některé subjekty mohly být ovlivněny konfliktem na Ukrajině. O to zajímavější je meziroční srovnání plánovaných a realizovaných aktivit v oblasti vzdělávání v kybernetické bezpečnosti. Průzkumu se zúčastnilo bezmála osmdesát 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.

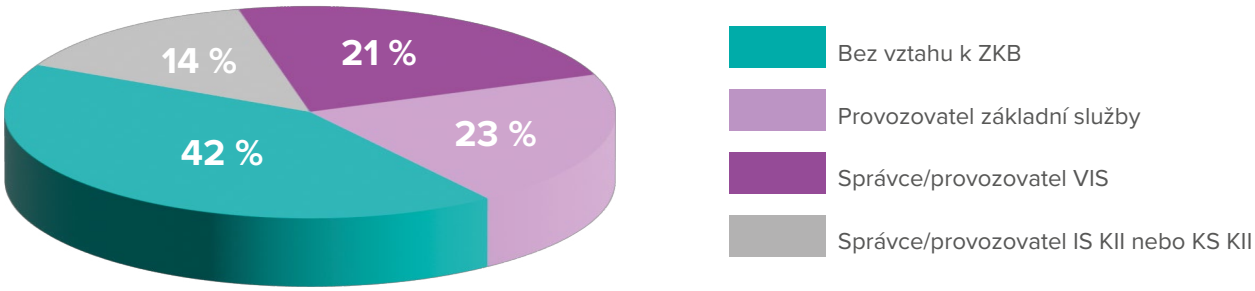


Procentuální zastoupení organizací dle oboru



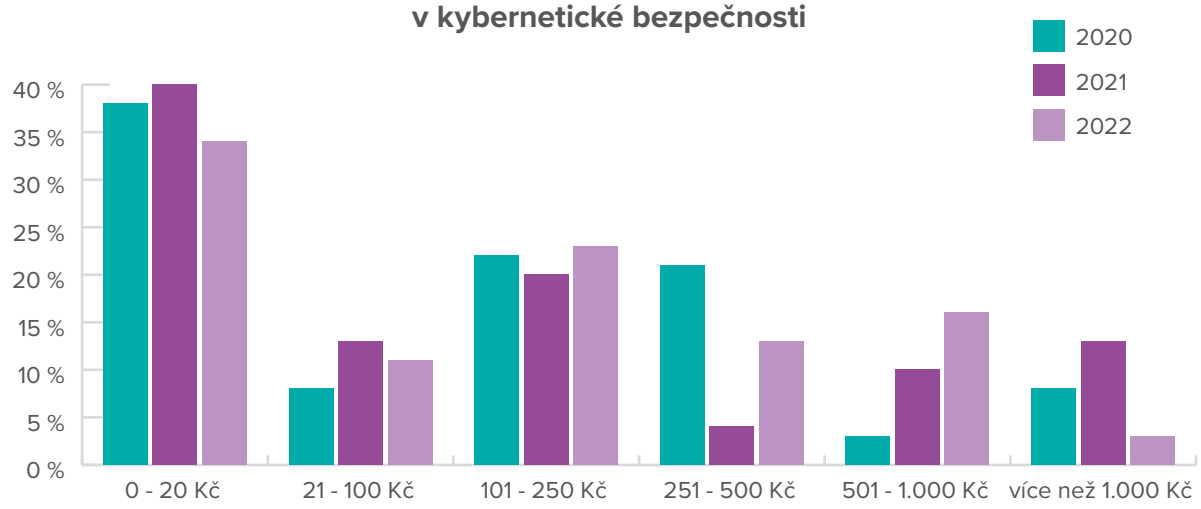
Aby interpretace dílčích výstupů nebyla zkreslena, je třeba upřesnit, že více než polovina respondentů průzkumu se řadí mezi povinné subjekty podle zákona o kybernetické bezpečnosti, jak ilustruje následující graf.

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. Aktuálně slábnoucí epidemie by však měla naznačovat spíše opačný trend. V grafu níže je možné sledovat porovnání investovaných prostředků do vzdělávání v letech 2020, 2021 a 2022. Jako pozitivní trend je možné označit postupný růst počtu organizací, které investují do vzdělávacích aktivit 501–1000 Kč na zaměstnance. Stejně tak meziročně vrostl počet firem investujících do vzdělávání mezi 251 Kč a 500 Kč na zaměstnance. Bohužel, množství organizací s ochotou investovat do vzdělávání zaměstnanců více než 1000 Kč meziročně významně poklesl. Subjekty s minimálním objemem investic do vzdělávání je sice méně, ale stále se drží na vysoké úrovni.

Zastoupení organizací dle výdajů na vzdělávání v kybernetické bezpečnosti

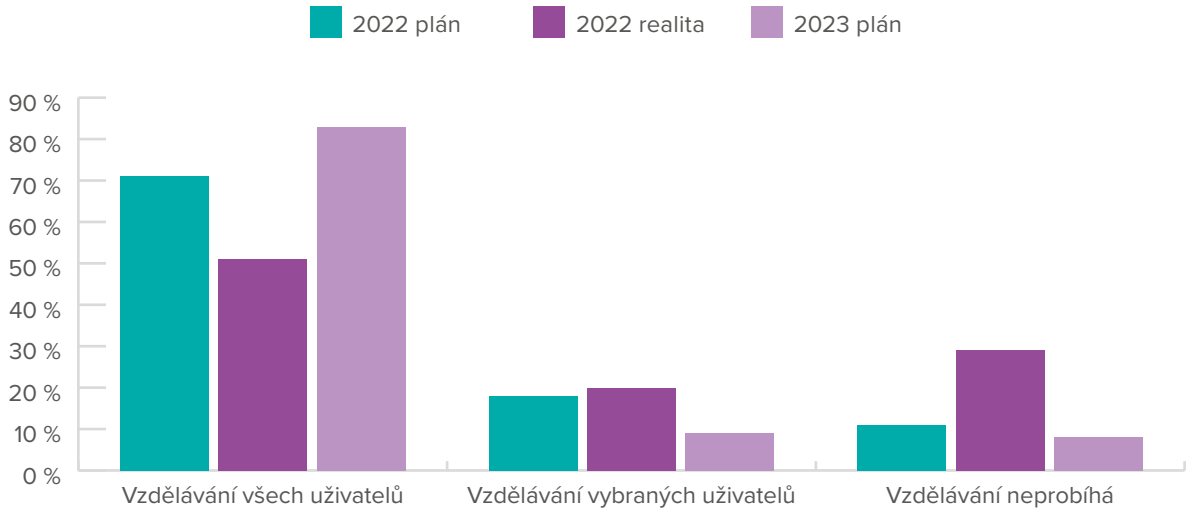


Průměrný měsíční náklad na zaměstnance

Vzdělávání uživatelů – realita versus plán

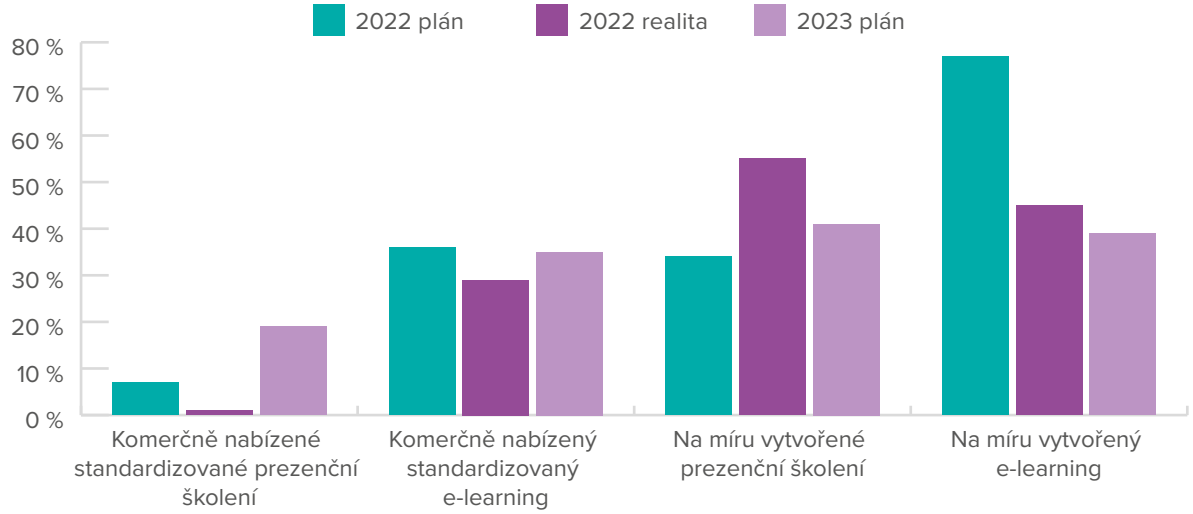
V této části průzkumu se zástupci organizací vyjadřovali k realizovaným a plánovaným aktivitám v oblasti vzdělávání uživatelů s výjimkou bezpečnostních rolí. Bohužel z grafu níže je patrné, že plány z roku 2021 pro vzdělávání všech uživatelů nebyly v roce 2022 zdaleka naplněny. Naopak počet organizací, kde vzdělávání vůbec neprobíhá je více než dvojnásobný oproti plánu z předchozího roku. Mírně optimistický trend je vidět alespoň u vzdělávání vybraných uživatelů, kde realita lehce předčila plán z roku 2021. Co se týče plánu vzdělávacích aktivit pro rok 2023, v podstatě se průřezově příliš neliší od plánu pro rok 2022, s výjimkou ve prospěch vzdělávání všech uživatelů na úkor vybraných. Jaká však bude realita je těžké predikovat zejména s ohledem na další faktory (např. konflikt na Ukrajině), které mohou významně ovlivnit výsledky.

Procentuální zastoupení organizací dle oboru



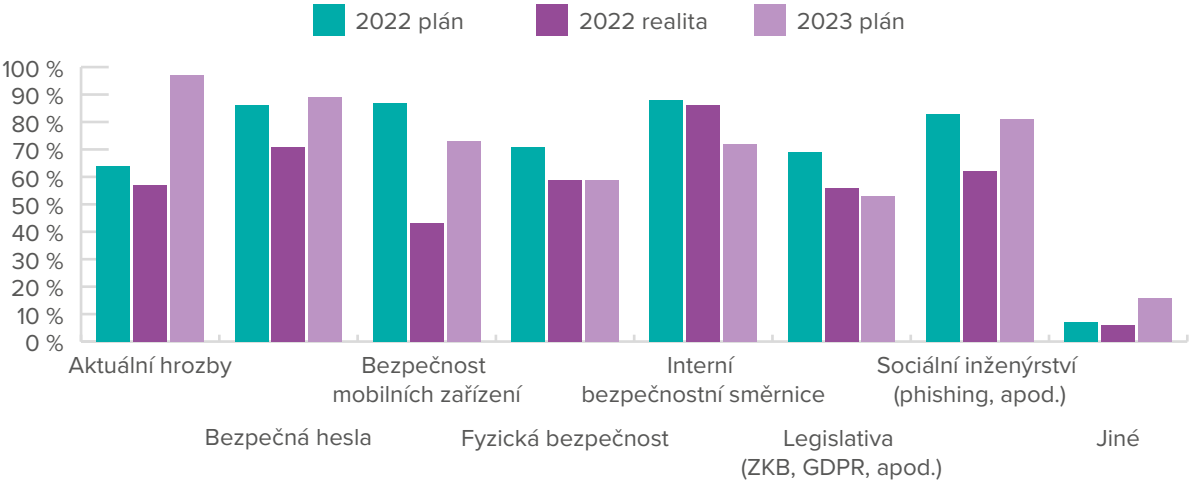
Zatímco na vzdělávání uživatelů obecně neměla probíhající pandemie významný dopad, jak bylo demonstrováno v předchozím grafu, jinak je tomu zákonitě s ohledem na plánované a realizované formy vzdělávání uživatelů. Jak je patrné z obrázku níže, preference e-learningových školení s ústupem pandemie klesá ve prospěch „na míru“ vytvořených prezenčních školení oproti plánu stanoveném na konci roku 2021. Z odpovědí týkajících se plánu na rok 2023 je možné predikovat postupný trend návratu k vyrovnanému poměru mezi e-learningovými nástroji a prezenčním školením. Stejně tak se dá očekávat konvergence mezi standardizovanými formami trainingu zaměstnanců a těmi „na míru“ vytvořenými.

Realizované/plánované formy vzdělávání uživatelů



Za nepříliš optimistický je možné pokládat vývoj v oblasti zaměření vzdělávání pro uživatele. Oproti plánovaným aktivitám došlo ve všech kategoriích k významnému poklesu v počtu firem zaměřujících se na danou oblast. Největší zájem byl obecně spojen s problematikou interních směrnic, bezpečných hesel a sociálního inženýrství. Naopak méně organizací se soustředilo na oblast aktuálních hrozeb, legislativy a bezpečnosti mobilních zařízení. Plán zaměření vzdělávacích aktivit pro uživatele na rok 2023 se příliš neliší od plánu pro rok 2022 s mírně klesajícím trendem, s výjimkou v oblasti aktuálních hrozeb, kde je výhled významně optimistický.

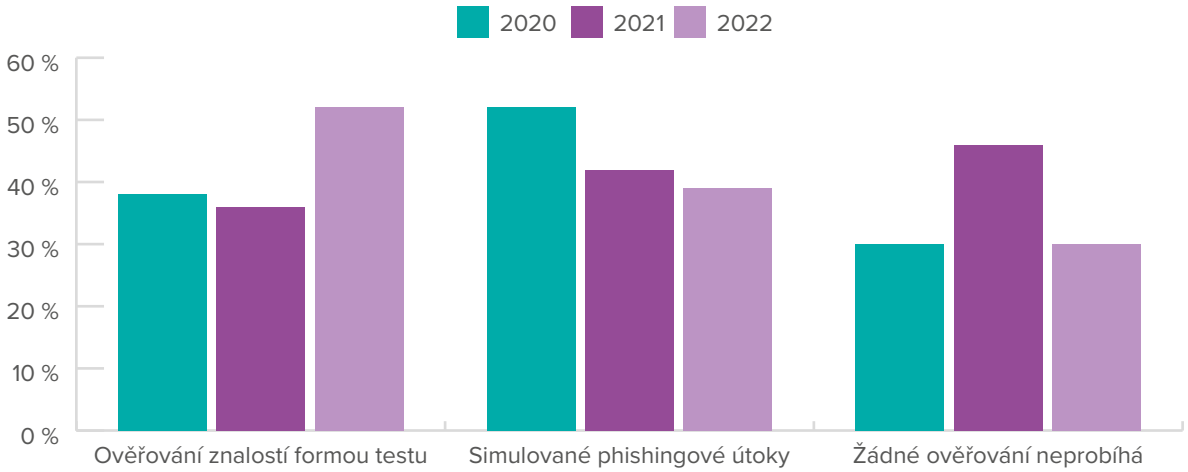
Zaměření vzdělávacích aktivit pro uživatele



Velice efektivní, ale zároveň také mezi zaměstnanci málo oblíbené, jsou aktivity spojené s ověřováním znalostí a ostražitosti uživatelů v oblasti kybernetické bezpečnosti. Obrázek níže ilustruje aktuální rozložení využívání těchto aktivit u sledovaného vzorku subjektů.

Celkový trend spojený s těmito aktivitami vykazuje pozitivní vývoj. Ověřování znalostí formou testů využilo meziročně významně více organizací s rozdílem 16 %. Počet organizací, zaměřujících se na ostražitost uživatelů pomocí simulovaných phishingových útoků klesl meziročně o 3 %. Pozitivní trend je možné pozorovat i na počtu organizací, kde žádné ověřování neprobíhá. Hodnota za rok 2022 vyrovnala výsledek z roku 2020 a výrazně vylepšila výsledek za rok 2021. Mírný optimismus může být spojen také s výhledem na rok 2023, kdy 83 % organizací plánuje zavést alespoň nějaké aktivity zaměřené na ověřování znalostí uživatelů v oblasti kybernetické bezpečnosti, což je zlepšení o 7 procentních bodů oproti výhledu v roce předchozím.

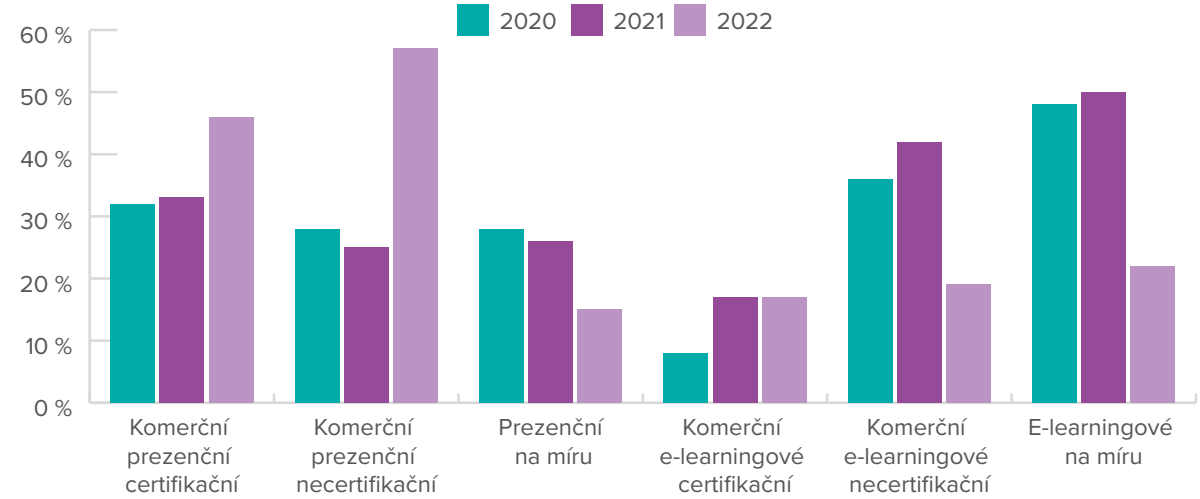
Ověřování znalostí a ostražitosti uživatelů



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 meziroční růst v oblastech prezenčního školení s výjimkou kategorie školení „na míru“. Naopak e-learningové formy vzdělávání bezpečnostních rolí zaznamenaly pokles v podstatě ve všech formách s výjimkou kategorie komerčních certifikačních kurzů, kde je situace shodná s hodnotou v roce 2021. Obecně e-learningové vzdělávací aktivity v roce 2022 byly postupně tlumeny s ustupující epidemií.

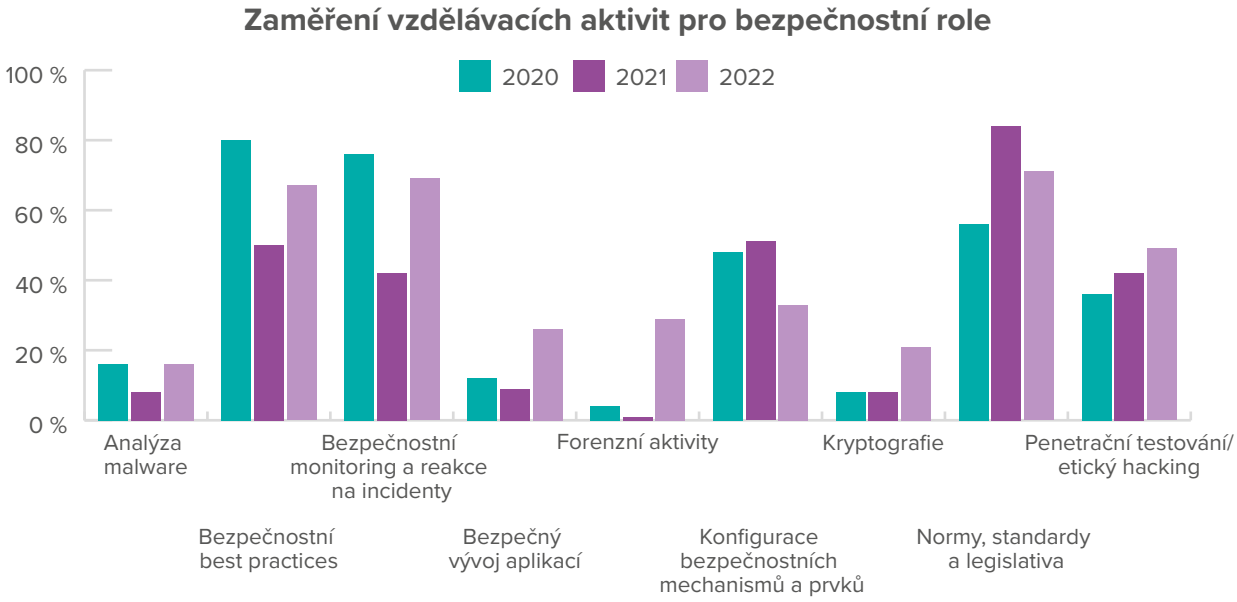
Realizované formy vzdělávání bezpečnostních rolí



Vzdělávání odborných rolí bývá na rozdíl od vzdělávání uživatelů mnohem specifičtěji zaměřeno, nicméně z průzkumu vyplývá, že společným atributem u obou těchto skupin je zvýšený zájem o rozšíření znalostí zákonné úpravy a návazné legislativy v oblasti kybernetické bezpečnosti.

Mezi další atraktivní oblasti vzdělávání pro odborné role evidentně patří bezpečnostní monitoring a reakce na incidenty a bezpečnostní best practices. Každé z výše vyjmenovaných zaměření vzdělávání bylo využito v roce 2022 více než polovinou respondentů.

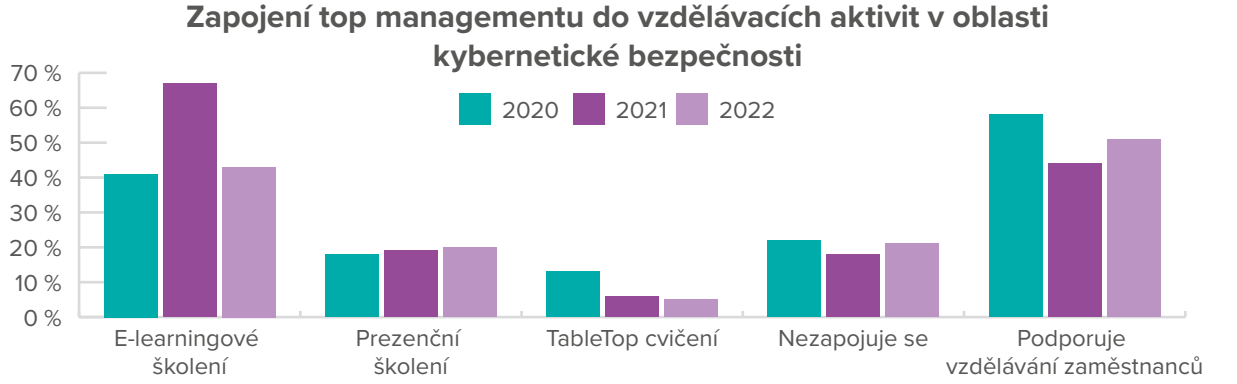
Mezi dlouhodobě „slabší“ témata z hlediska vzdělávání bezpečnostních rolí je možné zařadit oblasti kryptografie, forenzních aktivit, bezpečného vývoje aplikací a analýzy malware, kde však v roce 2022 přece jenom došlo určitému nárůstu zájmu, jak je patrné z grafu níže.



Zapojení top managementu do vzdělávacích aktivit

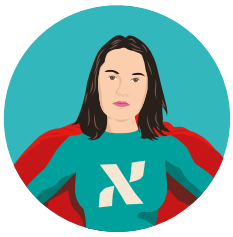
Vrcholový management organizací je možné považovat za speciální kategorii zaměstnanců se specifickými potřebami znalostí v oblasti kybernetické bezpečnosti. Manažer, který si není vědom aktuálních hrozeb, se může snadno stát terčem cíleného útoku.

Zajímalo nás tedy, jak se top manažeři vypořádávají s touto problematikou. Ne příliš pozitivní zprávou je, že meziročně stagnuje počet manažerů, kteří se vůbec nezapojují do vzdělávacích aktivit. Zároveň výrazně klesl podíl vedoucích pracovníků, kteří se vzdělávají formou e-learningu. Forma prezenčního školení si dlouhodobě udržuje stabilní hodnotu okolo 20 %, ale meziročně klesl zájem o TableTop cvičení, což pravděpodobně ještě souvisí s pandemickou situací. Zajímavým jevem je pak postupný návrat podpory vzdělávání zaměstnanců ze strany top managementu.

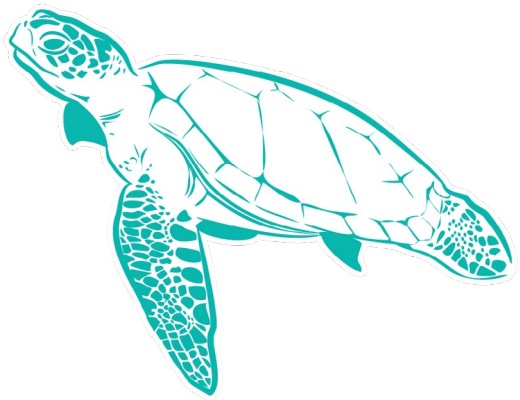


Závěr tohoto příspěvku je obohacen o zajímavé odpovědi z řad respondentů, týkající se top managementu a jeho orientace v kybernetické bezpečnosti a také vlivu epidemie na organizace. Celkem 98 % respondentů je přesvědčeno, že vyšší vzdělanost vrcholového managementu v kybernetické bezpečnosti má pozitivní vliv na rozvoj bezpečnosti v organizaci. Více než 60 % účastníků průzkumu souhlasí s názorem, že hlavním faktorem pro ochotu managementu investovat zdroje do kybernetické bezpečnosti jsou medializované kybernetické incidenty, případně interní incidenty. Zároveň 34 % 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. Více než třetina organizací vsadila na e-learningové nástroje pro vzdělávání zaměstnanců, nicméně aktuální trendy v rozvoji vzdělávacích aktivit jdou spíše směrem k návratu k prezenčním školením, jak dokazují výše uvedené výsledky.

Úroveň šifrování webserverů na českém internetu

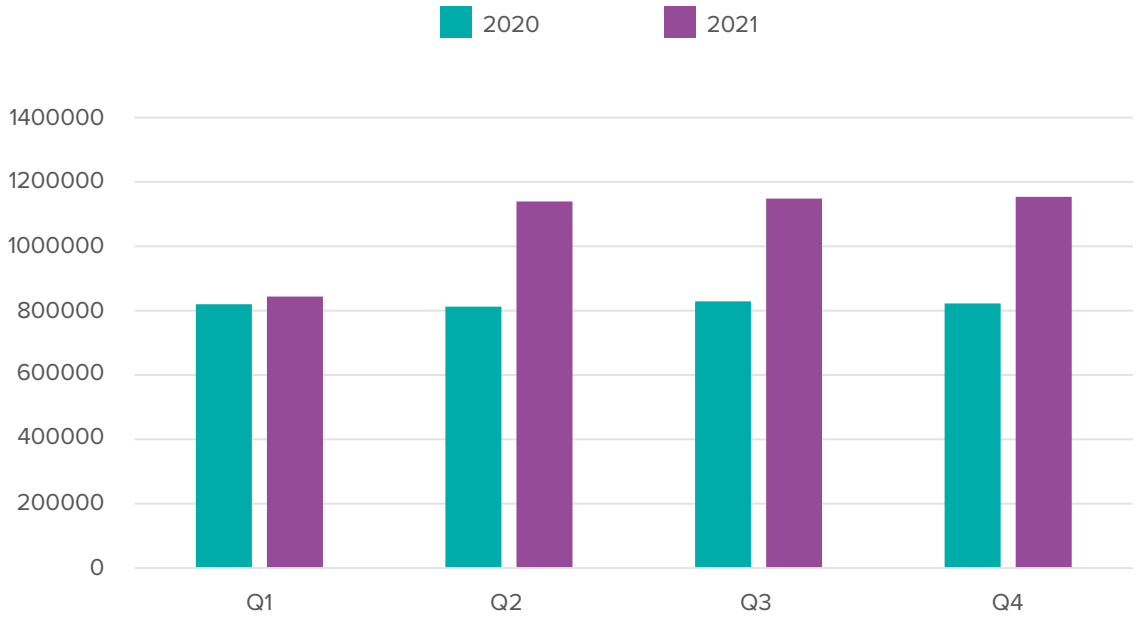


Oleksandra Kocyba



Tak jako minulý rok se podíváme na úroveň šifrování webových serverů na českém internetu. Z dat nahromaděných za rok 2022 na českém internetu se nejdříve podívejme na celkový počet detekovaných webových serverů, podporujících jak šifrovaný, tak i nešifrovaný provoz. V grafu můžeme vidět od druhého kvartálu výrazný nárůst celkového počtu webových serverů, což se poté promítá i do grafu níže, který porovnává poměr služeb HTTP a HTTPS na daných webových serverech.

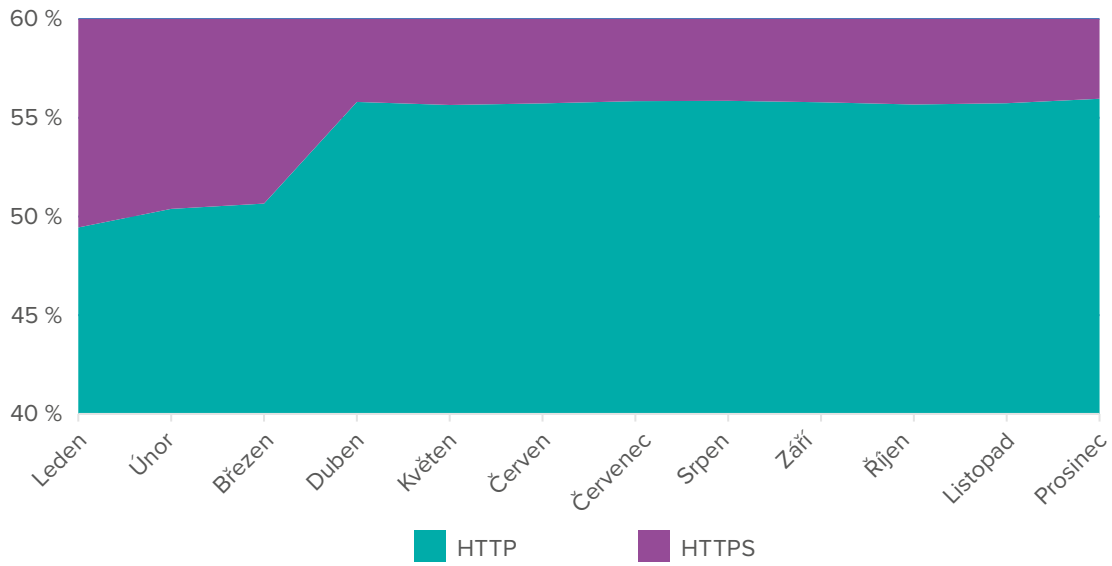
Porovnání počtu detekovaných webových serverů



Na grafu vidíme v druhém kvartálu jasné vychýlení v poměru webových serverů ve prospěch těch, které podporují nešifrovaný provoz. Změna poměru může souviset s celkovým nárůstem počtu webových serverů, kdy nové služby nemusí mít nastavenou podporu i pro šifrovanou komunikaci. Je důležité zmínit, že podpora protokolů HTTP i HTTPS není vzájemně exkluzivní. Mnoho webových serverů má otevřený jak port 80 (HTTP) používaný pro prvotní spojení s klientem, tak i port 443 (HTTPS), na který je klient následně přesměrován a kde poté probíhá komunikace šifrovaně.

Kdybychom dále tato čísla porovnali s grafem z minulého roku, držíme se u detekovaných webových serverů podporujících protokol HTTP přibližně na hodnotě 56 %. Podobnou hodnotu můžeme pozorovat i z minulého roku, a tak se poměr serverů podporujících HTTP a HTTPS protokoly udržuje přibližně stejný.

Poměr služeb HTTP a HTTPS na českém internetu

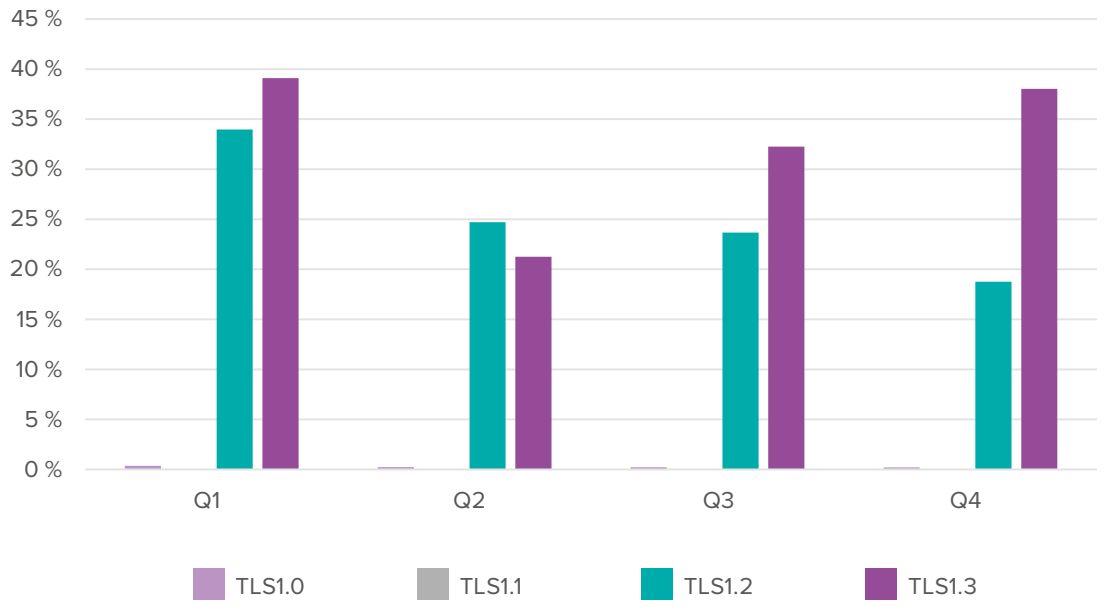


Analýza TLS a šifrovacích sad

Webová komunikace je šifrovaná pomocí protokolů TLS a předchůdce – SSL, jenž obsahuje známé zranitelnosti a z bezpečnostních důvodů by se již neměl používat. Nahradil jej TLS, který prochází vývojem již od roku 1999, od verze TLSv1.0 až po současnou verzi TLSv1.3., přičemž mezi doporučované verze od roku 2020 patří pouze TLSv1.2 a TLSv1.3. Na českém internetu se tato doporučení projevují - dle dat nahromaděných za rok 2022.

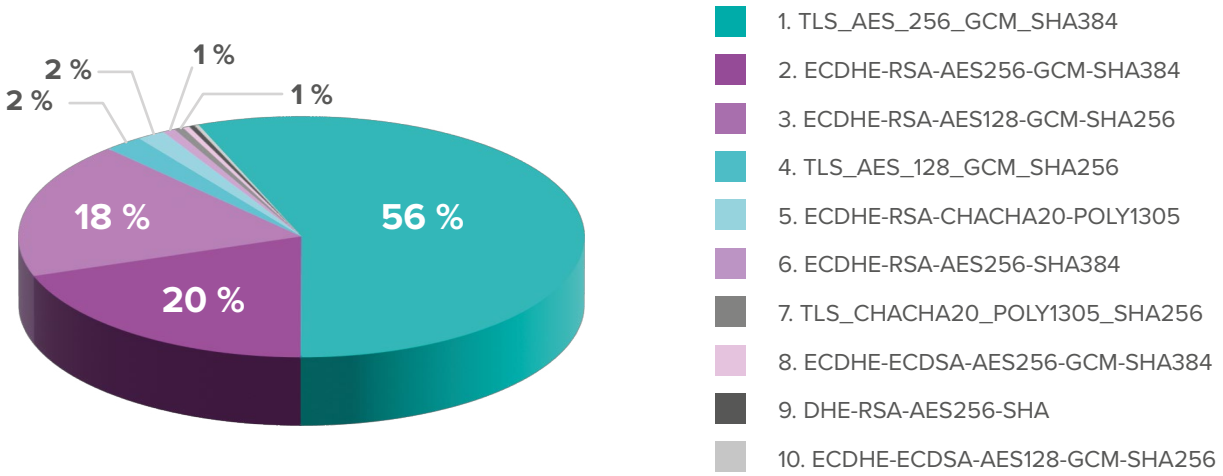
Z grafu můžeme pozorovat, jak v průběhu roku docházelo k postupnému snižování webových serverů podporujících TLSv1.0 (na 0,2 % ze všech detekovaných webserverů) a TLSv1.1 (na 0,001 %) a k nárůstu serverů podporujících TLSv1.3. V meziročním srovnání celkově vzrostl počet webových serverů podporujících šifrovanou komunikaci, zejména pak u TLSv1.3 se jedná o průměrný nárůst přibližně o 46 %.

Podpora verzí TLS na webových serverech - 2022



K zajištění šifrované komunikace však nestačí určit jen verzi TLS/SSL. Při navazování komunikace je nutné určit další důležité parametry, jako je šifrovací sada. Šifrovací sada určuje nejen algoritmus použitý při šifrování komunikace ale i algoritmus pro výměnu klíčů, algoritmus sloužící k autentizaci a MAC algoritmus zajišťující integritu přenášených dat. Vybraná šifrovací sada poté určuje jak bezpečná, kompatibilní a rychlá bude komunikace klienta se serverem.

Top 10 nejpoužívanějších šifrovacích sad



Šifrovacích sad je velké množství a pro tento report bylo vybráno 26 nejčastěji používaných. Jsou rozděleny do kategorií: Recommended (např. TLS-AES-256-GCM-SHA384), Secure (např. ECDHE-RSA-AES128-GCM-SHA256) a Weak (např. ECDHE-RSA-AES256-SHA384). V grafu níže jsou poté znázorněny počty webserverů podporujících danou kategorii šifrovacích sad. V porovnání s minulým rokem můžeme vidět postupný nárůst serverů podporující šifrovací sady kategorizované jako Recommended a i převýšení kategorie Secure, která vedla v prvních třech kvartálech roku 2021.

Webové servery podporující šifrovací sady dle kategorií

Tak jako z výsledků loňského reportu je i v letošním roce vidět pozitivní nárůst v počtu serverů podporujících šifrovanou komunikaci a postupná adaptace protokolu TLSv1.3 včetně bezpečnějších šifrovacích sad.

Analýza dat z e-mailových bran

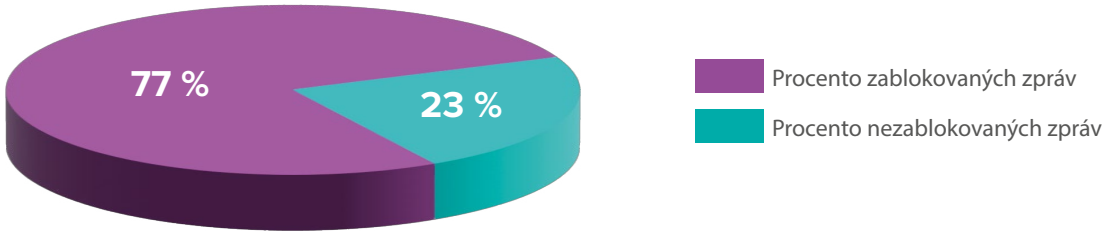
Michal Frýba

Tato část analýzy probíhala nad daty příchozích e-mailových zpráv, které byly přijaty vybranými e-mailovými branami v roce 2022.

V průběhu roku 2022 bylo zablokováno více než 76,6 % všech příchozích e-mailových zpráv. To znamená pokles o více než 10 % oproti předchozímu roku. Snížení počtu zablokovaných e-mailových zpráv může být způsobeno různými faktory. Některé statistiky naznačují, že spammeři se v současné době zaměřují spíše na kvalitu spamových e-mailů než na jejich kvantitu.

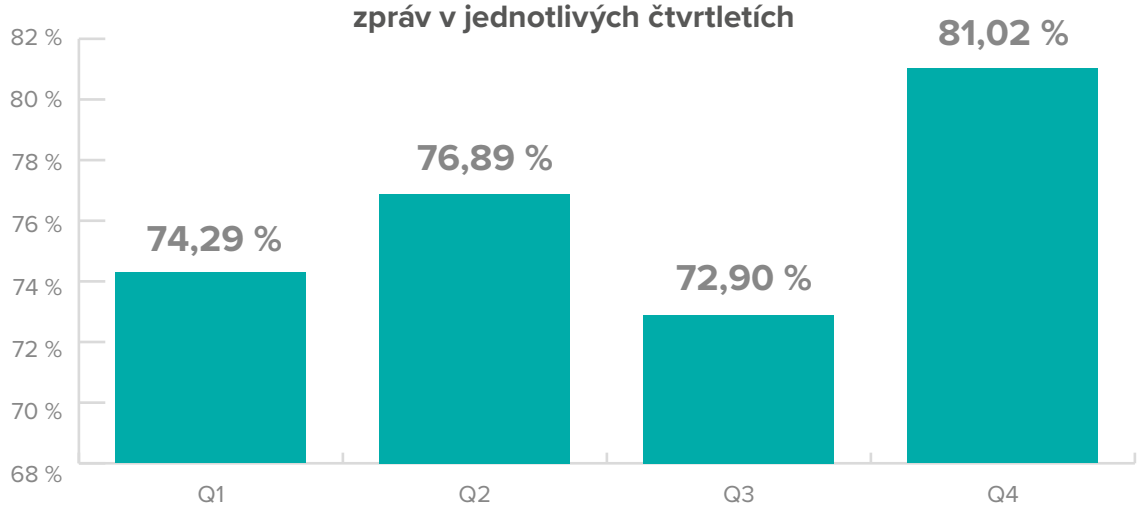
Lze ale spekulovat i o dalším faktoru, který může mít vliv na tento pokles - válka mezi Ruskem a Ukrajinou. Ruská federace se často řadí mezi státy, ze kterých pochází největší množství odeslaných spamových e-mailů. Nicméně v současné době se, vzhledem k situaci, může pozornost ruských spammerů více soustředit na jiné aktivity, jako je například propaganda ruského vlivu v regionu.

Zablokované vs. nezablokované e-mailové zprávy



Průměrně bylo v každém čtvrtletí roku 2022 zablokováno e-mailovými branami 76,6 % zpráv. Nejvyšší procento blokovaných zpráv bylo zaznamenáno v posledním čtvrtletí, které zahrnuje měsíce říjen, listopad a prosinec. V této době se počet zablokovaných zpráv vyšplhal na 81 procent.

Procento zablokovaných e-mailových zpráv v jednotlivých čtvrtletích



Po provedení agregace dat do jednotlivých čtvrtletí byl identifikován výrazný nárůst blokovaných e-mailových zpráv mezi třetím a čtvrtým čtvrtletím roku 2022. Příčinou této zvýšené aktivity se s největší pravděpodobností staly blížící se vánoční svátky a konec roku a přípravy spojené s těmito událostmi. V této době dochází k vyššímu výskytu neopatrného chování uživatelů, kteří očekávají doručení různých typů zásilek nebo faktur. Snižuje se tak jejich pozornost, a to zvyšuje pravděpodobnost úspěšného útoku.

Výše zmíněný trend je útočníkům dobře známý. V tomto období tedy zasílají velké množství spamových e-mailů obsahujících malware nebo phishingové zprávy, s cílem maximalizovat své zisky. Zpravidla se snaží napodobit důvěryhodné zdroje, jako jsou banky nebo doručovatelé zásilek, což zvyšuje pravděpodobnost, že oběť klikne na odkaz a otevře škodlivý obsah.

Níže uvedený graf poskytuje přehled o podílu zablokovaných zpráv v jednotlivých čtvrtletích, což umožňuje rozdíl lépe vidět. Pokles nicméně není až tak významný, jako tomu bylo v roce 2021, kdy byl rozdíl mezi třetím a čtvrtým čtvrtletím přibližně 20 %. Pozorovat lze také poměrně stabilní počty v první polovině roku.

Období dovolených a pokles počtu zablokovaných e-mailových zpráv

Třetí čtvrtletí, které zahrnuje měsíce červenec, srpen a září, je obvykle spojeno s větším množstvím dovolených ze strany uživatelů. Tento fakt lze pozorovat i v počtu zablokovaných zpráv, kdy se v tomto období vyskytuje výrazný pokles. Pravděpodobně je to z toho důvodu, že pro útočníky není efektivní odesílat velké množství zpráv se škodlivým obsahem, protože uživatelé na dovolené s nimi neinteragují.

Další vysvětlení může spočívat v tom, že sami útočníci jsou také na dovolených a neodesílají spamové a phishingové zprávy.

Analýza důvodu blokace e-mailových zpráv

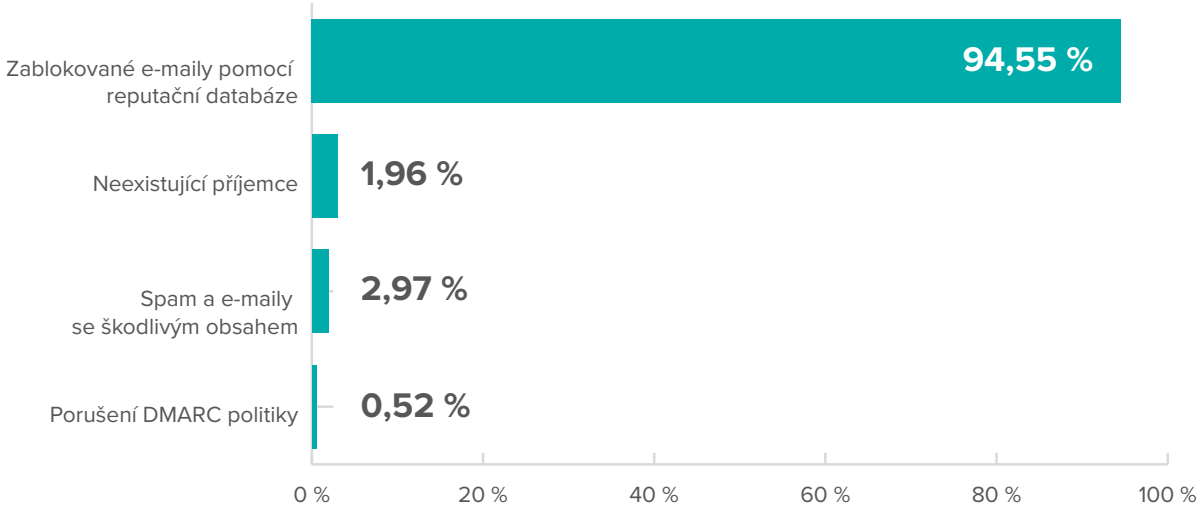
Při analýze důvodů blokace e-mailových zpráv na e-mailových branách jsme zjistili, že výrazná většina zablokovaných e-mailů byla zablokována pomocí reputační databáze (94,55 %). Reputační databáze přiděluje serverům skóre, a pokud je skóre nízké nebo negativní, pak je komunikace z tohoto serveru zablokována.

Další důvod blokace představují neexistující příjemci (2,97 %), což může být způsobeno chybou při zadávání e-mailové adresy nebo tím, že e-mailová adresa již neexistuje, ale stále je uložena v seznamech útočníků nebo je zveřejněna na stránkách společnosti.

Další blokovanou kategorií byly e-maily identifikované jako spam a e-maily se škodlivým obsahem, které představují 1,96 % zablokovaných e-mailů. Tyto zprávy obsahovaly odkazy na škodlivé webové stránky a pouze menší část měla přílohu obsahující software.

Posledním důvodem blokace e-mailů je porušení DMARC politiky. Tento důvod se týkal zhruba 0,52 % všech zablokovaných e-mailů. DMARC politika je založena na nastavení pravidel pro validaci a ochranu proti podvrženým e-mailům. Tato politika je nastavena u doménového jména v adrese odesílatele a kontroluje se na legitimní i podvržené e-maily. Pokud e-mail nesplňuje DMARC politiku, může být označen jako podezřelý nebo, jako v našem případě, zablokován na e-mailové bráně.

Zablokované e-mailové zprávy podle kategorií



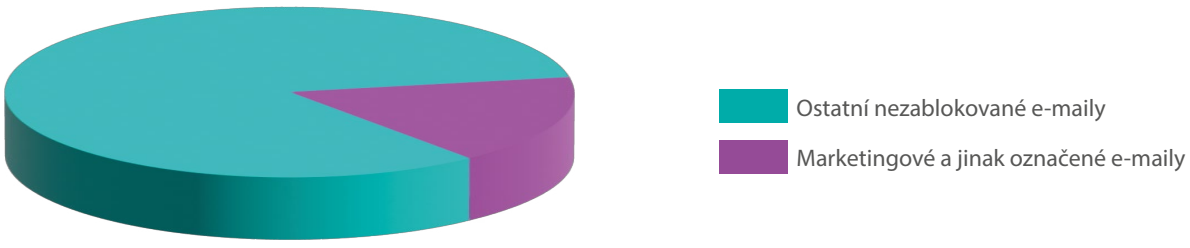
Marketingové a jinak označené e-mailové zprávy (Graymail)

E-mailové brány dokážou identifikovat a označovat e-mailové zprávy, které obsahují marketingové údaje nebo jsou zasílány ze sociálních sítí. Tyto typy zpráv jsou obvykle označovány jako „Graymail“. Někteří uživatelé je mohou považovat za nevyžádanou poštu, ale jiní si naopak tuto poštu vyžádali. Proto se tyto zprávy nacházejí v nejisté „šedé zóně“ mezi spamem a legitimními e-maily. Je třeba mít na paměti, že označení těchto e-mailových zpráv jako „Graymail“ je komplexní proces a nelze jednoznačně určit, zda se jedná o nevyžádanou poštu. Z celkového počtu analyzovaných zpráv tvořily přibližně 4 %.

E-mailové brány tedy tyto zprávy automaticky neblokují, ale označují je různými příznaky, jako například vložením textu „[Marketing]“ do předmětu e-mailové zprávy. V našem vzorku dat z e-mailových bran se 26,88 % z celkového počtu rozpoznaných graymailů označilo právě takto. Hromadné zprávy tvořily 65,09 % graymailů a zprávy ze sociálních sítí tvořily 8,03 %.

V celkovém vzorku nezablokovaných zpráv bylo procentuální zastoupení graymailu (tj. výše zmíněné kategorie) 17,2 %. Zbývajících 82,8 % nezablokovaných zpráv bylo považováno za legitimní e-maily, což odpovídalo 19,32 % z celkového počtu všech zpráv. V roce 2021 tvořily graymaily 9,87 % nezablokovaných zpráv, což odpovídalo 1,15 % celkového počtu. Jedná se tedy o výrazný nárůst.

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

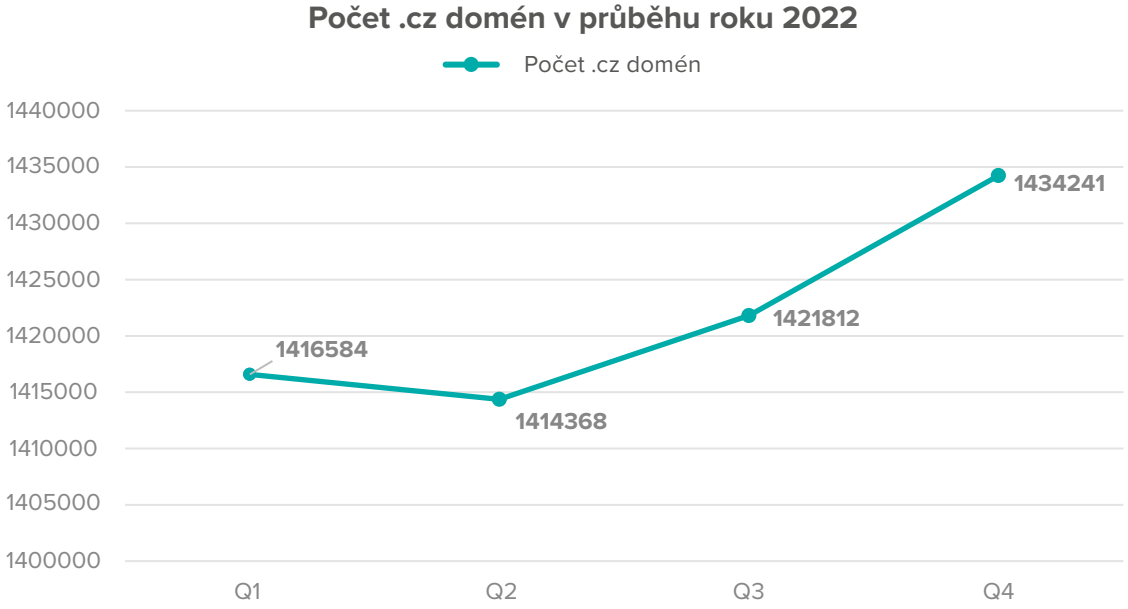


Stav adopce bezpečnostních mechanismů SPF, DKIM a DMARC v ČR

Milan Habrcetl

Bezpečnostní mechanismy Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) a Domain-based Message Authentication, Reporting and Conformance (DMARC) umožňují, při korektní konfiguraci, organizacím zamezit podvrhování jejich domén při posílání e-mailových zpráv. Útočníci tedy nemohou zneužít doménu organizace, která má správně nastavené bezpečnostní mechanismy SPF, DKIM a DMARC, a tím lze zabránit phishingovým útokům, které by zneužívaly legitimní doménu a které by si tímto způsobem jednoduše zvýšily důvěryhodnost e-mailových zpráv u uživatelů.

Data, která byla využívána v rámci analýzy, byla sesbírána na konci každého čtvrtletí roku 2022. Na základě takto sesbíraných informací bylo zjištěno, že se počet .cz domén v průběhu roku téměř nemění. Dle grafu níže lze vidět, že počet .cz domén se zvětšil o necelých 20 tisíc.



Mechanismus DKIM nelze ověřovat bez interakce a spolupráce s vlastníky domén a z toho důvodu není tento mechanismus zahrnut do analýzy níže.

Sender Policy Framework

Tento bezpečnostní mechanismus umožňuje organizacím definovat, které servery mohou odesílat e-mailové zprávy, které využívají danou doménu organizace. Kromě seznamu serverů, které mají toto oprávnění, by na konci SPF záznamu nemělo chybět pravidlo, jak zacházet se zprávami z ostatních serverů, které nebyly specificky definovány v tomto záznamu. Toto pravidlo může mít 4 různé hodnoty a to:

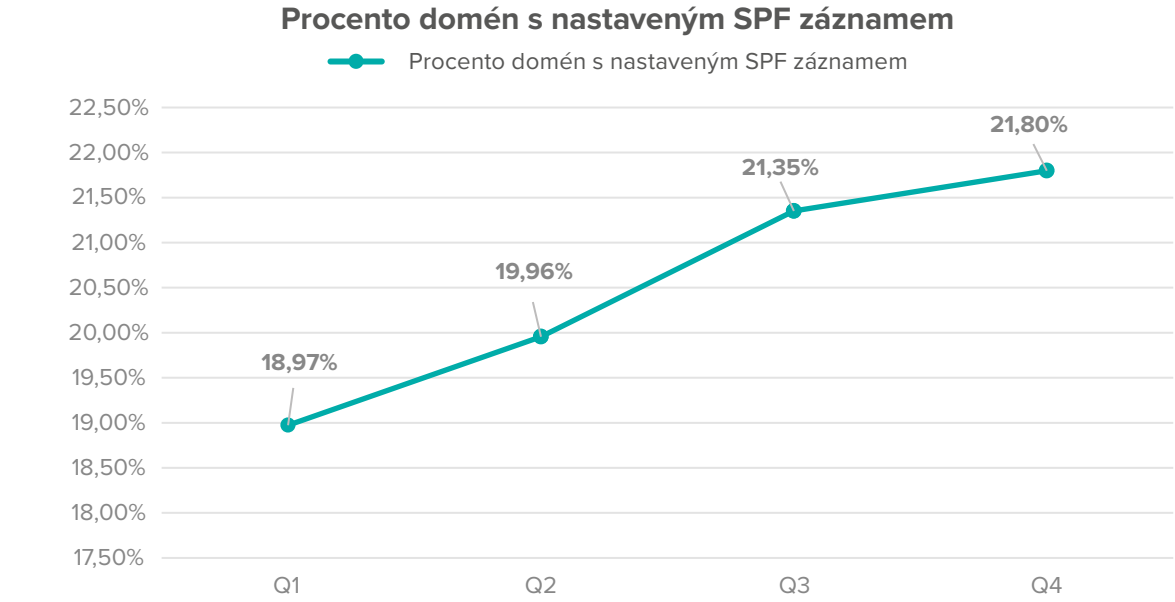
1. „-all“, což se označuje za politiku „fail“, podle které se e-mailová zpráva zahodí
2. „~all“, což se označuje za politiku „softfail“, podle které se e-mailová zpráva vloží do karantény, nebo se označí, ale přepošle uživateli
3. „?all“, což se označuje za politiku „neutral“, podle které se s e-mailovou zprávou nestane nic
4. „+all“, což se označuje za politiku „pass“, podle které mohou odesílat všechny servery zprávy s doménou, u které je nastaven tento SPF záznam

Příjemce si samozřejmě může upravit, co přesně se s e-mailovými zprávami na e-mailové bráně provede, například jestli se vloží do karantény i zprávy, které neprojdou SPF kontrolou s „fail“ politikou apod.

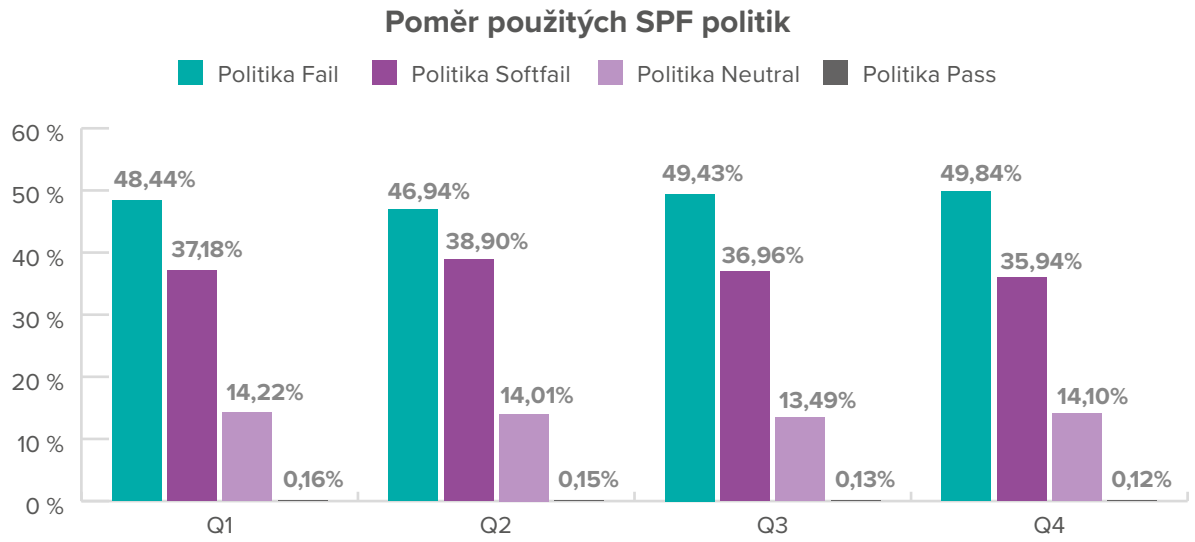
Doporučená konfigurace využívá první (-all) nebo druhé (~all) zmíněné pravidlo. Při prvotní konfiguraci je vhodné použít třetí typ (?all) a po vyzkoušení správné konfigurace oprávněných serverů je vhodné ho změnit na první nebo druhý typ. Čtvrtý typ tohoto pravidla by se pak neměl využívat nikdy, protože to znamená, že je SPF záznam zbytečný, jelikož jsou tímto způsobem oprávněny všechny servery k odesílání e-mailových zpráv z této domény.

Český internet a SPF záznamy

Adopce SPF mechanismu na doménách České republiky se průběžně během roku zvyšovala a na konci roku 2022 byl mechanismus SPF adoptován na více než pětině domén, přesněji na 21,80 procentech .cz domén.



Domény s nastaveným SPF záznamem pak byly rozděleny do čtyř skupin, dle pravidel pro ostatní, nespecifikované servery, tato pravidla jsou popsána výše. Většina domén, které měly nastaven nějaký SPF záznam, používala první dva popsané typy tohoto pravidla. Zbytek těchto domén měl většinou nastaven třetí typ tohoto pravidla a několik domén používalo silně nedoporučovaný typ pravidla, kde na konci roku 2022 takto bylo nastaveno 0,13 procent českých domén. Na následujícím grafu je znázorněn procentuální poměr těchto metrik.



Většina domén tedy používá doporučenou politiku fail nebo softfail. Na následujícím grafu je znázorněn poměr použití doporučené konfigurace SPF pravidel oproti použití nedoporučené konfigurace v konečném stavu roku 2022.

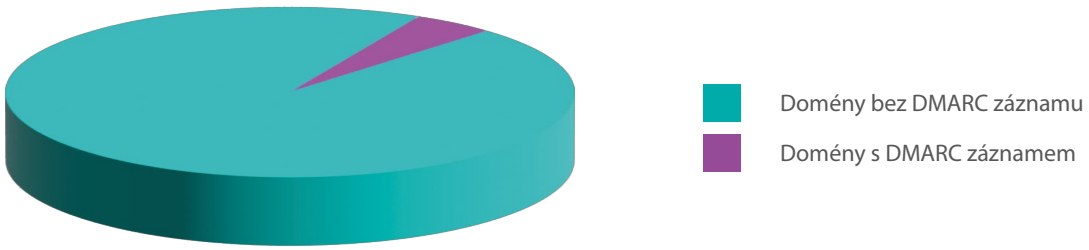
Poměr použití doporučené a nedoporučené konfigurace SPF záznamu na konci roku 2022

Český internet a adopce DMARC

Bezpečnostní mechanismus Domain-based Message Authentication, Reporting and Conformance (DMARC) umožňuje organizacím definovat politiku zacházení s e-mailovými zprávami, které neprojdou kontrolou pomocí mechanismů SPF a DKIM. Dále umožňuje upravit mechanismus kontroly těchto dvou mechanismů a tím organizace dokáže zabránit slabinám těchto mechanismů. Jedním z hlavních důvodů DMARC mechanismu je možnost získávání forenzních informací o e-mailech zablokovaných na základě SPF a DKIM. Tyto forenzní informace jsou odesílány v analytických reportech v rámci e-mailové zprávy na e-mailovou adresu, která je určena v DMARC záznamu. Tyto analytické reporty mimo jiné obsahují informace o důvodu blokace daného e-mailu. Organizace tímto způsobem může získat informace, že se někdo snaží podvrhovat jejich domény v rámci phishingových kampaní.

Z téměř jednoho a půl milionu (1 434 241) .cz domén byl na konci roku 2022 nastavený DMARC záznam pouze u necelých 5 procent z nich.

Poměr českých domén s DMARC záznamem a bez něj na konci roku 2022



V rámci statistických dat získaných z českých domén pak byly analyzovány dva parametry v DMARC záznamech, které jsou pro správné fungování DMARC mechanismu nutné.

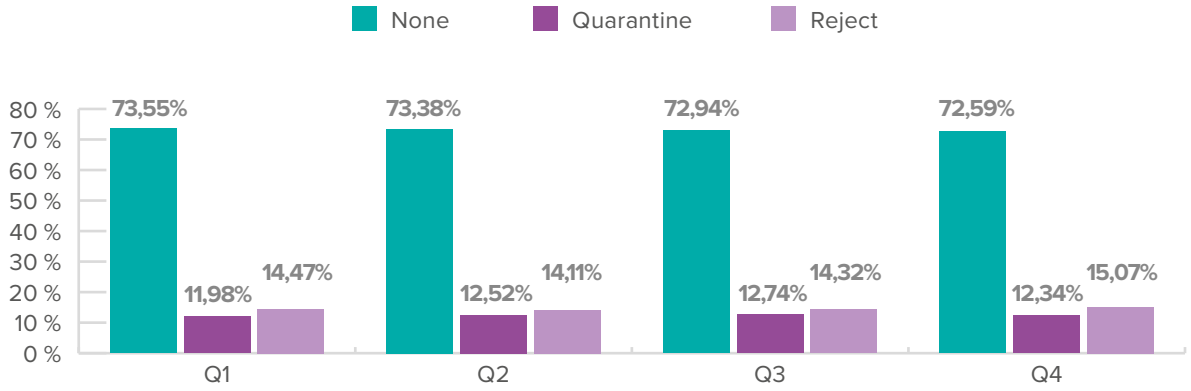
Jedním z těchto parametrů je parametr politiky „p“, který určuje, co se má provést s e-mailovou zprávou, která neprošla kontrolou mechanismů SPF a DKIM. Tento parametr může nabývat hodnot:

1. None – tato hodnota určuje, že se nelegitimní e-mailová zpráva nebude blokovat. Tuto hodnotu je doporučeno využívat po dobu několika měsíců po prvotním nastavení mechanismu DMARC a po vyhodnocení doručených DMARC reportů přepnout tuto hodnotu na jednu z následujících.

2. Quarantine – Tato hodnota způsobí to, že nelegitimní e-mailová zpráva bude označena jako spam a vložena do karantény, případně do adresáře se spamem.
3. Reject – Tato hodnota způsobí nedoručení nelegitimní e-mailové zprávy uživateli.

Stejně jako tomu je u SPF mechanismu, příjemce si na své e-mailové bráně může nakonfigurovat, co se reálně má s takovými zprávami provést a může tedy i v rámci politiky „Reject“ zprávu vložit do karantény místo jejího smazání apod.

V následujícím grafu je vyobrazen poměr využití těchto parametrů v jednotlivých kvartálech roku 2022:

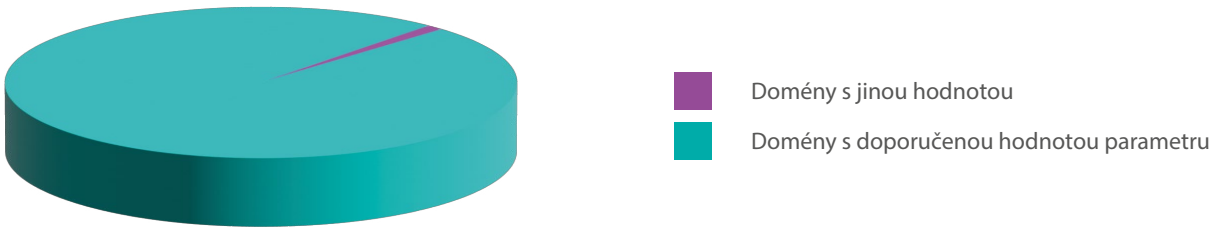


Druhým ze sledovaných parametrů je parametr pct, který určuje na kolik procent e-mailových zpráv, které neprošly kontrolou mechanismy SPF a DKIM má být aplikována politika z parametru popsaného výše. Doporučená hodnota tohoto parametru je 100, což znamená stoprocentní blokace nelegitimních e-mailových adres v případě reject politiky. Pokud není tento parametr v DMARC záznamu definován, jeho hodnota je automaticky nastavena na 100.

V naší analýze jsme rozdělili hodnoty tohoto parametru na dvě skupiny:
1. Hodnota nenastavena nebo nastavena na 100
2. Hodnota nastavena v rozmezí 0-99

V průběhu roku se počet českých domén, které mají definovaný tento parametr s doporučenou hodnotou, pohyboval kolem 99 procent z domén, které DMARC záznam mají nastaven. Toto lze vypozorovat v následujícím grafu, který znázorňuje stav na konci roku 2022:

Poměr českých domén s DMARC záznamem s doporučenou hodnotou parametru pct na konci roku 2022



Závěr

Adopce SPF mechanismu na české doméně (.cz) se oproti minulému roku zvýšila o 2 procenta a adopce mechanismu DMARC pouze o 1 procento, což nebyl tak velký nárůst, jaký byl očekáván kvůli ochrannému opatření, které Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) vydal 11. října 2021.

Toto opatření pojednává (https://www.nukib.cz/cs/infoservis/aktuality/1758-spravci-klicovych-systemu-musi-zabezpecit-sve-e-mailove-schranky/) o povinnostech zabezpečení e-mailové komunikace a mimo jiné popisuje povinnost a náležitosti implementace SPF, DKIM a DMARC mechanismů.

Kyberbezpečnostní technologie: buzzwordy a trendy

Jiří Herzig

V minulém ročníku jsme se podívali na technologie, které naši zákazníci používají a jakým směrem se chtějí v souvislosti s vylepšením kyberbezpečnostních technologií vydat. V tomto článku se zaměříme na možnosti, jaké v tomto ohledu máme. Internetem se šíří různé buzzwordy a hesla, často pouze jednoduché písmenné zkratky. Co si pod nimi představit a jaké jsou obecně trendy v kyberbezpečnosti? To si přečtěte v článku.

V dnešní době se bezpečnost začíná více a více zaměřovat na zabezpečení uživatelů a jejich koncových zařízení. Není to z toho důvodu, že by snad infrastruktura a perimetr byly v bezpečí a nehrozil jim žádný útok. Je to především proto, že s rozmachem chytrých mobilních telefonů, dostupností internetu a rozšíření služeb dostupných z cloudu, se útočníci orientují právě na uživatele a jejich zařízení. Uživatelé totiž často nejsou odborníci na bezpečnost a málokterý z nich přemýšlí o problémech jako riziku nekontrolovaného surfování po internetu, rozpoznání phishingového e-mailu od legitimního, případně o generování hesla o 12 znacích se složitostí minimálně 3 ze 4 pak ani nemluvě.

V našem snažení tyto uživatele ochránit, nám mohou pomoci moderní technologie, které se na danou problematiku orientují. Představme si některé tyto technologie blíže.

2FA/MFA

Dnes je potřeba mít ke každé službě či zařízení uživatelský účet. Bez něj jsou možnosti velice omezené, pokud vůbec nějaké. V případě používání více samostatných účtů je problémem zapamatování si hesel, proto je nutné používat některého ze správců hesel. V případě že používáme např. OAuth a přistupujeme k více službám pomocí jednoho Google účtu, je potřeba mít tento účet, stejně jako přihlášení do správce hesel, dobře zabezpečen. Pokud nám totiž někdo toto heslo odcizí a my nemáme přihlášení ochráněno i jiným způsobem, útočník velice snadno získá velkou kontrolu nad naším elektronickým životem. Standardem se dnes stává použití druhého faktoru a stále častěji i více než dvou faktorů. Nevyužijeme tedy pouze to, co známe (jméno a heslo), ale i to co máme (zařízení, token) případně i to kdo jsme (biometrika). Výběr řešení je bohatý a některá z nich jsou nabízena i bezplatně. Pro nás pak bude důležité vybrat to, které splní všechny požadavky na funkčnost, náročnost nasazení, podporu a integraci s ostatními službami, a to za přijatelnou cenu. Novinkou v této oblasti je využití tzv. passwordless, díky kterému se vyvarujeme používání hesel a ověřování pak bude více závislé na dalších faktorech. Tato funkce je implementována u několika produktů světových výrobců (Microsoft, Apple, Cisco aj.).

EDR/XDR

Poté co se náš uživatel úspěšně přihlásí na své pracovní zařízení (notebook, mobilní telefon, pracovní stanice či tablet), je nezbytné mít zabezpečené i toto zařízení. Bylo by velice nepříjemné, pokud by se uživatel bezpečně přihlašoval, ale jeho práce by byla sledována pomocí KeyLoggeru, malware odesílal informace o zařízení či informací v něm uložených, případně nějaký ransomware toto zařízení zašifroval a po našem uživateli vyžadoval úplatu za dešifrování. Pryč je doba obyčejného antiviru, který zablokoval již známou hrozbu a uložil soubor do karantény. Útočníci se dnes zaměřují na zero-day útoky, fileless malware, případně jiné možnosti, jak obejít klasický antivirus. Je proto téměř nutností zařízení, která opouští bezpečný perimetr naší sítě a uživatelé z nich pracují z námi neznámých míst, případně svých domovů, zabezpečit pomocí EDR (Endpoint Detection and Response). Ten se zaměřuje na zařízení jako celek, změny chování procesů, pohyb a chování souborů, instalovaný software a další. XDR (eXtended Detection and

Response) rozšiřuje tuto ochranu na další zařízení a služby, jako jsou servery, cloudová úložiště, e-mail a jiné. Pomocí strojového učení, umělé inteligence, holistického přístupu a integrace napříč různými technologiemi dokáže přinést lepší přehled a ochranu, a to i pomocí prevence, detekce a případné reakce na incidenty.

SASE (Secure Access Service Edge)

V dnešní době velice často zmiňované heslo. SASE je chápáno jako spojení infrastruktury a bezpečnosti. Infrastruktura je v SASE zastoupena pomocí SD-WAN, tedy Softwarově Definovaná sít WAN. Pokud bychom SD-WAN ze SASE vynechali, získáme další heslo, které se nově začíná objevovat, a to SSE (Security Service Edge). O čem je tedy tato bezpečnost? Základem jsou SWG (Secure Web Gateway), Firewall jako služba, CASB (Cloud Access Security Broker), ZTNA (Zero-Trust Network Access) a hlavně řízení z jednotného prostředí umístěného v cloudu. SASE je zaměřeno na ochranu uživatele při jeho pohybu na internetu a je řízeno identitou tohoto uživatele. Dalo by se říci, že pro každého uživatele může poskytnout jiná pravidla. Zajistí kontrolu webových adres a kategorií, případně poskytne webovou proxy s možností dešifrování obsahu a kontrolu malware (SWG). Cloudový firewall zajistí IDS/IPS pro všechny uživatele, nezávisle na tom, odkud se připojují do internetu, bez potřeby zajišťovat fyzický hardware. CASB nám umožní kontrolu ostatních cloudových služeb a úložišť, přístup a kontrolu oprávnění uživatelů v těchto službách a případně vynucení bezpečnosti, jako je zákaz posílání příloh pomocí freemailových služeb, ukládání souborů na neschválená cloudová úložiště a jiné. Zero-trust využije multifaktorové ověření uživatele a zajištění nejmenšího potřebného oprávnění, které tento uživatel potřebuje. Dále také kontinuálně ověřuje, že tento uživatel je stále ten, koho ověřil. Největší výhodou řešení SASE je jednoznačně jeho integrace všech těchto funkcí do jednoho prostředí a tím usnadnění nastavení a správy. Jistě je možné takové řešení postavit od různých vendorů, nicméně si tím přiděláme více starostí, než bude výsledný zisk.

Nezávisle na technologiích, produktech a vendorech je potřeba sebe i uživatele vzdělávat. Velkým trendem je právě vzdělávání, zejména běžných uživatelů. Je třeba naše uživatele naučit rozpoznat škodlivý e-mail, používat silná hesla a nespoléhat se jen na základní nastavení služeb. O vzdělávání se více dočtete v jiném článku v tomto Security reportu.

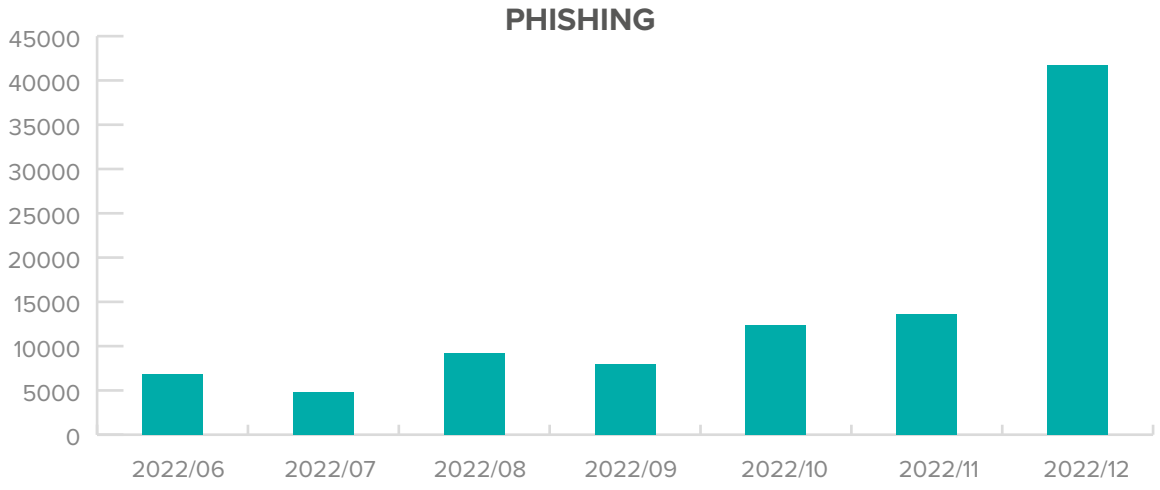
Kyberbezpečnost začíná být chápána jako součást každé sítě. Někde toto zjištění přijde včas, jinde bohužel až když je pozdě a škody jsou napáchány. Je ale vidět, že vznikají nové koncepty a architektury, které se pokoušejí nám, kteří se snažíme zabezpečit ostatní uživatele, usnadnit práci. Ať už je ale koncept, technologie, funkce či architektura jakákoliv, vždy bude potřeba těch, kteří tuto práci vykonají. Je proto důležité najít si správného partnera, který se kyberbezpečnosti věnuje a pokládá ji za důležitou nejen jako součást svých služeb, ale zejména jako směr, kterým je třeba se v našem elektronickém světě ubírat. Vždy bude někdo, kdo bude chtít získat naše data. A vždy bude někdo, jako je Alef, kdo se bude snažit vás před tímto ochránit. Na závěr mi nezbývá než dodat: Buďte v bezpečí a „Trust the Strong“.

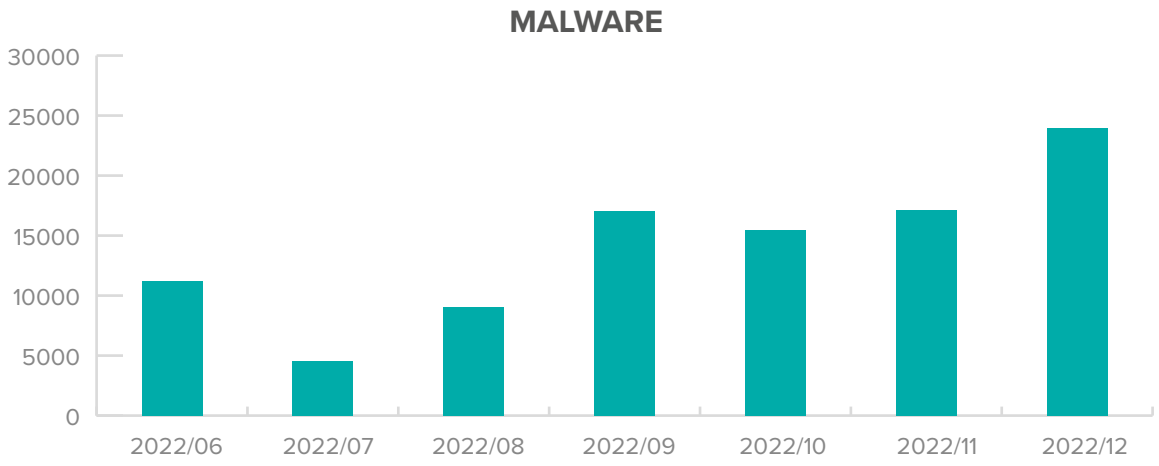
Analýza událostí zachycených IPS sondami

Stanislav Techlovský

Následující část reportu se zabývá analýzou dat z IPS (Intrusion Prevention System) sond pod zprávou společnosti ALEF Nula a.s. Analýza se zaměřuje na data z období posledních dvou kvartálů roku 2022.

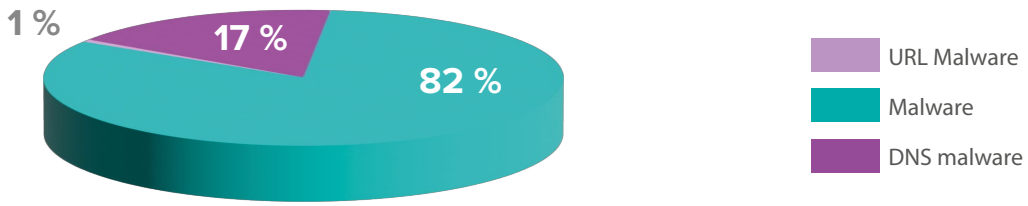
V první části analýzy se nejprve podíváme na phishing. IPS sondy detekovaly incident vždy, když se uživatel pokusil navštívit blokované phishingové stránky. Největší počet incidentů z minulého roku byl detekován v prosinci v množství 41774 incidentů, což je 47x násobné zvýšení oproti předchozímu roku za stejný měsíc. Ke konci roku 2022, obdobně jako v minulých letech došlo k postupnému nárustu phishingových útoků souvisejících s vyšší aktivitou uživatelů na internetu. V posledním kvartálu roku 2022 byli útočníci nejaktivnější v prosinci, kdy provedli více jak 41 tisíc phishingových útoků. Ve třetím kvartálu bylo nejvíce phishingových útoků detekováno v měsíci srpnu, kdy bylo provedeno přes 9 tisíc útoků.





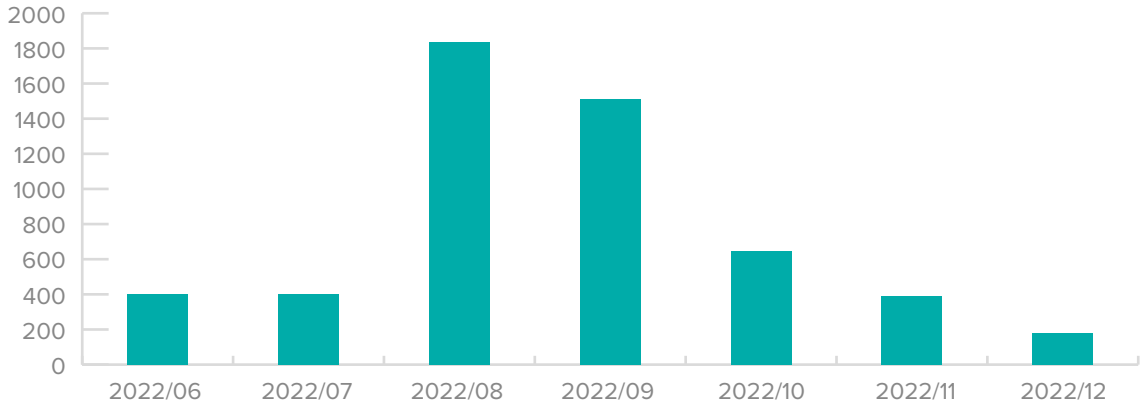
Za poslední dva kvartály roku 2022 bylo největší množství incidentů spojených s malwarem zachyceno IPS systémy v měsíci prosinci, šlo o bezmála 24 tisíc událostí. Jedná se o 73% pokles oproti předchozímu roku za totožné období. Vyšší četnost těchto útoků je dána vyšší uživatelskou aktivitou na internetu spojenou s koncem roku, k obdobnému počtu detekovaných incidentů v tomto období dochází pravidelně, jak ukazují mimo jiné i data z předešlých let. Ve třetím kvartálu bylo nejvíce incidentů spojených s malwarem detekováno v měsíci září, kdy bylo detekováno přes 17 tisíc útoků.

MALWARE STRUKTURA



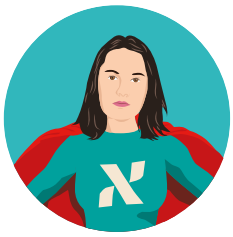
Detekce spojené se škodlivým kódem člení sledované IPS systémy do tří základních kategorií. V kategorii malware se nacházejí události, při kterých byla identifikována shoda s reputační databází IPS, která obsahuje IP adresy, na nichž se vyskytuje nebo vyskytoval malware. Porovnává se při tom jak zdrojová, tak i 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 2022 byla struktura detekcí malwaru následující: z 82 % byly detekce výskytu malwaru realizované pomocí reputační databáze, ze 17 % se jednalo o detekci využívající kontrolu DNS a ve zbylém 1 % byl malware odhalen prostřednictvím provedené 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 srpnu 2022 byl zachycen nejvyšší počet pokusů o těžbu kryptoměn o celkovém množství 1836 pokusů. Oproti předchozímu měsíci červenci se jednalo o 460 % nárůst. Druhým měsícem s nejvyšším množstvím pokusů o těžbu kryptoměn byl měsíc září, kdy bylo zablokováno 1509 pokusů, v následujících třech měsících došlo vždy k pozvolnému poklesu pokusů o těžbu kryptoměn, obdobně jako v minulém roce.

Dopad využití služby IP reputační databáze na provoz



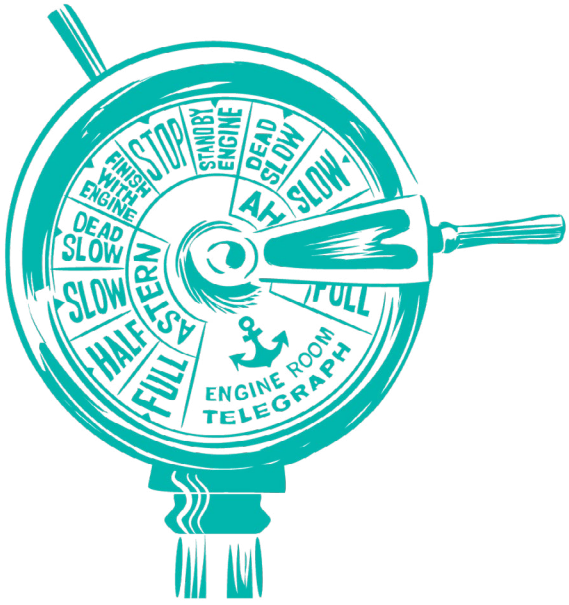
Oleksandra Kocyba

IP reputační databáze je služba poskytující informace o reputaci IP adres, umožňující organizacím a poskytovatelům služeb zvýšit úroveň ochrany svých aplikací a zamezit případným webovým útokům, nechtěné emailové komunikaci a dalším hrozbám. Tyto databáze sbírají a analyzují celou řadu parametrů, na základě kterých poté vyhodnocují reputaci IP adres a přiřazují ji reputační skóre. Existuje celá řada faktorů, na základě kterých mohou být IP adresy hodnoceny, například pokud jsou spojeny s vysokým počtem spam stížností, byly zdrojem infekcí malwarem nebo jiným škodlivým softwarem, byly nebo jsou součástí botnetu, podílely se na webových útocích jako jsou například DDoS útoky či na základě historie provozu IP adresy. Na základě tohoto, mohou být v rámci databáze IP adresy dále kategorizovány, například BrightCloud používá následující kategorie: Spam Sources, Windows Exploits, Web Attacks, BotNets, Scanners, Denial of Service, Reputation, Phishing, Proxy, Mobile Threats and TOR Proxy.

Pro tuto část reportu, jsme na webovém aplikačním firewallu zprovoznili službu IP reputační databáze pro aplikace vystavěné do internetu. Dále jsme určili, které kategorie IP adres budou při detekci blokované, a které blokované nebudou, ale budou pouze zaznamenávané. Toto rozhodnutí jsme provedli zejména z důvodu zamezení co nejvyššímu počtu případných falešných pozitiv. Blokovali jsme následující kategorie: Mobile Threats, Phishing, Denial of Service, Scanners, BotNets, Web Attacks, Windows Exploits. Kategorie Tor Proxies, Proxy, Reputation a Spam Sources byly poté pouze monitorovány.

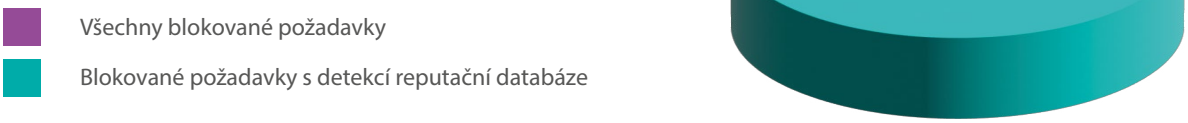
Pro podrobnější analýzu dopadu využití služby IP reputační databáze na provoz a počet ilegálních a blokovaných požadavků jsme se zaměřili na jeden vzorový týden, ze kterého jsou zpracované následující výstupy. Pro lepší orientaci v následujícím textu si ještě definujeme používané výrazy: ilegální a blokovaný požadavek. Ilegální požadavek, je takový požadavek, který je z pohledu webového aplikačního firewallu považovaný za potenciálně škodlivý, ovšem není blokovaný, je pouze zaznamenán. Blokovaný požadavek, je pak ten, který porušuje pravidla bezpečnostní politiky a je následně i zablokovaný, tedy neprojde k cílové aplikaci.

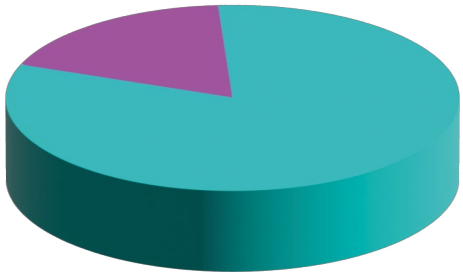
V rámci testovacího týdne se počet ilegálních požadavků na testovanou aplikaci pohyboval přibližně na hodnotě 101 000 a počet blokovaných požadavků na hodnotě 1300. Z celkového počtů ilegálních požadavků technologie IP reputační databáze označila 24 124 záznamů v rámci některé z kategorií vybraných pro záznam. Celkem potom IP reputační databáze označila 1 065 záznamů z blokovaných požadavků v rámci některé z kategorií vybraných pro blokování. Tedy 23.3 % všech ilegálních požadavků bylo kategorizováno pomocí pravidel bezpečnostní politiky, pomocí IP reputační databáze nebo kombinací obojího. V případě blokovaných požadavků se jednalo o 81.8 % ze všech zablokovaných požadavků.



Podíl požadavků detekovaných reputační databází na ilegálních požadavcích

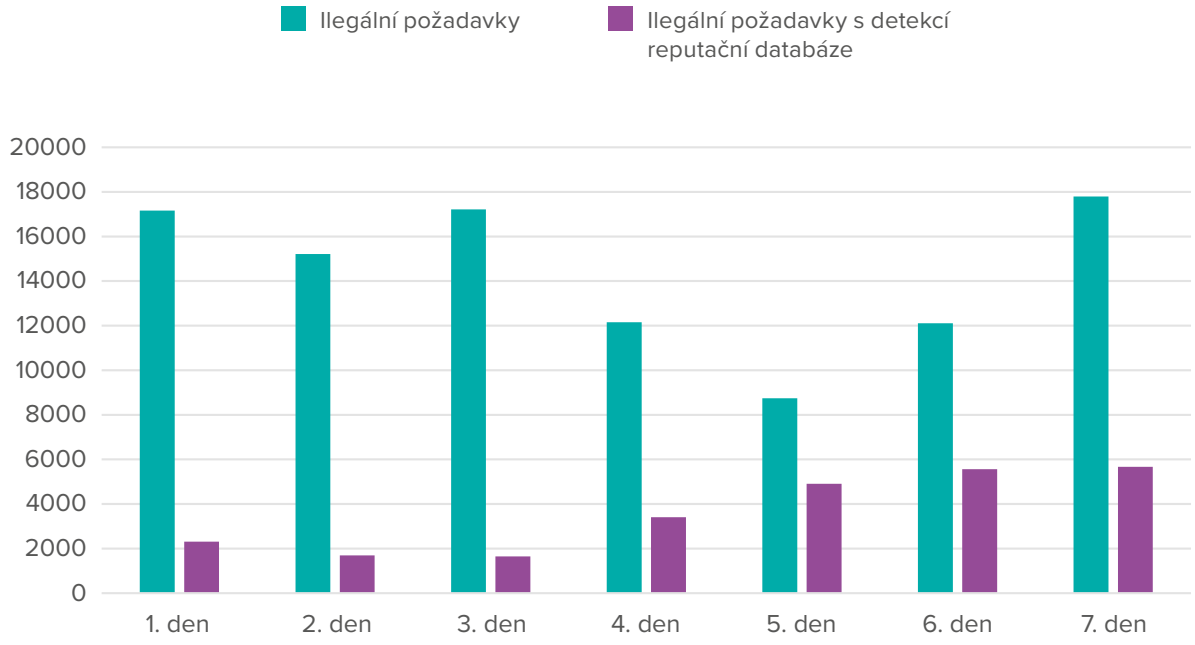
Podíl požadavků detekovaných reputační databází na blokovaných požadavcích



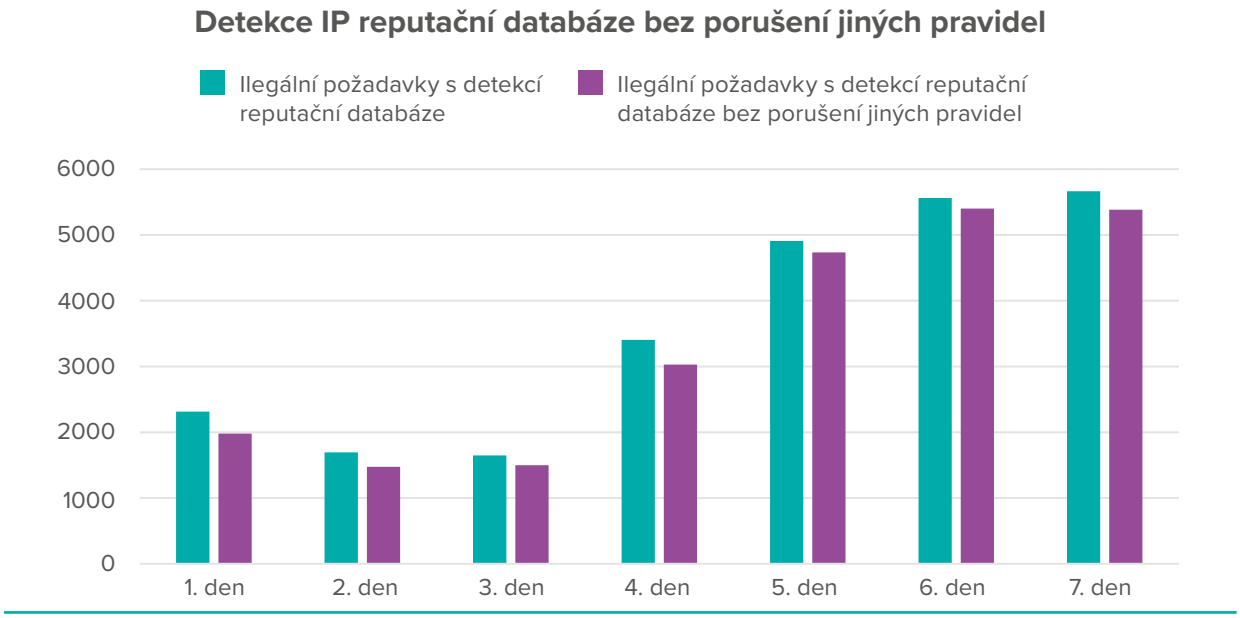


Z analýzy průměrných hodnot v rámci jednotlivých dní vychází podobné hodnoty. V průměru se za 24 hodin detekuje přibližně 14 600 ilegálních požadavků, z nichž téměř čtvrtina je kategorizována pomocí IP reputační databáze. Denně se jedná o hodnoty pohybující se v rozmezí 11 % až 50 % ze všech ilegálních požadavků.

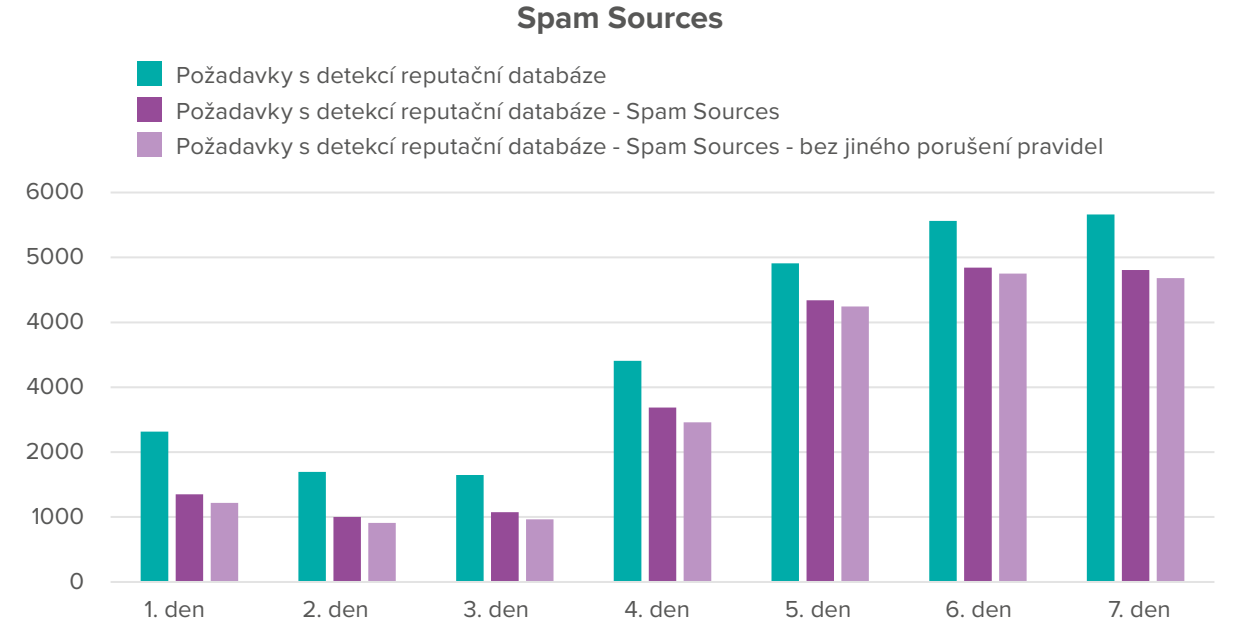
Podíl detekcí IP reputační databáze na ilegálních požadavcích



Významné je i procento, které bylo detekováno pouze pomocí služby IP reputační databáze. Jde o požadavky, které by žádné jiné pravidlo bezpečnostní politiky nezachytilo, a bez detekce pomocí služby IP reputační databáze by se jednalo o legitimní požadavek. Jde o průměrně 3 360 požadavků za den, tedy 22.9 % všech ilegálních a blokovaných požadavků.



Nejčastěji detekované kategorie v rámci testování byly Spam Sources, Scanners, Windows Exploits a Phishing. Mezi nimi dominuje kategorie Spam Sources, která tvoří největší procento detekcí. Denně se jednalo o 58 % až 88 % veškerých záchytů služby IP reputační databáze a značné procento, v průměru až 70 % byly požadavky, které byly detekovány pouze pomocí dané služby a neporušily by žádné pravidlo v bezpečnostní politice.



Druhou nejčastěji detekovanou kategorií byly Scanners, kde se jednalo o 20 % až 38 % z ilegálních požadavků, z nichž přibližně jedna pětina byly požadavky detekované pouze pomocí služby IP reputační databáze. V menší míře se poté vyskytovaly kategorie jako Botnets a Proxy.

Z výsledků reportu je patrné, že nezanedbatelné procento provozu je detekováno pouze pomocí služby IP reputační databáze, a to až pětina, a zároveň také velké procento provozu je detekované kromě pravidel bezpečnostní politiky i díky reputační databázi. Ta tak tvoří velmi užitečný nástroj nejen pro doplnění bezpečnostních ochran v organizacích ale i pro zlepšení celkové úrovně zabezpečení a „záplatování možných mezer“.

Události a trendy roku 2022

Stanislav Novotný

V roce 2022 jsme mohli být svědky nespočtu významných úniků dat, cílených útoků na kritickou infrastrukturu, závažných zranitelností či enormně velkých DDoS útoků. Útočníci navíc neustále vyvíjejí nové techniky a taktiky k provádění útoků a zcizení dat. Z toho důvodu je důležité o nich být obeznámen a být tak před útočníky o krok napřed.

Proto Vám v rámci našeho reportu přinášíme přehled o hlavních událostech roku 2022, jejich dopadu a opatřeních přijatých k jejich zmírnění. Cílem této části reportu je tak poskytnout vhled do současného stavu kybernetické bezpečnosti ve světě a pomoci Vám učinit informovaná rozhodnutí o strategii v rámci kybernetické bezpečnosti ve Vaší organizaci.

Leden

Na začátku ledna bylo stále dominantní událostí dění okolo **Log4Shell** – zranitelnosti v komponentě Log4j, která v rámci Java aplikací umožňuje provádět komplexním způsobem logovací úkony. V lednu už byla tato zranitelnost několikrát zazáplatovaná – naneštěstí se v každé nové záplatě vždy objevila zranitelnost nová, a tak pokračovalo hledání záplaty, která by byla bezproblémová.

Ruská FSB v lednu oznámila, že se jí podařilo zatknout 14 členů skupiny za ransomwarem **REvil**. USA údajně poskytly Rusku o těchto osobách informace potřebné k jejich zatčení.

Ten samý týden, co Rusko publikovalo tuto informaci, byl změněn vzhled 15 webových stránek patřících ukrajinské vládě. Ty tak po nějakou dobu zobrazovaly pouze proti-ukrajinský text. Většina odborné komunity se klonila k názoru, že za tímto útokem stojí ruský útočný aktér. Podle Ukrajinského ministra mělo jít spíše o krycí aktivitu, která měla za úkol pouze odvést pozornost od závažnějších operací v kyberprostoru směrem proti Ukrajině.

Tou závažnější událostí byl malware, který mířil na Ukrajinské organizace a na který upozornil Microsoft Threat Inteligence Center. Šlo o **wiper**, destruktivní typ malwaru. Microsoftu se nepodařilo v té době identifikovat vazby na žádnou škodlivou skupinu, ale tento útok značně připomínal dřívější útok prováděný pomocí malwaru NotPetya, a tak bezpečnostní komunita prakticky jednohlasně připsala tento malware Rusku. Situace mezi Ruskem a Ukrajinou se tak značně vyostřovala i v kyberprostoru.

Únor

V únoru proběhly **Olympijské hry** v Pekingu a ty tak přilákaly pozornost i kybernetických zločinců. Česká televize se prakticky od jejich začátku potýkala s DDoS útoky, které znemožňovaly sledovat webové vysílání.

Situace mezi Ruskem a Ukrajinou se dále vyostřovala. Stránky Ukrajinských ministerstev byly vystavovány masivním DDoS útokům. Ukrajinští občané také dostávali zprávy, které měly za úkol šířit paniku. Například falešná oznámení o tom, že z bankomatů nejdou vybírat peníze. DDoS útoky na bankovní portály znemožňovaly lidem také připojení k internetovému bankovnictví. Ukrajina uvedla, že země je už delší dobu terčem masivní hybridní války, jejímž cílem je vyvolat v lidech úzkost a podkopat důvěru Ukrajinců v obranu Ukrajiny. USA, Velká Británie a další státy připsaly útoky ruské rozvědce GRU. Ruská vláda kategoricky odmítla všechna tato, podle ní, lživá obvinění – nikdy prý neprováděla a neprovádí žádné záškodnické operace v kyberprostoru. Kromě toho Ukrajině dělal starosti již zmíněný wiper, který byl kryptograficky podepsaný legitimním vývojářským certifikátem, a tak se mu dařilo efektivně obcházet antivirové nástroje.

24. února ve 4 hodiny ráno Rusko zaútočilo na Ukrajinu. Vláda po začátku invaze vyzvala IT komunitu, aby nabídla své odborné znalosti a schopnosti a vytvořila tak, jak to sama nazvala, **IT armádu** odborníků. Tuto armádu pak rozdělila na dvě skupiny,

jedna měla na starost obranu a fortifikaci hlavně kritické infrastruktury, ta druhá naopak protiútoky. V Telegram skupině, která čítala okolo 200 tisíc členů, se lidé organizovali k DDoS útokům na Ruské cíle.

Různé skupiny za různými druhy ransomwarů se přikláněly na jednu, nebo druhou stranu. Skupina **Conti** jako jedna z mála vyjádřila podporu Rusku, což následně vedlo k leaku jejích interních chat logů a zdrojových kódů.

CZ.NIC zablokoval v Česku weby šířící dezinformace o této invazi a NÚKIB vydal varování před útoky z Ruska a urgoval k aktualizaci všech kritických systémů.

Skupina **Lapsus** v únoru napadla a úspěšně exfiltrovala data od společnosti NVIDIA, které po údajné hack-back operaci skupina LAPSUS následně kompletně vypustila online.

Březen
Rusko začalo velmi silně cenzurovat zahraniční stránky. Úřad **Roskomnadzor** zablokoval v Rusku Facebook, Twitter a spoustu dalších zahraničních portálů s novinkami. Rusko si také vytvořilo vlastní certifikační autoritu.

V kyberprostoru dále bouřil konflikt mezi Ruskem a Ukrajinou. Na obou stranách probíhaly DDoS útoky nebo dezinformační kampaně. Žádné větší škody ale Ukrajina v kyberprostoru nezaznamenala.

Skupina Lapsus získala a zveřejnila 190Gb dat společnosti Samsung, včetně jejich zdrojových kódů. Napaden touto skupinou byl také Vodafone, Ubisoft, Microsoft a dřívější průnik do své sítě skupinou Lapsus oznámila také Okta. Tyto úspěchy přivedly skupinu Lapsus do hledáčku vyšetřovacích orgánů. Spekulovat se začalo o věku leadra skupiny Lapsus, kterému mělo být údajně pouhých 16 let a pocházel z Anglie. Londýnská policie následně oznámila, že zatkla 7 osob ve věku 16-21 let za jejich údajné napojení na skupinu Lapsus. Lapsus pak oznámil, že si na nějakou dobu bere dovolenou.

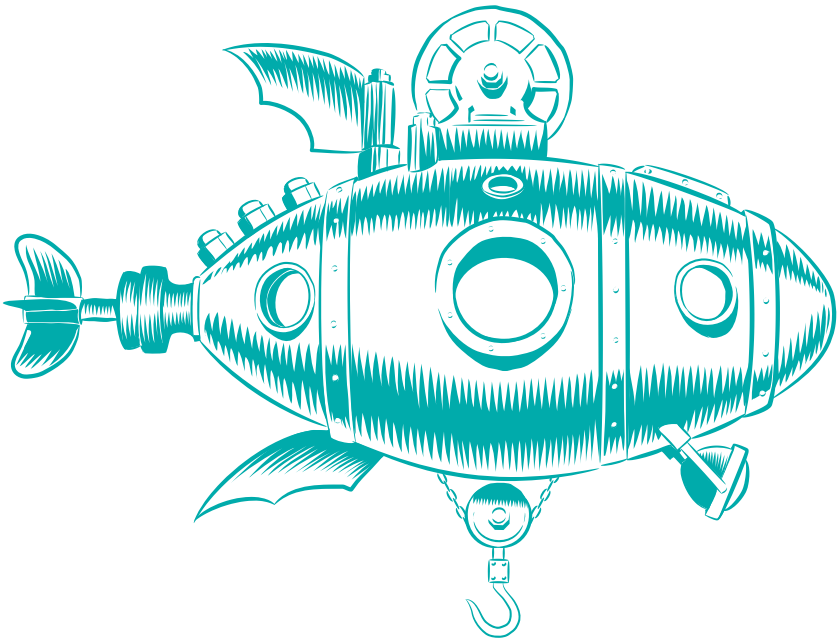
V březnu také čelil Úřad Prahy 5 kybernetickému útoku, který vyřadil jeho systémy a různé služby na několik dní.

Duben
Na začátku dubna byla zveřejněna zranitelnost v Javě při použití frameworku Spring, která dostala jméno **Spring4Shell**. Podobnost se zranitelností Log4shell byla z velké část ale pouze ve jméně. I když byla Spring4Shell závažnou Remote Code Execution zranitelností, bylo pro zneužití této zranitelnosti potřeba, aby server oběti běžel v nestandardní konfiguraci. Spring a Log4j používají navíc řádově odlišné počty potenciálně zranitelných systémů. Jednalo se tedy o kritickou zranitelnost, neměla ale potenciál zasáhnout stejné množství systémů jako Log4Shell. Naopak zranitelnost Log4Shell stále trápila organizace, a i do internetu bylo v dubnu viditelných spoustu systémů, které byly zranitelné. Ukrajina a Rusko na sebe v dubnu stále útočily pomocí DDoS útoků. Od začátku invaze bylo také identifikováno asi 5 různých druhů wiperů, které byly použity při útocích na Ukrajinské instituce. Ruští útočníci se také pokoušeli pomocí nové verze malwaru Industroyer neúspěšně útočit na Ukrajinskou energetiku.

Proruská skupina Killnet prováděla v dubnu ve větší míře DDoS útoky na České státní i soukromé instituce. Jednalo se třeba o stránky Komerční banky, úřadu vlády, fakulty informatiky ČVUT v Praze nebo Českých Drah. Po určitou dobu tak byly nedostupné vybrané systémy. To bylo třeba v případě Českých Drah nepříjemné, žádné vážnější následky tyto útoky ale neměly.

Skupina Lapsus se vrátila na scénu a mezi její další oběti se přihlásil T-Mobile. Ze 7 zatčených osob se napojení na skupinu Lapsus potvrdilo pouze u jednoho.

Květen
V neděli 8. května musel nově zvolený Kostarický prezident Chaves vyhlásit **nouzový stav** a jako důvod uvedl pokračující útoky skupiny za ransomwarem Conti. Útoky a jejich následky nakonec trvaly několik měsíců a Kostarická vláda je časem prohlásila za válečné a teroristické činy. V mnoha případech byly rozličné systémy vyřazeny z provozu úplně a související náklady byly odhadovány na 30 milionů dolarů za každý den trvání útoků. Země musela nakonec požádat o pomoc společnost Microsoft, USA a další země, aby jí pomohly krizi zvládnout.



Skupině Conti se tak dostalo nejspíše více pozornosti, než by tato skupina chtěla. Tak udělala to, co už skupina nějakou dobu plánovala, Její členové se rozdělili do menších, ale stále centrálně řízených skupin, které měly stylem poradenství poskytovat svou expertízu v menších ransomware skupinách. Útoky pod hlavičkou Conti už ale provádět neplánovali.
17. 5. se Ředitelství silnic a dálnic stalo terčem ransomware útoku. Ředitel ŘSD oznámil, že se z útoku budou vzpamatovávat několik měsíců a dohledání záloh bude obtížné.

Došlo také k reaktivaci části staré infrastruktury za ransomwarem REvil a modifikované kódy tohoto ransomwaru se začaly objevovat na internetu. Probíhaly nové útoky pod hlavičkou REvil, ale v tu chvíli nešlo s jistotou říci, zda za nimi stojí staří členové této skupiny, nebo jejich staří partneři, či zda byli členové této skupiny, kteří byli zatčeni v lednu, propuštěni.

Byla objevena zero-day zranitelnost Folina, umožňující RCE v produktech Microsoft Office. Mechanismus, který Folina zneužívala, už popsal ve své bakalářské práci v roce 2020 student z univerzity v Německu. Zranitelnost Folina byla následně Microsoftem záplatována.

Červen
Společnost Cloudflare úspěšně čelila DDoS útoku o síle **26 milionu požadavků za sekundu**. Byl to do té doby největší zaznamenaný HTTPS DDoS útok. Botnet, který za tímto útokem stál, byl pojmenován Mantis. Jednalo se totiž o botnet, který pomocí nevelkého počtu unesených zařízení s relativně vysokou výpočetní technikou dokázal vygenerovat tak velké množství požadavků.

Rusko a Čína se ostře ohradili proti vyjádření šéfa kybernetického velení USA o provádění ofensivních akcí v kyberprostoru proti Rusku.

Proběhlo cvičení od společnosti Enisa – CyberEurope 2022. V rámci něho si různé týmy v rozličných státech v Evropě vyzkoušely obranu proti útokům na nemocniční zařízení.

Litva čelila silným DDoS útokům, protože tamní vláda v rámci sankcí EU směrem k Rusku zavedla omezenou blokádu přepravy zboží mezi Ruskem a Kaliningradskou exklávou.

CISA v červnu varuje před stále probíhajícím zneužíváním zranitelnosti Log4Shell.

Červenec
V červenci se oficiálně potvrdilo, že ŘSD napadl ransomware, který měl podle jeho ředitele vyřadit z provozu okolo 1000 serverů. ŘSD se podařilo většinu systémů obnovit.

Prohlubuje se napětí mezi USA a Čínou co se týče technologií. Tentokrát FBI varovala, že zařízení Huawei, která se nacházejí v blízkosti amerických vojenských zařízení, představují velké znepokojení.

Srpen
1. 8. oslavil NÚKIB 5. narozeniny.

Zákazník služby Google Cloud Armor byl zasažen HTTPS DDoS útokem o výši **46 milionů požadavků za sekundu**, což z něj učinilo největší zaznamenaný HTTPS DDoS útok v historii, který byl o téměř 80 % větší, než jeho předchůdce.

Černá Hora čelila velkým kybernetickým útokům na svou infrastrukturu. Primárním cílem byly státní organizace. Dopady tohoto útoku pocítily hlavně dopravní služby a rozvody vody a elektřiny. Útok Černá Hora připsala Rusku.

Pieter Zatko, bývalý ředitel bezpečnosti Twitteru, podal podklad k prošetření fungování Twitteru americkému SEC. V Twitteru podle něj při jeho příchodu do funkce neexistovalo žádné řízení přístupu, platforma podle něj není robustní technicky ani lidsky. Twitter navíc podle něj nedostál svým dřívějším závazkům stran ochrany osobních údajů. Spekuluje se o nákupu Twitteru Elonem Muskem.

Září

Albánie na začátku září oznámila, že přerušila veškeré diplomatické styky s Íránem, z důvodu kybernetických útoků na její infrastrukturu. Jednalo se tak o vůbec první takto tvrdou reakci na kybernetický útok.

Bývalý CSO Uberu, Joe Sullivan, byl shledán vinným a odsouzen za spáchání trestného činu pokusu o utajení kybernetického útoku na společnost Uber v roce 2016.

Skupina Lapsus se vrátila zpátky na scénu. Údajný 17letý útočník se dostal v polovině září do sítě společnosti Uber a tam se dlouhou dobu volně pohyboval a stahoval data.

V druhé polovině září se také začaly šířit po internetu videa z připravované hry GTA 6. Útočník oznámil, že se mu podařilo dostat do sítě společnosti Rockstar a ukrást zdrojové kódy jak hry GTA 6, tak hry GTA 5. Údajně se mělo jednat o stejného útočníka, který stál za problémy Uberu.

Microsoft v září potvrdil dvě zero-day zranitelnosti v Microsoft Exchange on premise. Exploit těchto dvou zranitelností dostal název ProxyNotShell. Microsoft vydal několikrát upravovaný postup pro mitigaci, protože se komunitě několikrát tento navržený postup podařilo obejít.

Říjen

Chybná konfigurace serveru Azure Blob Storage umožnila neověřený přístup k některým datům zákazníků a partnerů společnosti Microsoft. Společnost SocRadar, která tuhle miskonfiguraci identifikovala, ho nazvala BlueBleed.

Dva kyberzločinci byli v USA odsouzeni. Jeden k 20 letům a druhý k 25 letům vězení za kybernetické útoky, respektive za scamování obětí. Soud v USA se těmito velkými tresty tak nejspíše snažil odstrašit další potenciální zločince.

Globální kryptoměnová burza Binance také v říjnu utrpěla kybernetický útok, při kterém útočníci ukradli její vlastní token BNB v hodnotě 570 milionů dolarů. Zločinci zneužili zranitelnost na cross-chain coin bridge v blockchainu BNB.

Listopad

Elon Musk se stal oficiálně majitelem Twitteru a okamžitě jeho novým CEO. Provedl spoustu změn, bohužel většina z nich nebyla domyšlená, a tak způsobila značné bezpečnostní problémy. Nový Twitter program - Twitter Blue, útočníci okamžitě využili k napodobování značek a osobností, a k promování různých kryptoscamů. Phishing se také spustil na ověřené uživatele Twitteru, které se útočníci snažili oklamat na základně zmatku s novým ověřováním uživatelů.

Austrálie měla velké problémy s kyberbezpečností a s ochranou dat svých občanů. Po ransomware útoku na soukromou pojišťovací společnost Medibank útočníci zcizili data všech jejich současných i minulých zákazníků. Po tom, co společnost Medibank odmítla zaplatit výkupné, začali útočníci vypouštět data jejich zákazníků na Dark Web. Australská vláda následně upravila legislativu. Subjektům v Austrálii tak hrozí mnohonásobně větší postihy a větší pravomoci dostal i vyšetřovací orgán.

USA zakázaly prodej telekomunikačních technologií od čínských společností. Některé státy v USA také zakázaly instalaci aplikace TikTok na vládních zařízeních.

Velká Británie v listopadu začala scanovat části svého internetu a hodlá aktivně hledat zranitelné systémy.

Prosinec
Radou Evropské unie byl přijat návrh směrnice NIS2, čímž byl zakončen celý schvalovací proces této směrnice na úrovni EU. Jednotlivým členským státům tak začala běžet lhůta 21 měsíců na transpozici nových požadavků do vlastních legislativních prostředí.

Neoprávněná osoba získala v prosinci přístup ke cloudové úložné službě třetí strany, kterou používala společnost LastPass k ukládání archivních záloh svých produkčních dat. Po získání přístupového klíče ke cloudovému úložišti a dešifrovacích klíčů ke kontejneru duálního úložiště zkopíroval útočník ze zálohy některé informace o zákaznických účtech.

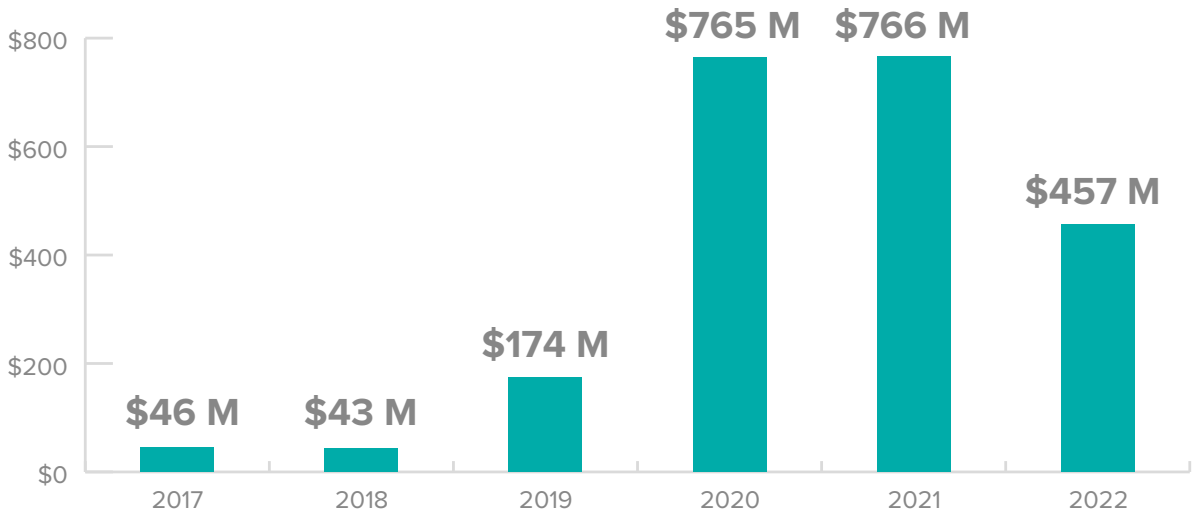
Trendy, které stojí za zmínku:

Meziroční pokles o přibližně 40 % v placení výkupného
V roce 2022 vylákaly ransomwarové skupiny od obětí přibližně 456,8 milionu dolarů, což představuje výrazný pokles, a to o přibližně 40 % oproti rekordním 765 milionům dolarů zaznamenaným v předchozích dvou letech.

Podle údajů společnosti Chainalysis není tento pokles zisků způsoben menším počtem útoků, ale spíše nárůstem počtu obětí, které odmítají útočníkům zaplatit.

Průměrná životnost ransomwaru klesla ze 153 dnů v roce 2021 na pouhých 70 dnů v roce 2022, a to navzdory vysoké aktivitě ransomwaru.

Total value received by ransomware attackers, 2017–2022
Ransomware profits per year (Chainalysis)



Společnost Coveware identifikovala od roku 2019 také trend klesající míry placení výkupného. 59 % obětí se v roce 2022 rozhodlo výkupné nezaplatit.

Ransomware payment percentage (Coveware)

	2019	2020	2021	2022
Paid	76 %	70 %	50 %	41 %
Did Not Pay	24 %	30 %	50 %	59 %

Profesionalizace Ransomware skupin
Zpráva společnosti Check Point z března roku 2022 odhalila vnitřní fungování skupiny za Conti ransomware. Tyto úniky ukázaly, že Conti, aktivní skupina hlavně v první polovině roku 2022, řešila své záležitosti pomocí známých firemních prvků, včetně procesu přijímání zaměstnanců, platů a bonusů.

Tento přístup, podobný fungování korporací, ukazuje, že ransomware se stal profesionálním, týmově koordinovaným podnikáním.

„Tyto skupiny si prošly svou „start-up“ kulturou a v roce 2022 byly ty větší a úspěšnější schopny začít škálovat a rozšiřovat své operace a učinit je tak trochu oficiálnějšími a robustnějšími,“ řekl Keegan Keplinger, vedoucí výzkumu a reportingu ve společnosti eSentire.

Kyberzločin se tak stal v roce 2022 mnohem organizovanějším. Vzestup zaznamenaly také služby jako Ransomware-as-a-service (RaaS). Skupiny jako LockBit, nebo Conti, využívají modely RaaS, které prodávají a inzerují na Dark Webu. Často také nabízejí podporu při vydírání, hostování stránek s leaky a služby cryptotransakcí.

Podle zprávy společnosti Trend Micro vzrostl počet skupin zabývajících se RaaS jen v prvním čtvrtletí roku 2022 o 63,2 %.

Rozvíjet se také začaly služby DDoS as a service.

Rozvoj umělé inteligence
Umělá inteligence zažila v roce 2022 velký skok v podobě nástroje ChatGPT. Je to chatbot vyvinutý společností OpenAI a spuštěný v listopadu 2022. ChatGPT je postaven na rodině velkých jazykových modelů GPT-3 společnosti OpenAI a byl vyladěn pomocí různých technik učení.

Tento nástroj tak může potenciálně představovat velkou pomoc kyberkriminálníkům. Od psaní phishingových zpráv po psaní kódu, i nesofistikovaný útočník může získat relativně sofistikovaný kód. Do budoucna se tento nástroj bude zlepšovat a představuje tak riziko výrazné pomoci útočníkům v různých odvětvích jejich činnosti.

Závěr
Závěrem lze říci, že zprávy minulého roku ze světa kybernetické bezpečnosti by měly sloužit jako varovný signál pro všechny firmy, aby braly zabezpečení svých dat vážně. Kybernetické hrozby jsou stále pokročilejší a sofistikovanější a důsledky narušení bezpečnosti mohou být drtivé, a to jak z hlediska finančních ztrát, tak poškození pověsti společnosti. Je důležité, aby organizace investovaly do svého zabezpečení a měly proaktivní přístup od správy zabezpečení svých dat ke školení svých zaměstnanců. Důsledky zanedbání kybernetické bezpečnosti jsou dnes zkrátka příliš velké na to, aby je bylo možné ignorovat.

Bezpečnostní dohled a stav Security Operations v roce 2022

Daniel Neumann

Problematice bezpečnostního dohledu jsme se rozhodli věnovat i ve stávajícím vydání Alef Security report 2023. Aktuálně získaná data tak máme možnost porovnat s předchozími ročníky a zjistit tak trendy v chování organizací v oblasti bezpečnostního dohledu.

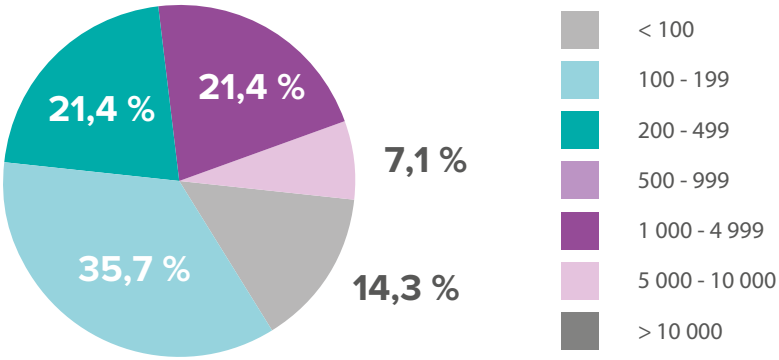
Pokrok v oblasti digitální transformace vedl k tomu, že i rok 2022 dal vzniknout novým hrozbám pro kybernetickou bezpečnost. V průběhu pandemie koronaviru se mnoho společností muselo flexibilně přizpůsobit novým podmínkám. Práce na dálku a vysoký podíl home–office otevřely nové přístupové body a možnosti pro kybernetické útoky. Další významnou hrozbou byla také válka na Ukrajině, která se odehrávala nejen na poli bitevním, ale i mediálním a v online prostoru.

Doprava, energetika, zdravotnictví, finance a další kritická odvětví jsou ve své hlavní činnosti stále více závislé na digitálních technologiích. Digitalizace sice nabízí obrovské příležitosti a přináší řešení množství výzev, kterým Evropa čelila nejen v průběhu krize COVID-19, ale zároveň vystavuje ekonomiku a společnost kybernetickým hrozbám. Kybernetické útoky a kyberkriminalita jsou nejen v Evropě, ale po celém světě, čím dál častější a sofistikovanější. Očekává se, že k internetu věcí bude v roce 2024 na celém světě připojeno přes 20 mld. zařízení, uvedený trend tak jistě bude pokračovat i v budoucnu. Firemní IT není často schopné projíždět detailně logy ze všech nástrojů, které v síti mají, provádět včas a pravidelně kontroly zranitelností, zajišťovat updaty, školit zaměstnance, a i pro sebe zajistit odpovídající úroveň znalostí nutných pro efektivní chod IT. Podstatným faktorem je též možnost zajištění odpovídající úrovně pracovníků IT, kterých je na trhu nedostatek. V takovém případě může být pověstným vytržením trnu z paty externí podpora IT ve formě služby, jakou může být například bezpečnostní dohled, chcete-li Security Operations Center. Stejně jako i v minulých letech jsme v rámci Security Reportu oslovili naše zákazníky a poprosili je o vyplnění několika otázek vztažených k tématu bezpečnostního dohledu. Tímto bychom jim rádi poděkovali za jejich čas a sdělené informace, které budou využity pro potřeby tohoto článku.

Velikost organizace představuje podstatný faktor, který se promítá do velikosti IT oddělení a nákladů do zajištění lidských zdrojů. Zároveň ovlivňuje skutečnost, jak k otázce bezpečnosti přistupovat. Bezpečnostní dohled není výjimkou. Existují organizace důvěřující svým zaměstnancům a spoléhající na jejich opatrnost. Tento přístup s sebou ovšem nese jistou míru rizika a mnohdy se nevyplácí. V každém případě je nutné zajistit zaměstnancům dostatečnou informovanost a umožnit pravidelná bezpečnostní školení, jejichž cílem je povýšení bezpečnostního povědomí napříč organizací. Druhou možností je zřízení vlastního IT oddělení. Podle jeho velikosti a počtu interních IT specialistů se odvíjí schopnost komplexně obsáhnout problematiku kybernetické bezpečnosti. V případě malého oddělení bude bezpečnost na adekvátní úrovni zajištěna jen velice obtížně. Větší oddělení ovšem znamená významnou finanční zátěž. Organizace tak stojí před volbou – omezená bezpečnost nebo vysoké provozní náklady.

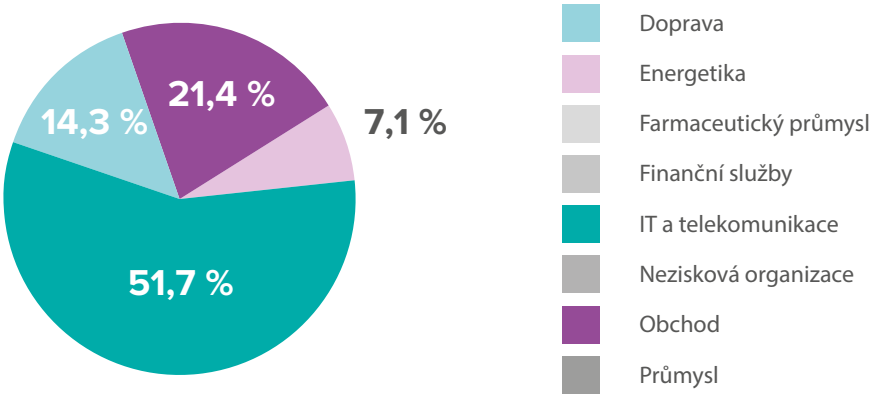
Nyní se již přesuňme k samotnému reportu. Na níže uvedeném grafu lze vidět, že jsou v rámci našeho dotazníkového šetření zastoupeny jak organizace o několika stovkách zaměstnanců, tak i ty, jejichž počet přesahuje 5 000. Většinové zastoupení na úrovni téměř tří čtvrtin představují organizace do 500 zaměstnanců.

Kolik zaměstnanců má Vaše organizace?



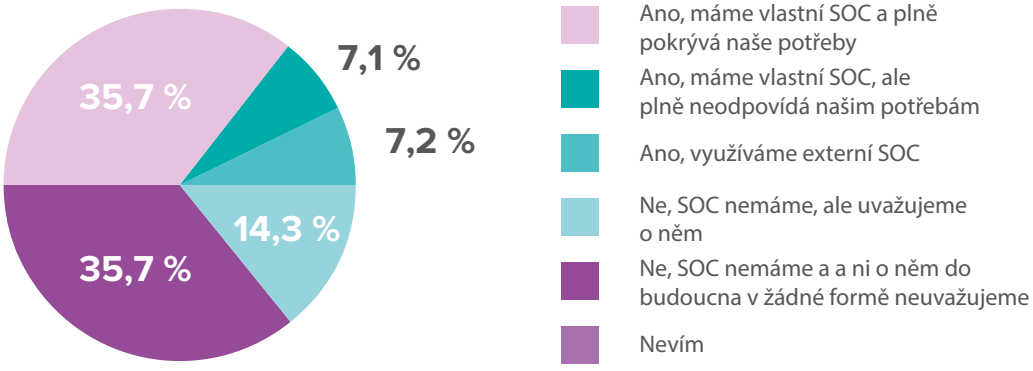
Z hlediska oborového zastoupení mezi tazateli nejvíce figurovali zástupci z IT a telekomunikací (lehce přes polovinu).

V jakém sektoru Vaše organizace působí?



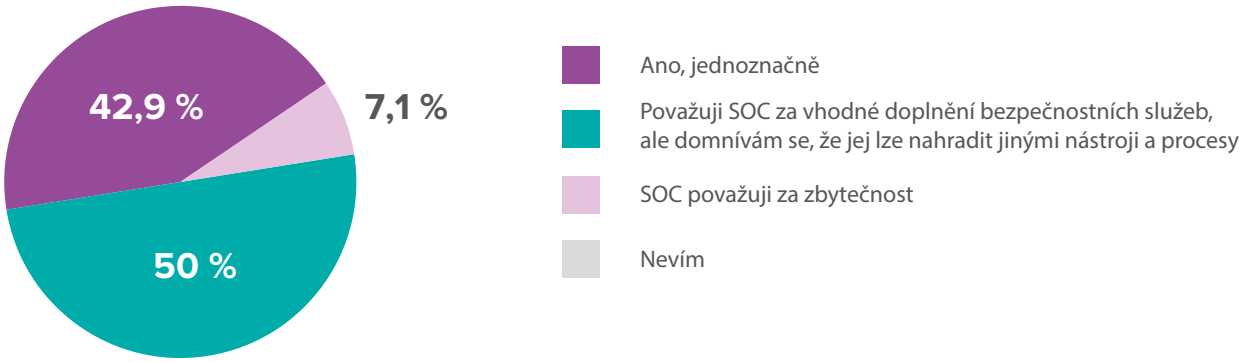
V samotném úvodu šetření nás zajímalo, kolik procent z dotázaných využívá služeb SOC. Zhruba třetina zákazníků má vlastní SOC, který plně pokrývá jejich potřeby. Stejný podíl naopak SOC nemá a ani o něm do budoucna v žádné formě neuvažuje. Necelých 15 % SOC nemá, ale uvažuje o něm. Oproti výsledkům reportu z minulého roku tak můžeme pozorovat nárůst podílu organizací s vlastním SOC o necelých 15%.

Využíváte služby SOC (Security Operations Center)?



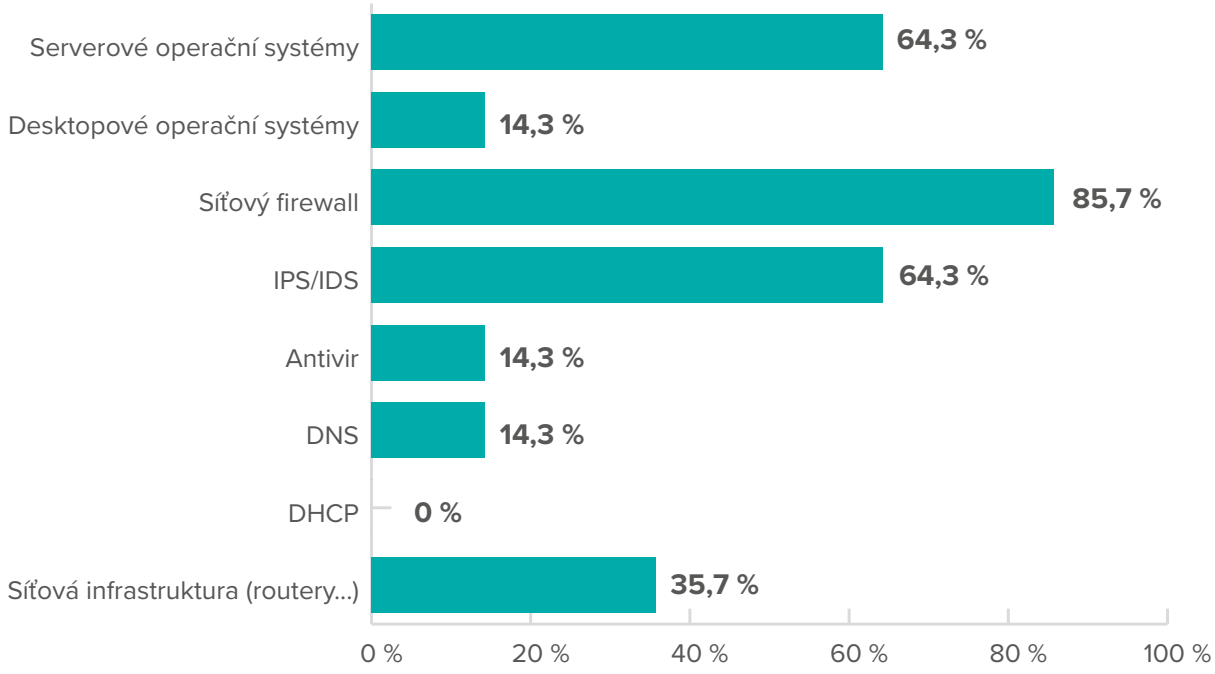
Považujete SOC za nutnost? Slabší polovina dotázaných odpověděla „ano, jednoznačně“. V porovnání s předchozím obdobím došlo k poklesu o zhruba 20%, a to na úkor tazatelů, kteří považují SOC za vhodné doplnění bezpečnostních služeb, ale domnívají se, že jej lze nahradit jinými nástroji a procesy.

Považujete SOC za nutnost?



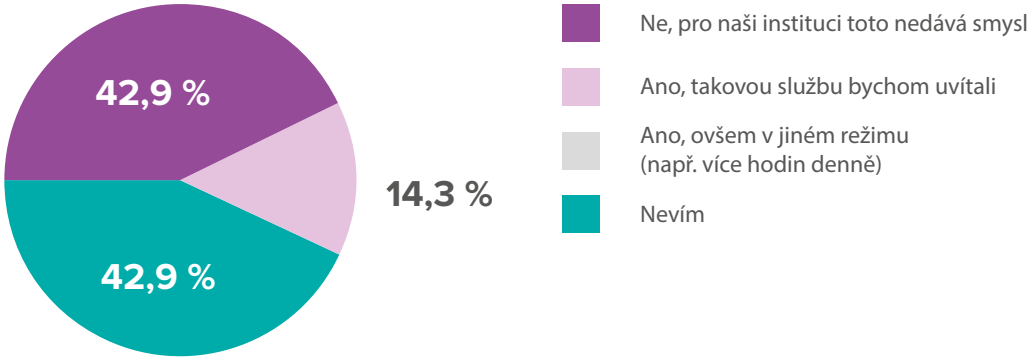
V rámci bezpečnostní analýzy hraje významnou roli zaznamenávání dat za účelem jejich analýzy (logování). Logy z jakých tří typů systémů považují oslovené organizace za nejvýznamnější? V pořadí dle důležitosti to byl síťový firewall, serverové operační systémy a IPS/IDS. Výsledky se od předchozích let v tomto případě prakticky nezměnily.

Logy z jakých tří typů systémů považujete za nejpodstatnější z pohledu použití v rámci bezpečnostní analýzy?



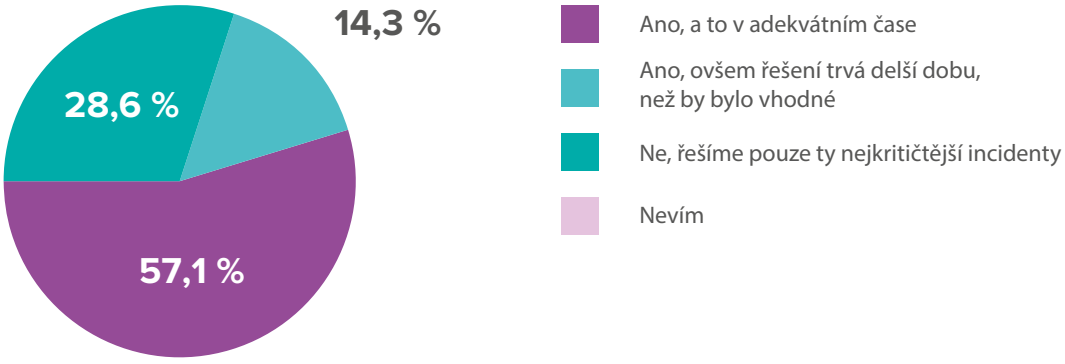
Bezpečnostní dohled bývá standardně v režimu 8×5 či 24×7. Tento rozsah služby je jistě velice efektivní a s vysokou pravděpodobností pomůže odhalit nekalé aktivity útočníků při samém počátku, představuje ovšem variantu, která je z důvodu časové vytíženosti značně nákladná a většina organizací si ji z tohoto důvodu nemůže dovolit. Existují samozřejmě i případy, kdy okamžitá reakce není potřeba, neboť organizace nespadá do kategorie kriticky významných a řešení incidentů snese určitý časový odklad. Pro tyto případy by dávalo smysl využít omezenou formu bezpečnostního dohledu, kdy by se bezpečnostní specialista nedíval do zákazníkova prostředí v reálném čase, ale retrospektivně, několikrát denně. Kumulativní souhrn denního dohledu by tak činil např. 1 hodinu každý pracovní den. Pro 42,9 % oslovených tento typ dohledu nedává smysl. Stejný podíl si přínosem bezpečnostního dohledu v této podobě není jistý a 14,3 % organizací by jej uvítalo.

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



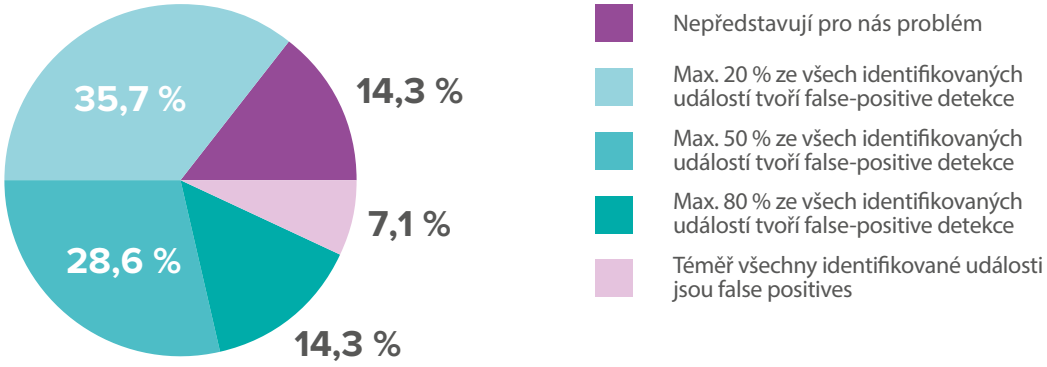
V dnešní době se každé IT oddělení potýká s řešením bezpečnostních incidentů. Jejich množství se odvíjí od mnoha faktorů – „atraktivnosti“ dotyčné organizace pro útočníky, bezpečnostních technologiích schopných tyto incidenty identifikovat a zkušenostech členů IT oddělení. Zvládají oslovené instituce řešit každý odhalený bezpečnostní incident? Více než polovina ano, a to v adekvátním čase. Jedná se tak o meziroční nárůst o více než 35 %. Silnější čtvrtina je schopná řešit pouze ty nejkritičtější incidenty a 14,3 % odpovědělo, že incidenty zvládá řešit, ale pomaleji, než by bylo vhodné.

Zvládáte řešit každý bezpečnostní incident?



Díky automatizovaným skenům sítě, IPS, SIEMu a dalším nástrojům získává IT data, se kterými následně pracuje. Ne vždy se ovšem jedná o data validní. V mnohých případech se může jednat o chybné detekce událostí, tzv. „false-positive“. Pokud se musí pracovníci IT zabývat vysokým počtem takovýchto detekcí, jedná se o plýtvání jejich drahocenným časem, resp. zdroji celé organizace. Jak to vypadá v praxi? Představují false-positive detekce problém, se kterým se často setkáváme? Získaná data ukazují, že pro cca sedminu organizací nepředstavují problém. Ve zhruba třetině případů tvoří maximálně 20 % všech identifikovaných událostí a v 28,6 % případů tvoří max 50 % ze všech identifikovaných událostí. Oproti předchozímu roku tak došlo u této kategorie k nárůstu o více jak 20 %.

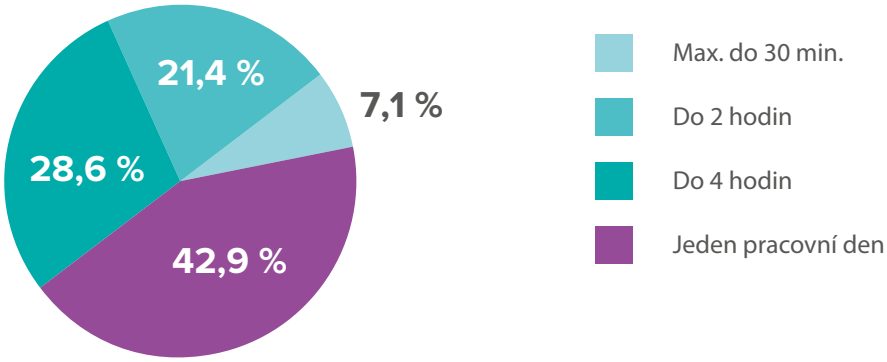
Jsou false-positive detekce problém, který Vás nadmíru zatěžuje? Pokud ano, kolik % z celkového počtu identifikovaných bezpečnostních událostí představují právě false-positives?



Kybernetické bezpečnostní incidenty bývají nepředvídatelné, vznikají a vyvíjejí se často ve velmi krátké době a zasažené subjekty i osoby odpovědné za reakci na incidenty a zmírnění jejich účinku musí proto reagovat velice rychle. Minimalizace reakční doby na incident je tak jednou z nejefektivnějších forem obrany vedoucí ke zmírnění dopadu incidentu.

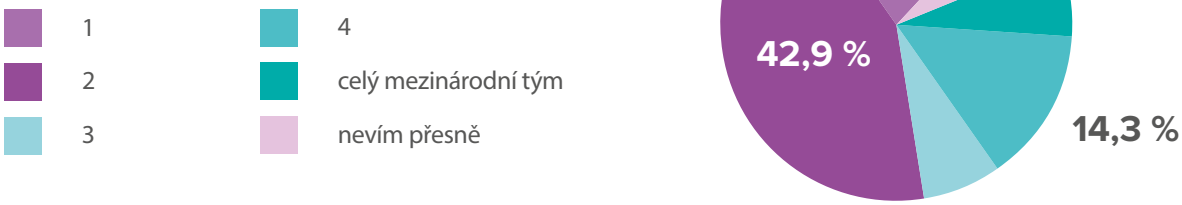
V rámci dotazníku nás zajímalo, jakou reakční dobu na nekritický bezpečnostní incident považují organizace za dostatečnou. Přibližně 30 % si myslí, že reakce do 4 hodin je dostatečná. Zhruba pětinové zastoupení měla skupina, pro níž jsou adekvátní dobou řešení 2 hodiny a 42,9 % respondentů se ztotožňuje s řešením během 1 pracovního dne.

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



Kolik lidí je v rámci organizace oficiálně zodpovědných za reakci na incidenty? Nejčastěji se jedná o 2 zodpovědné osoby (42,9 %). Velice často je to pouze 1 osoba (21,4 %).

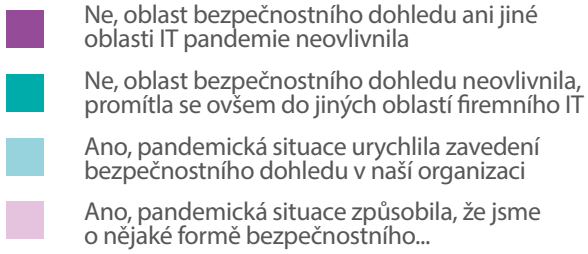
Kolik lidí v rámci Vaší organizace je oficiálně zodpovědných za reakci na incidenty?

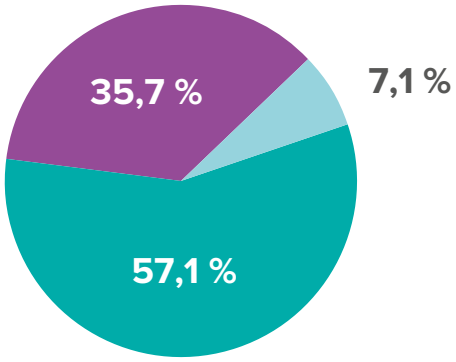


Několik předchozích let bylo ovlivněno pandemií COVID – 19. Zajímalo nás, zda pandemie nějakým způsobem ovlivnila oblast bezpečnostního dohledu. Zhruba 36 % respondentů odpovědělo, že pandemie oblast bezpečnostního dohledu neovlivnila žádným způsobem. U 7,1 % organizací pandemická situace urychlila zavedení bezpečnostního dohledu.

Zbytek dotázaných, tedy cca 57 %, nezaznamenal změnu v oblasti bezpečnostního dohledu, ale uznává, že se pandemie promítla do jiných oblastí firemního IT. Ani zde meziročně nelze hovořit o změně přístupu, neboť odpovědi z předchozího období byly téměř totožné.

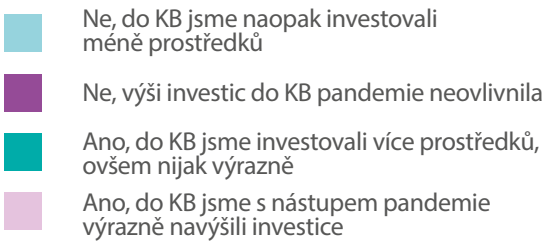
Ovlivnila pandemie týkající se COVID-19 nějakým způsobem oblast bezpečnostního dohledu ve Vaší organizaci?

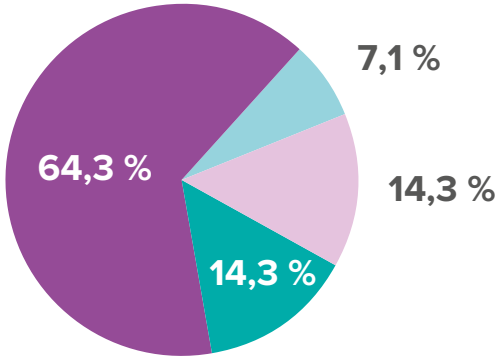




Závěr průzkumu věnujeme výši investic určených na zajištění kybernetické bezpečnosti v návaznosti na pandemickou situaci. Více jak 64 % účastníků průzkumu uvedlo, že výši investic do kybernetické bezpečnosti pandemie neovlivnila. V případě 14,3 % respondentů došlo k navýšení investic, ovšem nijak výraznému a stejný podíl dotázaných reagoval výrazným nárůstem investic do KB.

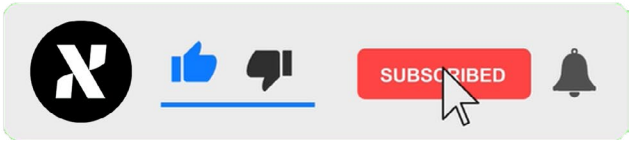
Změnila se s nástupem pandemie COVID-19 výše investic do oblasti kybernetické bezpečnosti (KB) ve Vaší organizaci?





Novinky, rozhovory, doporučení.

Sledujte náš kanál ALEF Security zaměřený na kybernetickou bezpečnost!



ALEF

Pro více informací kontaktujte cz-sales@alef.com