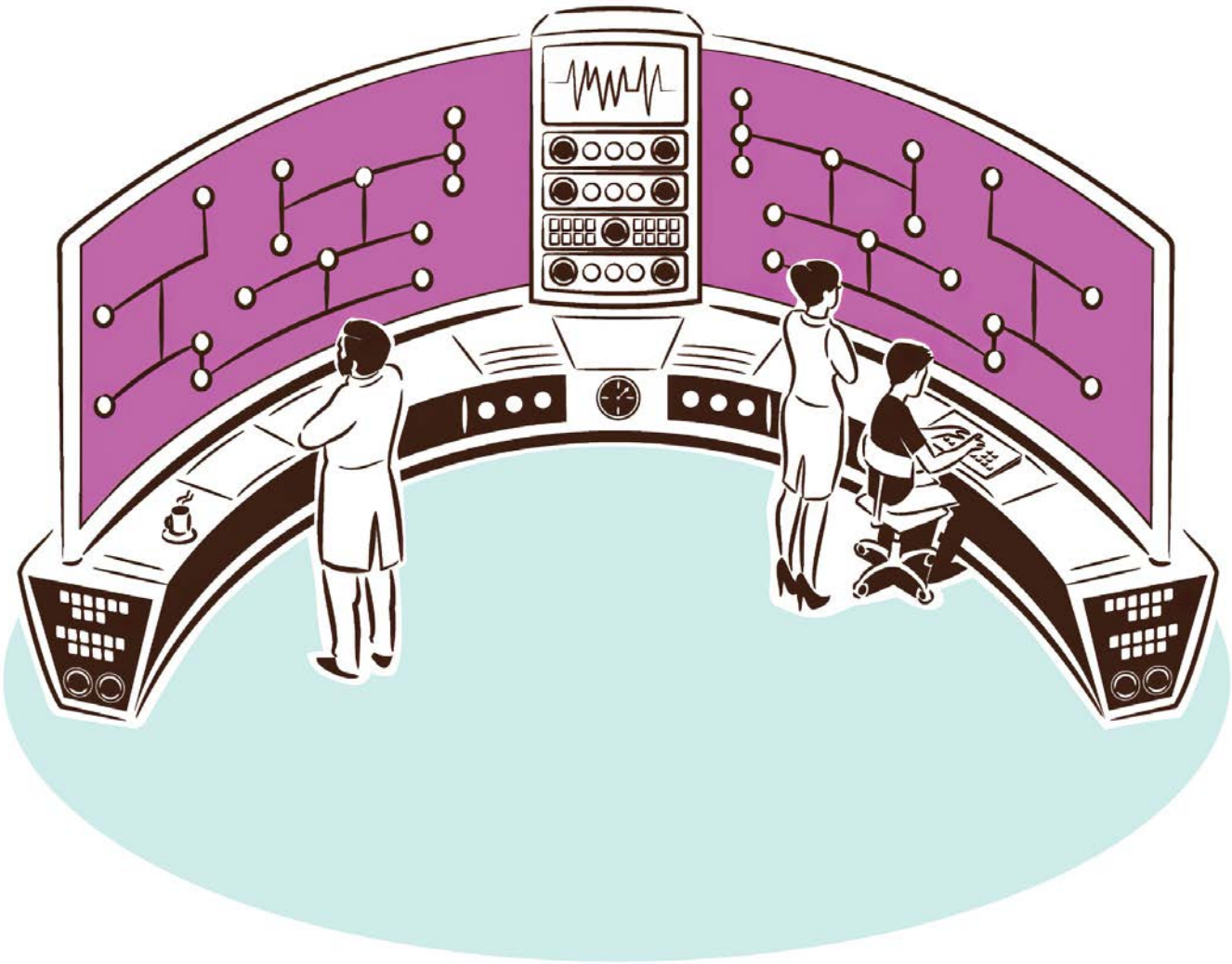
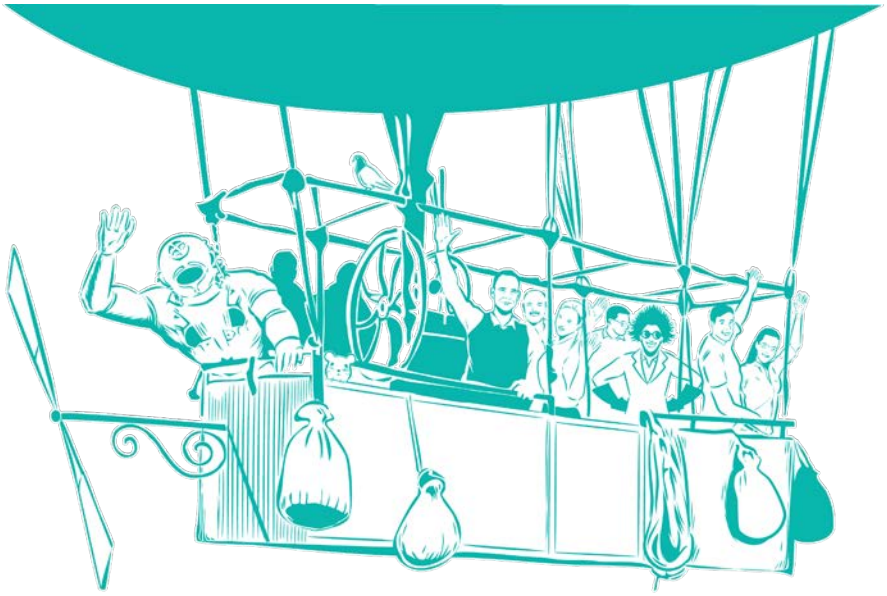
ALEF

Security Report 2022



Trust the Strong
www.alef.com

Obsah



Úvod

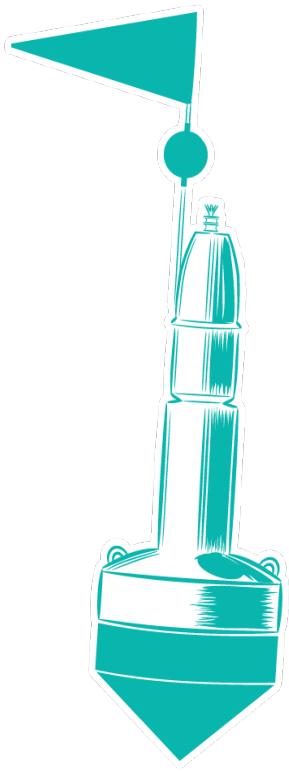
V posledních dvou letech jsme byli v souvislosti s pandemií COVID-19 svědky bezprecedentních změn v oblasti vývoje informačních a telekomunikačních technologií. To, co bylo dříve výsadou velkých společností, se stalo standardem pro fungování většiny organizací napříč všemi segmenty trhu. Virtuální meetingy, online konference, práce z domova, to vše s podporou cloudových služeb, se pod tlakem okolností stalo neodmyslitelnou součástí našich životů. Každá akce však vyvolává reakci, a aktuální trendy v komunikaci s sebou přinesly i nové a sofistikovanější aktivity útočníků. Udržet krok v rámci efektivní obrany není rozhodně jednoduchá disciplína, a je na každé instituci či jednotlivci, jak se tohoto nelehkého úkolu zhostí.

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.

Klíčovým 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 do následujících stránek, můžete se těšit mimo jiné na článek týkající se 0-day zranitelností ve světě Windows, příspěvek týkající se úrovně šifrování webserverů na českém internetu, aktuální trendy v oblasti bezpečnostního vzdělávání, analýzu 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. zabezpečení cloudového prostředí nebo bezpečnostního dohledu. Vzhledem k přetrvávající epidemické situaci může být rovněž zajímavé porovnání dat s výstupy z loňského roku, který již byl pandemií plně ovlivněn. 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.

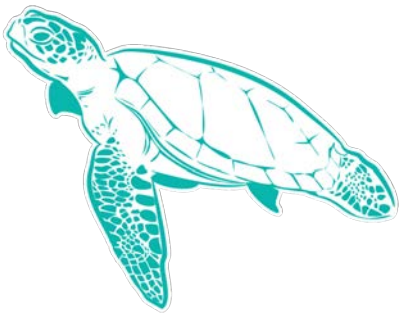


Analýza událostí zachycených IPS sondami

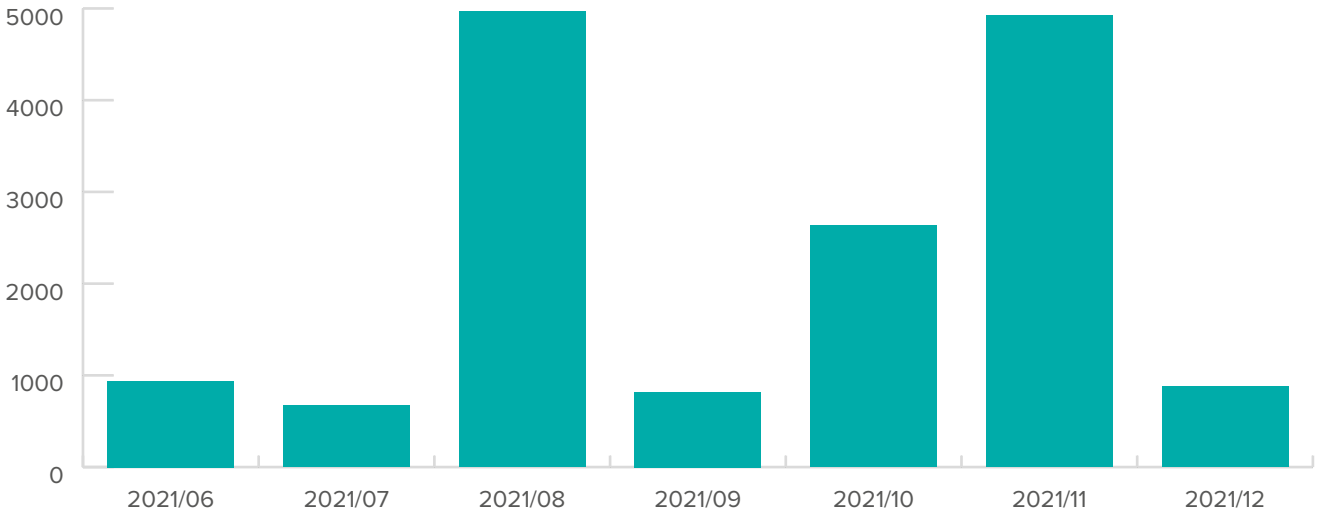
Stanislav Techlovský

Následující část reportu se zabývá analýzou dat z IPS (Intrusion Prevention System) sond pod správou společnosti ALEF Nula a.s. Analýza se zaměřuje na data z období posledních dvou kvartálů roku 2021.

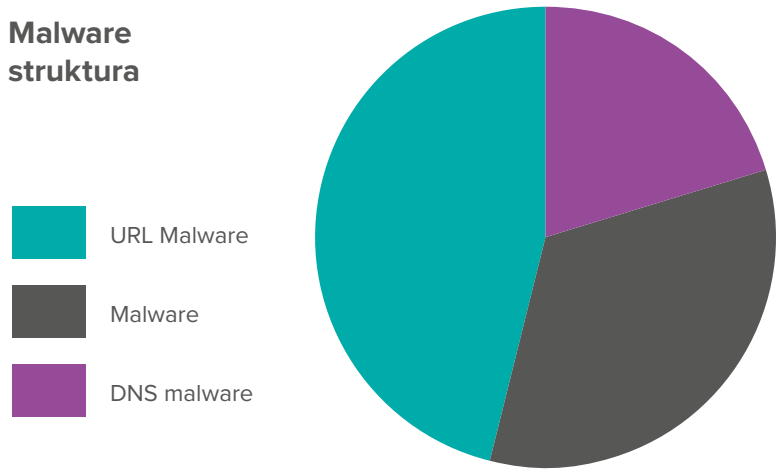
V první části analýzy se nejprve podíváme na phishing. IPS sondy detekovaly incident vždy, když se uživatel pokusil navštívit blokované phishingové stránky. Nejvíce incidentů z minulého roku bylo detekováno v měsíci srpnu v množství 4966 incidentů, což je bezmála 36 % snížení oproti předchozímu roku za stejný měsíc. Ke konci roku 2021, jak již bývá zvykem, došlo k postupnému nárůstu phishingových útoků souvisejících s vyšší aktivitou uživatelů na internetu. V posledním kvartálu roku 2021 byli útočníci nejaktivnější v měsíci listopadu, kdy provedli celkem 4926 phishingových útoků. Jedná se o 44 % snížení oproti předchozímu roku za totožné období.



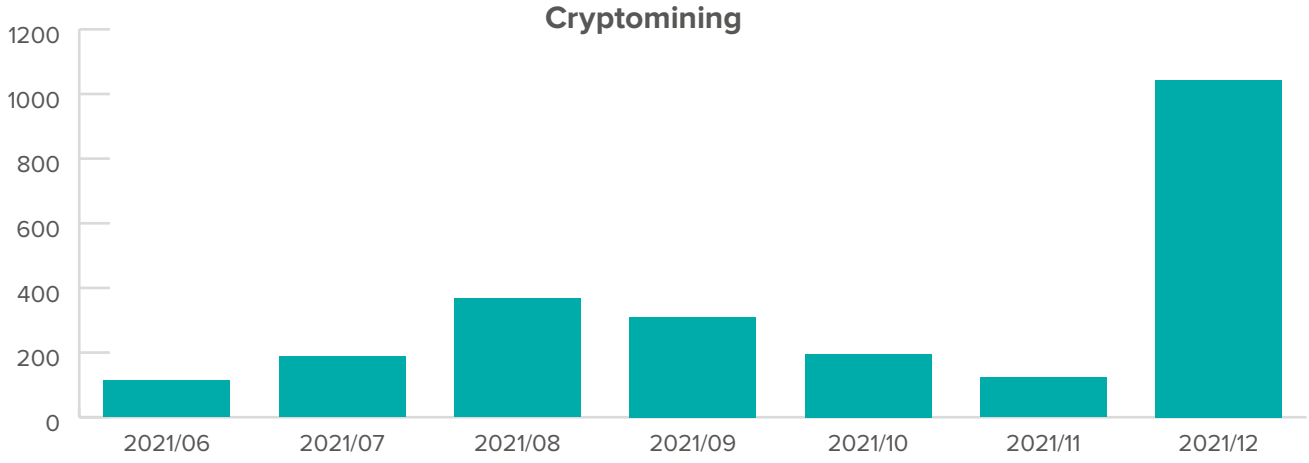
Phishing



Za poslední dva kvartály roku 2021 bylo největší množství incidentů spojených s malwarem zachyceno IPS systémy v měsíci červenec, šlo o bezmála 233 tisíc událostí. Jedná se o 26 % nárůst oproti předchozímu roku za totožné období. V prosinci bylo detekováno bezmála 89 tisíc incidentů, oproti předchozímu měsíci listopadu jde o 259 % nárůst. Vyšší četnost těchto útoků je dána vyšší uživatelskou aktivitou na internetu spojenou s koncem roku, k obdobnému nárůstu incidentů v tomto období dochází pravidelně, jak ukazují mimo jiné i data z předešlých let.



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 2021 byla struktura detekcí malwaru následující: z 34 % byly detekce výskytu malwaru realizovaného pomocí reputační databáze, ze 46 % byl malware odhalen prostřednictvím provedené URL kontroly a ze zbylých 20 % se jednalo o detekci využívající kontrolu DNS (viz. graf Detekce škodlivého kódu).



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 prosinci 2021 byl zachycen nejvyšší počet pokusů o těžbu kryptoměn o celkovém množství 1043 pokusů. Oproti předchozímu měsíci listopadu se jednalo o 848 % nárůst. Druhým měsícem s nejvyšším množstvím pokusů o těžbu kryptoměn byl měsíc srpen, kdy bylo zablokováno 368 pokusů, v následujících třech měsících došlo vždy k pozvolnému poklesu pokusů o těžbu kryptoměn.

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.

Sender Policy Framework

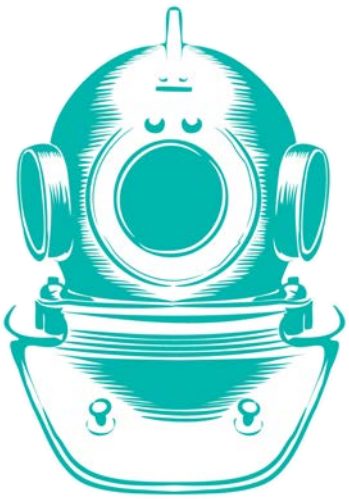
Tento bezpečnostní mechanismus umožňuje organizacím definovat, které servery mohou odesílat e-mailové zprávy, které využívají domény organizace. Kromě seznamu serverů, které mají toto oprávnění, by na konci SPF záznamu nemělo chybět pravidlo, jak zacházet se zprávami z ostatních serverů, které nebyly 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

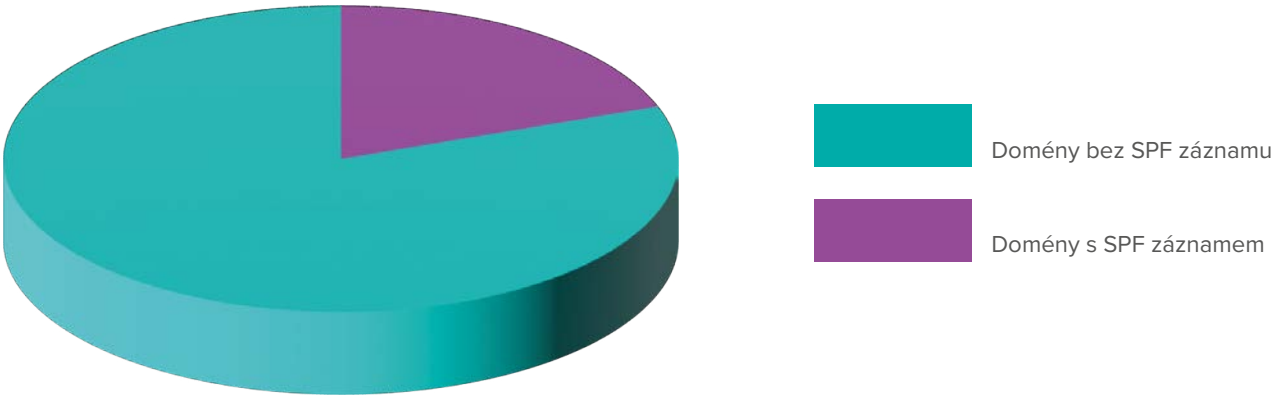
Český internet a SPF záznamy

Na konci roku byly získány statistiky o bezpečnostních mechanismech na doménách České republiky, tedy výhradně se jedná o .cz domény. Těchto domén existovalo 1 400 754. Téměř pětina českých domén měla v době sběru dat nastavený SPF záznam.

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.

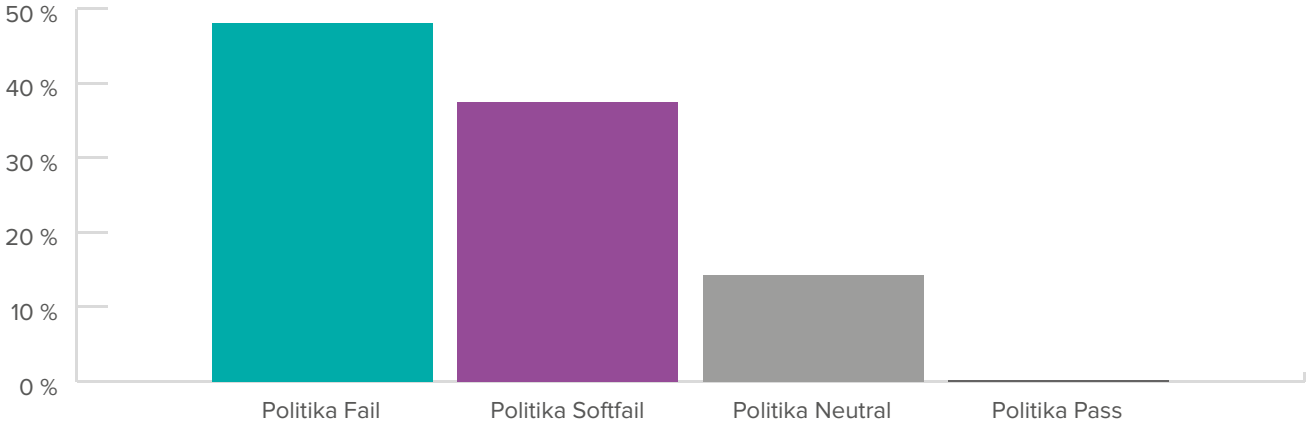


Poměr českých domén s SPF záznamem a bez něj

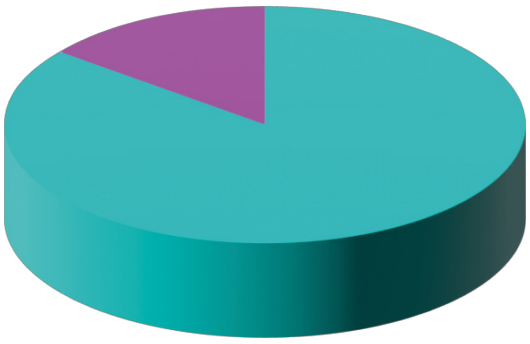


Domény s nastaveným SPF záznamem pak byly rozděleny do čtyř skupin, dle pravidel pro ostatní, nespecifikované servery, tato pravidla jsou popsána výše. Většina domén, které měly nastaven nějaký SPF záznam, používala první dva popsané typy tohoto pravidla. Zbytek těchto domén měl většinou nastaven třetí typ tohoto pravidla a několik domén používalo silně nedoporučovaný typ pravidla (0,17%). Na následujícím grafu je znázorněn procentuální poměr těchto metrik.

Poměr typů politiky SPF záznamů



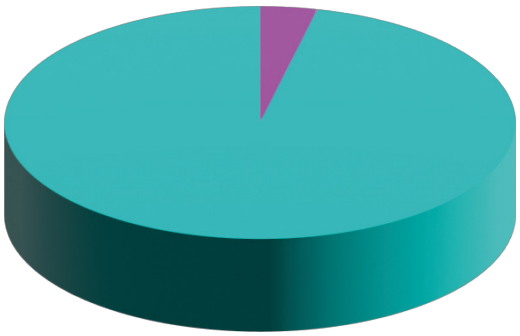
Většina domén tedy používá doporučenou politiku fail nebo softfail. Na následujícím grafu je znázorněn poměr použití doporučené konfigurace SPF pravidel oproti použití nedoporučené konfigurace.



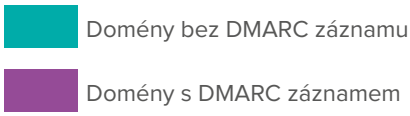
Český internet a adopce DMARC

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 (1 400 754).cz domén byl na konci roku 2021 nastavený DMARC záznam pouze u necelých 4 procent z nich.



Poměr českých domén s DMARC záznamem a bez něj

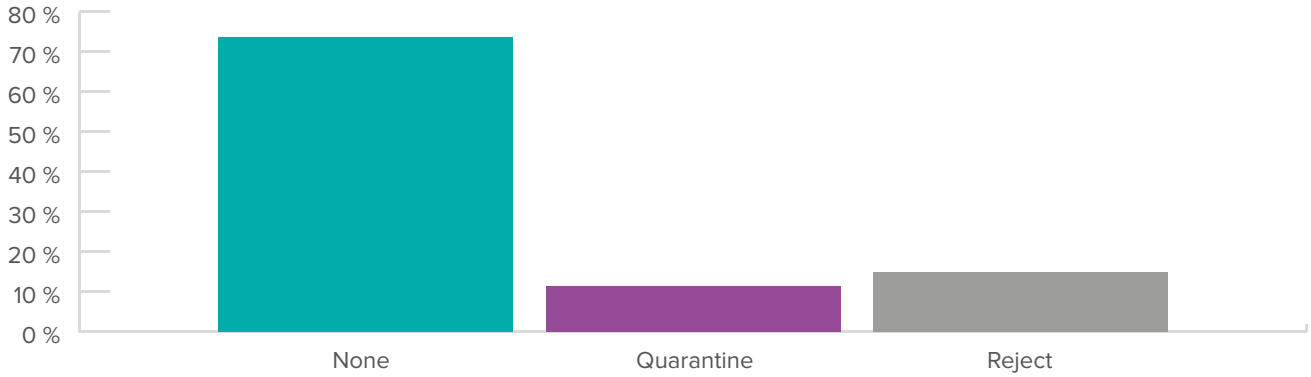


V rámci statistických dat získaných z českých domén pak byly analyzovány dva parametry v DMARC záznamech, které jsou pro správné fungování DMARC mechanismu nutné.

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.

Poměr typů politiky DMARC záznamů

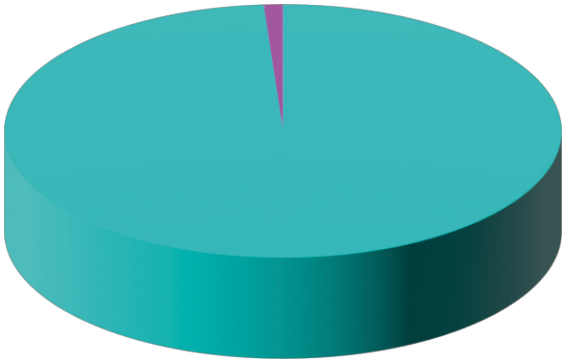


Druhým ze sledovaných parametrů je parametr pct, který určuje na kolik procent e-mailových zpráv, které neprošli kontrolou mechanismy SPF a DKIM má být aplikována politika z parametru popsaného výše. Doporučená hodnota tohoto parametru je 100, což znamená stoprocentní blokace nelegitimních e-mailových zpráv 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

Většina českých domén, které mají nastavený DMARC záznam, mají definovaný tento parametr s doporučenou hodnotou. Toto lze vypozorovat v následujícím grafu:



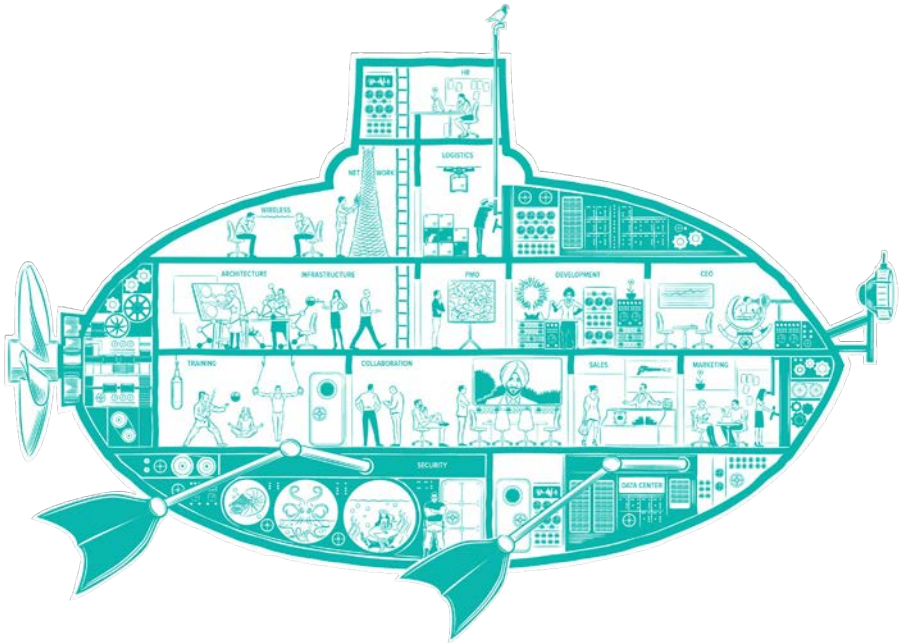
Poměr českých domén s DMARC záznamem s doporučenou hodnotou parametru pct

Domény s jinou hodnotou

Domény s doporučenou hodnotou parametru

Závěr

Tuto statistiku bude zajímavé sledovat v nadcházejícím roce, protože Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) vydal 11. října 2021 vyhlášku o povinnosti zabezpečení e-mailové komunikace. V této vyhlášce (https://www.nukib.cz/cs/infoservis/aktuality/1758-spravci-klicovych-systemu-musi-zabezpecit-sve-e-mailove-schranky/) je mimo jiné popsána povinnost implementace SPF, DKIM a DMARC mechanismů. Některá opatření, která jsou popsána v této vyhlášce, musejí mít státní instituce zavedeny od 1. ledna 2022, další opatření až od 1. července 2022. Povinné subjekty ze soukromého sektoru musejí mít tato opatření zavedena od 1. ledna 2023.



Bezpečnostní dohled a stav Security Operations v roce 2021

Daniel Neumann

Problematice bezpečnostního dohledu jsme se rozhodli věnovat i ve stávajícím vydání Alef Security report 2022. Aktuálně získaná data tak máme možnost porovnat s předchozími dvěma ročníky a zjistit případné změny chování v oblasti bezpečnostního dohledu.

V 21. stolení nejsou slova jako kybernetická bezpečnost či kybernetický útok ničím neznámým. Dočteme se o nich v novinách, baví se o nich lidé na ulici a často bývají hlavním tématem večerních zpráv. Každý zodpovědný zaměstnavatel by měl své zaměstnance pravidelně upozorňovat na rizika ukrytá v kyberprostoru, zaměstnance školit a ideálně i testovat jejich praktické znalosti a reálnou připravenost na konkrétní typy hrozeb. Položme si ovšem otázku. Opravdu se tomu tak děje? A pokud ano, v jaké frekvenci, kvalitě a s jakým reálným dopadem? Firmy vlastní a uchovávají čím dál více citlivých dat, v důsledku čehož roste poptávka po nástrojích/službách zajišťujících IT bezpečnost. Výdaje určené na kybernetickou bezpečnost se tak stávají pravidelnou součástí rozpočtu, jenž se v mnohých případech zvyšuje rok co rok.

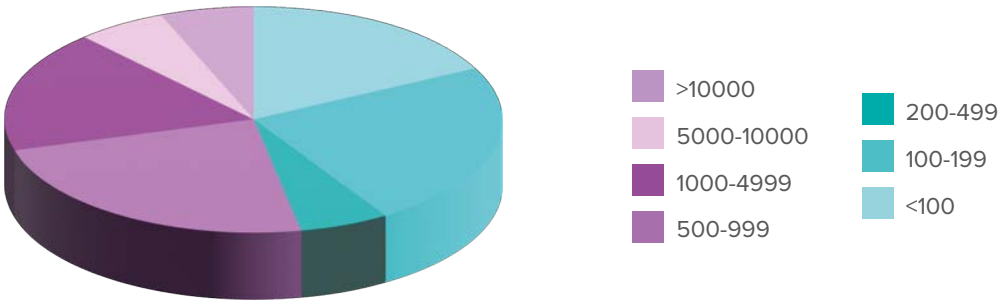
Hackeři jsou čím dál rafinovanější a řada bezpečnostních nástrojů pro ně nepředstavuje velkou překážku. Na jejich hrozby je potřeba reagovat co nejrychleji. V případě kybernetického útoku se počítá každá minuta. Včasná reakce může postiženou organizaci ušetřit od neočekávaných finančních výdajů, poškození dobrého jména či omezení plynulého chodu organizace. Bez kvalitní bezpečnostní ochrany se v dnešní době žádná firma neobejde. Věřím, že mi dáte za pravdu, když budu tvrdit, že odborníků na kybernetickou bezpečnost je na lokálním trhu momentálně akutní nedostatek. Firemní IT mnohdy dělá, co může, ale není jednoduše v jeho silách 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. Je toho prostě moc. 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 požádali 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, jak k otázce bezpečnosti přistupovat. Bezpečnostní dohled není výjimkou. Některé organizace důvěřují svým zaměstnancům a spoléhají na jejich opatrnost. Tento přístup s sebou ovšem nese jistou míru rizika. V každém případě je nutné zajistit zaměstnancům dostatečnou informovanost a umožnit pravidelná bezpečnostní školení, která by měla zvýšit bezpečnostní povědomí napříč organizací. Druhou možností je zřízení vlastního IT oddělení. V návaznosti na jeho velikost a počet 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 značnou finanční zátěž. Organizace tak stojí před volbou – omezená bezpečnost, nebo vysoké provozní náklady.

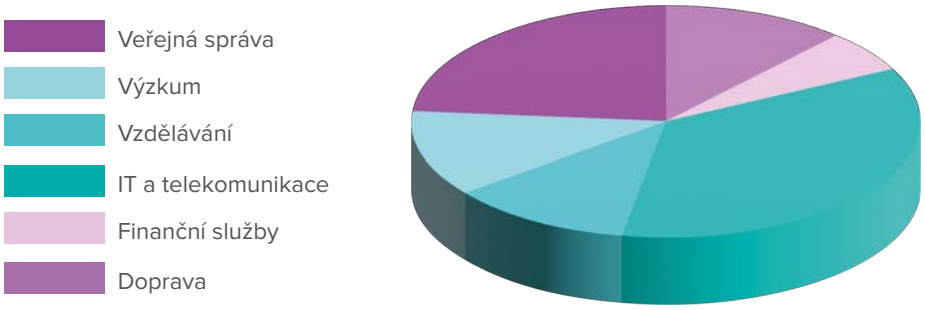
Na níže uvedeném grafu lze vidět, že jsou v rámci našeho dotazníkového šetření zastoupeny jak organizace o několika stovkách zaměstnanců, tak i ty, jejichž počet přesahuje 10 000.

Kolik zaměstnanců má Vaše organizace?



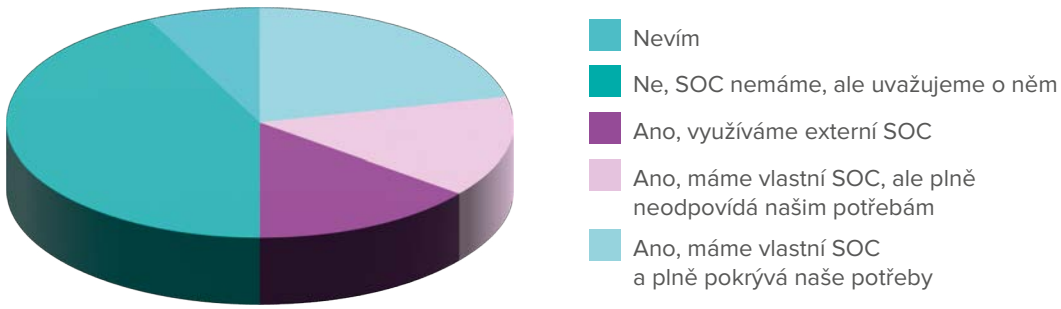
Z hlediska oborového zastoupení mezi respondenty nejvíce figurovali zástupci z IT a telekomunikací (cca třetina), následováni státní správou (cca pětina) a dále energetickým průmyslem (14,3 %) a sektorem dopravy (14,3 %).

V jakém sektoru Vaše organizace působí?



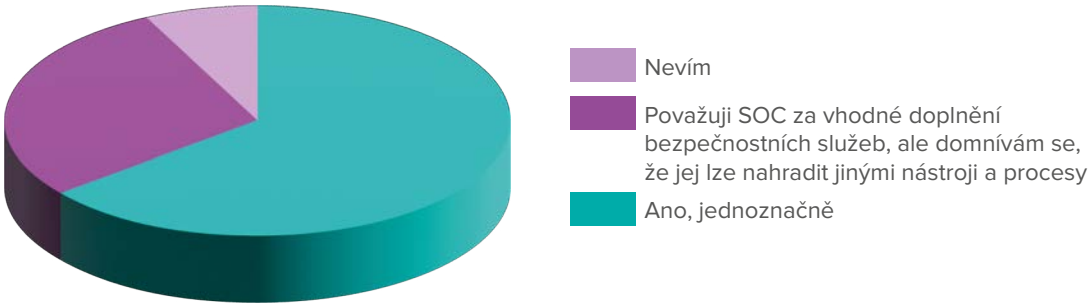
V samotném úvodu šetření nás zajímalo, kolik procent z dotázaných využívá služeb SOC. Pětina zákazníků má vlastní SOC, který plně pokrývá jejich potřeby. Zhruba 15 % sice SOC vlastními silami provozuje, ten ovšem úplně nevyhovuje interním potřebám. Obdobné zastoupení pak představuje počet organizací využívajících služeb externího SOC. Více jak 40 % SOC nemá, ale uvažuje o něm. Podobné výsledky přinesl report i v minulém roce. Stále tedy platí, že fáze „uvažujeme o SOC“ trvá roky a ve výsledku nevede k ničemu (tvrdý verdikt, který bohužel naprosto koresponduje s praktickými zkušenostmi). Potěšující je, že nikdo neodpověděl, že SOC organizace nemá a ani o něm neuvažuje.

Využíváte služeb SOC (Security Operations Center)?



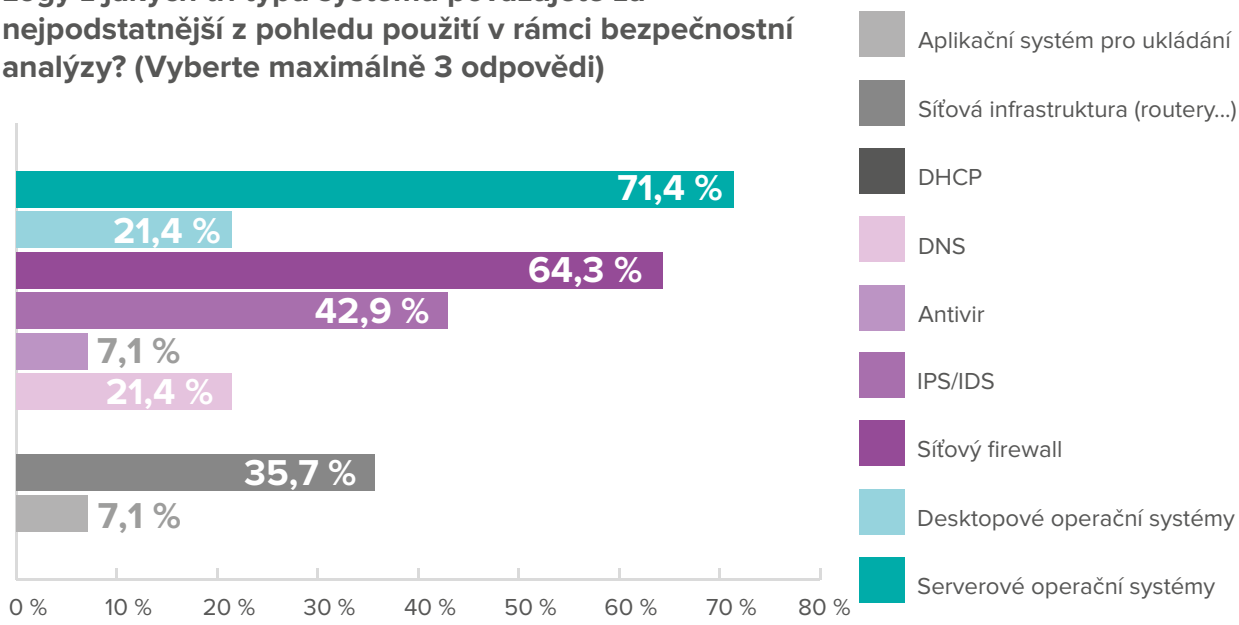
Považujete SOC za nutnost? Zhruba dvě třetiny odpověděly „ano, jednoznačně“. V porovnání s předchozím obdobím došlo k nárůstu o zhruba 15 %, a to na úkor respondentů, kteří považují SOC za vhodné doplnění bezpečnostních služeb, ale domnívají se, že jej lze nahradit jinými nástroji a procesy.

Považujete SOC za nutnost?



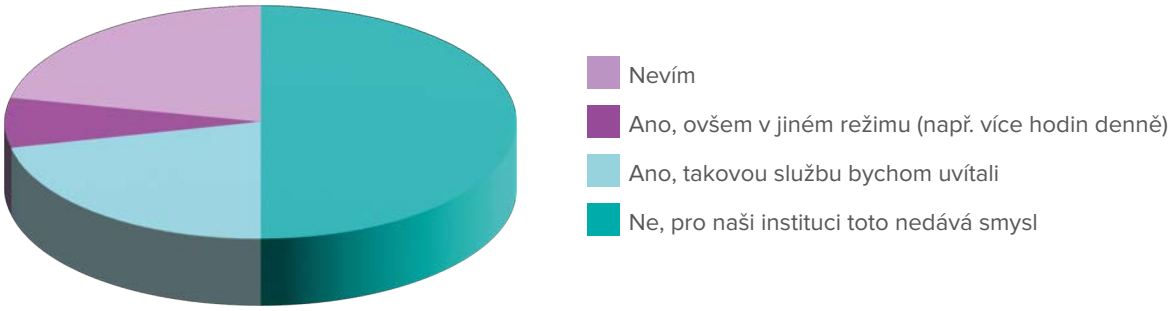
V rámci bezpečnostní analýzy hraje významnou roli zaznamenávání dat za účelem jejich analýzy (logování). Logy z jakých tří typů systémů považují oslovené organizace za nejvýznamnější? V pořadí dle důležitosti to byly serverové operační systémy, síťový firewall a IPS/IDS. Výsledky se od předchozího roku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

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



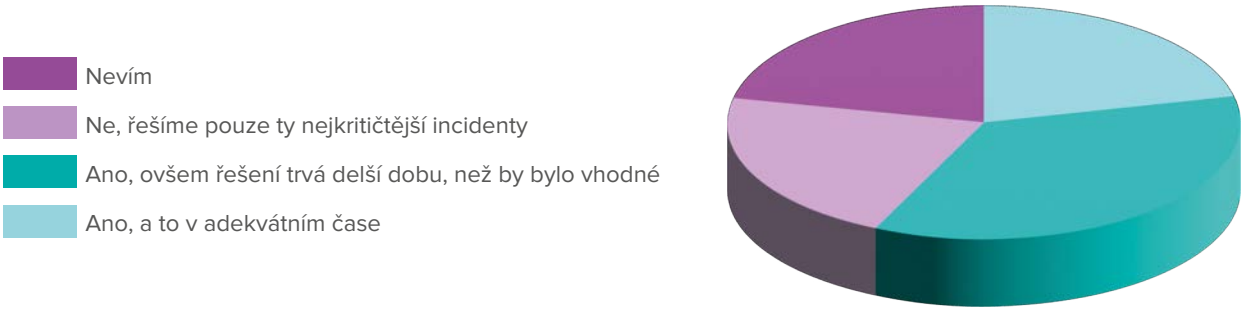
Bezpečnostní dohled bývá standardně v režimu 8x5 či 24x7. Tento rozsah služby je jistě velice efektivní a s vysokou pravděpodobností pomůže odhalit nekalé aktivity útočníků při samém počátku, představuje ovšem variantu, která je z důvodu časové vytíženosti značně nákladná a většina organizací si ji z 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 polovinu oslovených tento typ dohledu nedává smysl, pětina by jej naopak uvítala a dalších 20% si není jisto.

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



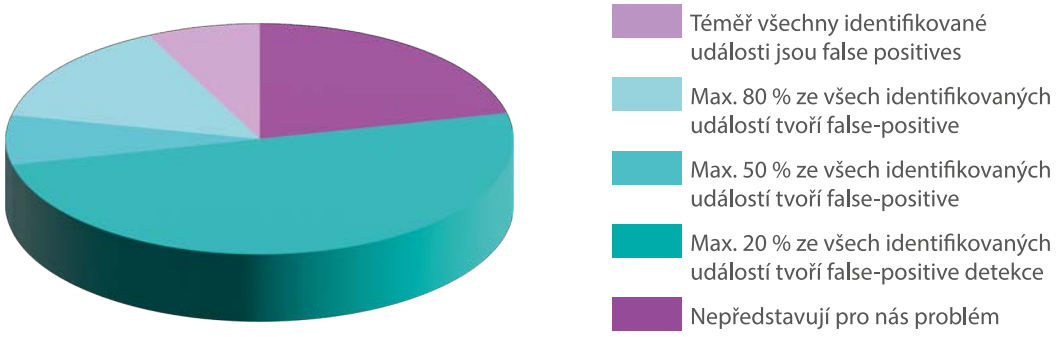
V dnešní době se každé IT oddělení potýká s řešením bezpečnostních incidentů. Jejich množství se odvíjí od mnoha faktorů – „atraktivnosti“ dotyčné organizace pro útočníky, bezpečnostních technologiích schopných tyto incidenty identifikovat a zkušenostech členů IT oddělení. Zvládají oslovené instituce řešit každý odhalený bezpečnostní incident? Pětina ano, a to v adekvátním čase. Třetina sice ano, ale řešení trvá delší dobu, než by bylo vhodné. Pětina je schopná řešit pouze ty nejkritičtější incidenty.

Zvládáte řešit každý odhalený bezpečnostní incident?



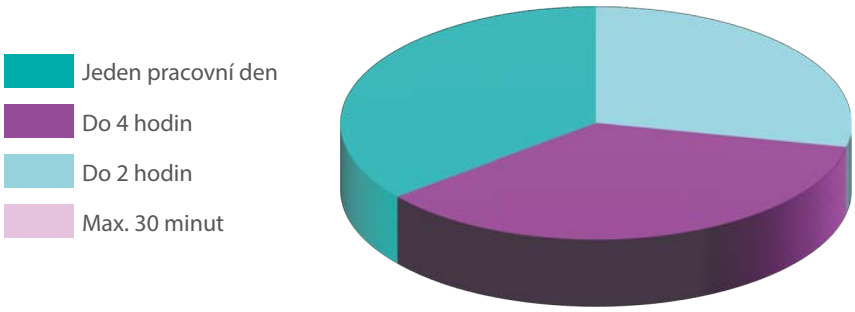
Díky automatizovaným skenům sítě, IPS, SIEMu a dalším nástrojům získává IT oddělení data, se kterými následně pracuje. Ne vždy se ovšem jedná o data validní. V mnohých případech se může jednat o chybné detekce událostí, tzv. „false-positive“. Pokud se musí pracovníci IT zabývat vysokým počtem takovýchto 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 pětinu organizací nepředstavují problém. V polovině případů tvoří maximálně 20 % všech identifikovaných událostí. Obdobné výsledky uváděl i report v předchozím roce, kdy uvedené dvě kategorie též vykázalo více jak 70% dotázaných organizací.

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



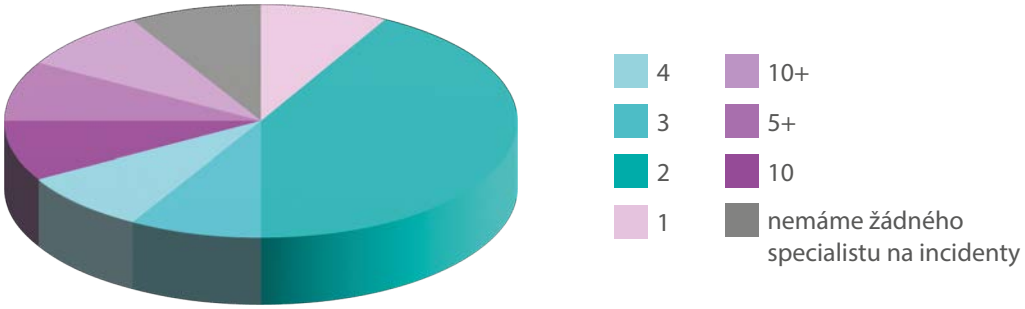
Kybernetické bezpečnostní incidenty bývají nepředvídatelné, vznikají a vyvíjejí se často ve velmi krátké době a zasažené subjekty i osoby odpovědné za reakci na incidenty a zmírnění jejich účinku musí proto reagovat velice rychle. Minimalizace reakční doby na incident je tak jednou z nejefektivnějších forem obrany vedoucí ke zmírnění dopadu incidentu. V rámci dotazníku nás zajímalo, jakou reakční dobu na nekritický bezpečnostní incident považují organizace za dostatečnou. Přibližně třetina si myslí, že reakce do 4 hodin je dostatečná. Stejné zastoupení měla skupina, pro níž je adekvátní dobou řešení jeden pracovní den. Necelých 30 % respondentů se ztotožňuje s dobou kratší než 2 hodiny.

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



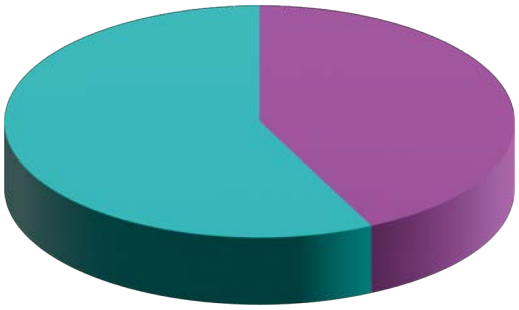
Kolik lidí je v rámci organizace oficiálně zodpovědných za reakci na incidenty? Třetina oslovených organizací zvolila 2 zodpovědné osoby. Další odpovědi na tuto otázku jinak byly značně nesourodé, neboť v některých organizacích je zodpovědná pouze jedna osoba, jinde je takových lidí více jak 10.

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



Rok 2021, stejně jako rok 2020, byl v jistém směru unikátní. Bohužel nikoli v pozitivním slova smyslu. Důvodem je pandemie týkající se COVID – 19. Zajímalo nás, zda pandemie nějakým způsobem ovlivnila oblast bezpečnostního dohledu. Zhruba 43 % respondentů odpovědělo, že pandemie oblast bezpečnostního dohledu neovlivnila žádným způsobem. 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?

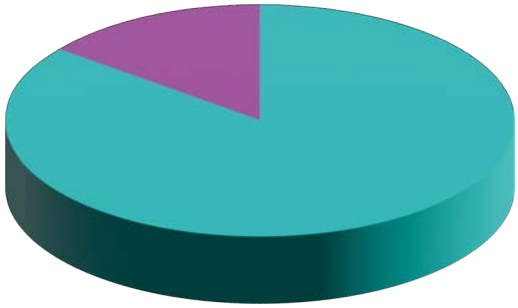


- Ne, oblast bezpečnostního dohledu neovlivnila, promítla se ovšem do jiných oblastí firemního IT
- Ne, oblast bezpečnostního dohledu ani jiné oblasti IT pandemie neovlivnila

Závěr průzkumu věnujeme výši investic určených na zajištění kybernetické bezpečnosti v návaznosti na pandemickou situaci. Více jak 85 % účastníků průzkumu uvedlo, že výši investic do kybernetické bezpečnosti pandemie neovlivnila. V případě 14,3 % respondentů došlo k navýšení investic, ovšem nijak výraznému.

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

- Ano, do KB jsme investovali více prostředků, ovšem nijak výrazně
- Ne, výši investic do KB pandemie neovlivnila



Protokol DNS a analýza provozu v roce 2021

Jan Šimůnek

Rok 2021 přinesl několik zajímavých aktualit v prostředí DNS, které ve většině případů souvisí s postupným přechodem na šifrované varianty protokolu DNS. Za zmínku stojí například implementace Oblivious DoH (oDoH) nebo DDR (Discovery of Designated Resolvers). Zajímavý pohled také nabízí analýza adaptace šifrovaných variant a množství přeložených dotazů veřejně dostupnými servery. Na závěr tohoto textu se podíváme na bezpečnost řešenou na úrovni DNS a množství blokovaných dotazů za uplynulý rok na domény spojené se škodlivými aktivitami.

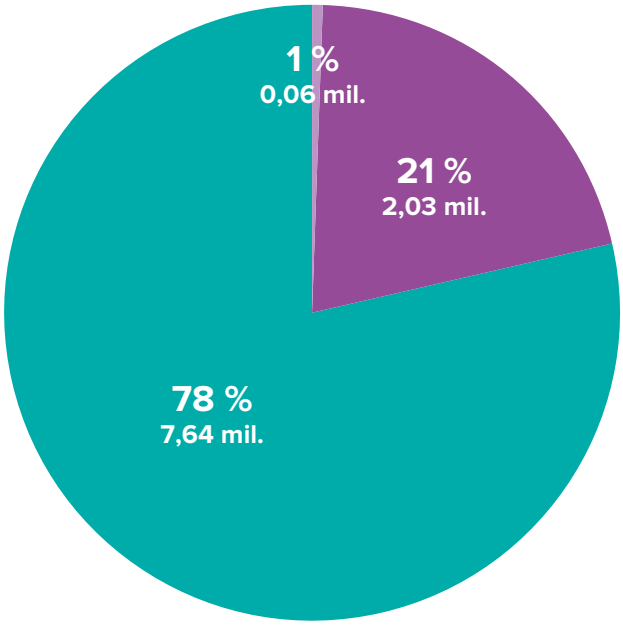
Začněme novinkami, které se v minulém roce udály. První z nich je protokol oDoH s cílem minimalizovat možnost správců rekurzivních resolverů monitorovat aktivity koncových uživatelů. Princip je založen na použití proxy systému, který přeposílá šifrované dotazy na server poskytující překlad a skrývá zdrojovou adresu iniciující strany. Proxy server maskuje svou adresou klienty posílající dotazy a tím znemožňuje možnost již zmíněné korelace dotazů a koncových stanic. Běžný uživatel se s tímto protokolem může setkat například u zařízení Apple iOS 15 nebo macOS Monterey při zapnutí funkce iCloud Private Relay.

Dalším zajímavým konceptem představeným v minulém roce je DDR. Jedná se o mechanismus navržený firmami Cloudflare, Microsoft, Apple a Fastly. DDR je schopný bez manuální konfigurace rozpoznat možnosti DNS serveru a automaticky přepnout do šifrované podoby ve formě DNS over HTTPS (DoH) nebo DNS over TLS (DoT). To však pouze za předpokladu, že je tato funkce serverem podporovaná. Celý princip je založen na odeslání plaintext dotazu na DNS server se SVCB záznamem obsahující „*_dns.resolver.arpa*“. Odpovědí jsou již zmíněné podporované možnosti šifrování a následná komunikace tak může probíhat v zabezpečené podobě.

Statistiky odbaveného provozu rekurzními resolvery

Následující část textu se zabývá pohledem na odbavený provoz na veřejných rekurzivních resolverech. Poskytnutá data pochází ze společnosti Cisco Umbrella. Statistiky zahrnují jak consumer (OpenDNS), tak enterprise (Umbrella) provoz směřující na rekurzivní resolvery a porovnávají začátek a konec roku 2021 během vybraného dne v časech, kdy počty dotazů dosahují globálního maxima. Hodnoty v grafech udávají počet dotazů za sekundu pro jednotlivé podporované protokoly: DNS over 53 a šifrované verze DoH a DNSCrypt. Nutné je taktéž objasnit, že dotazy skrze DNSCrypt jsou preferovanou variantou šifrované podoby a ve velké míře jsou generovány klientským softwarem instalovaným přímo na koncových stanicích. V případě tohoto typu dotazu se tedy velmi pravděpodobně jedná o stanice nacházející se převážně mimo firemní síť.

Ze statistik je možné pozorovat pouze mírný nárůst využití protokolu DoH. Oproti tomu 15% nárůst z celkového množství položených dotazů je možné spatřit u protokolu DNSCrypt. Tento nárůst je tak velmi pravděpodobně způsoben rostoucím počtem práce z domova související s pandemií Covid-19.

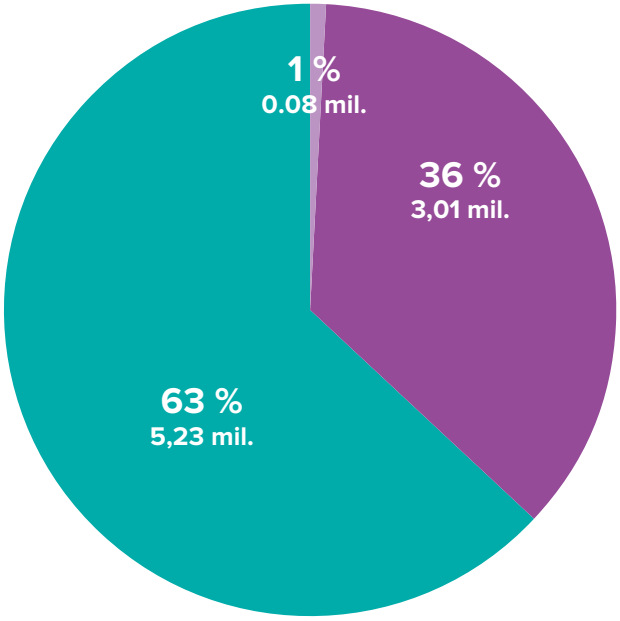


Počet dotazů za sekundu, únor 2021

Do53
DNSCrypt
DoH

Počet dotazů za sekundu, prosinec 2021

Do53
DNSCrypt
DoH

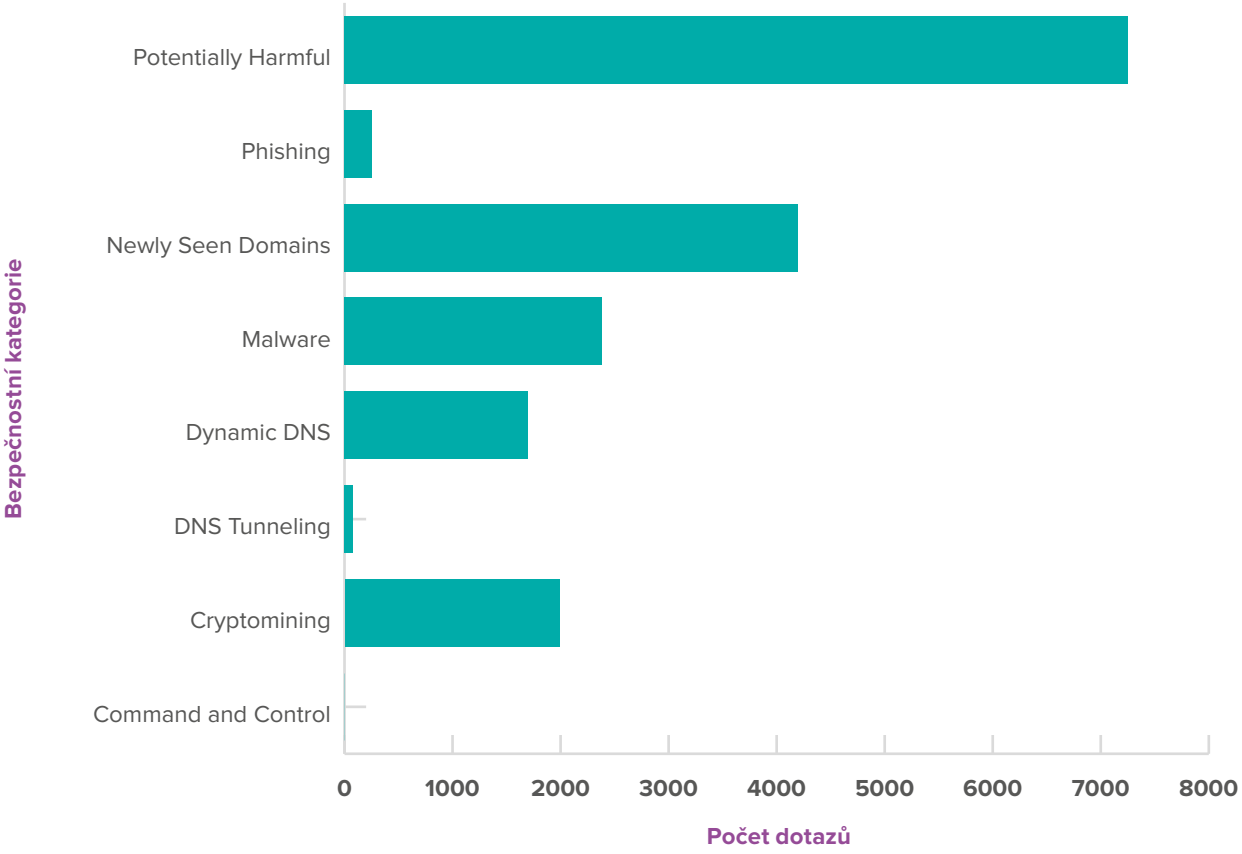


Detekování komunikace na škodlivé domény
Detekce a následná blokace DNS dotazů, které směřují na škodlivé domény je funkce, kterou poskytují některé rekurzivní resolvery. Tento způsob ochrany se jeví jako efektivní řešení v decentralizované architektuře s cílem zabezpečit koncové stanice a znesnadnit útočníkům jejich aktivity.

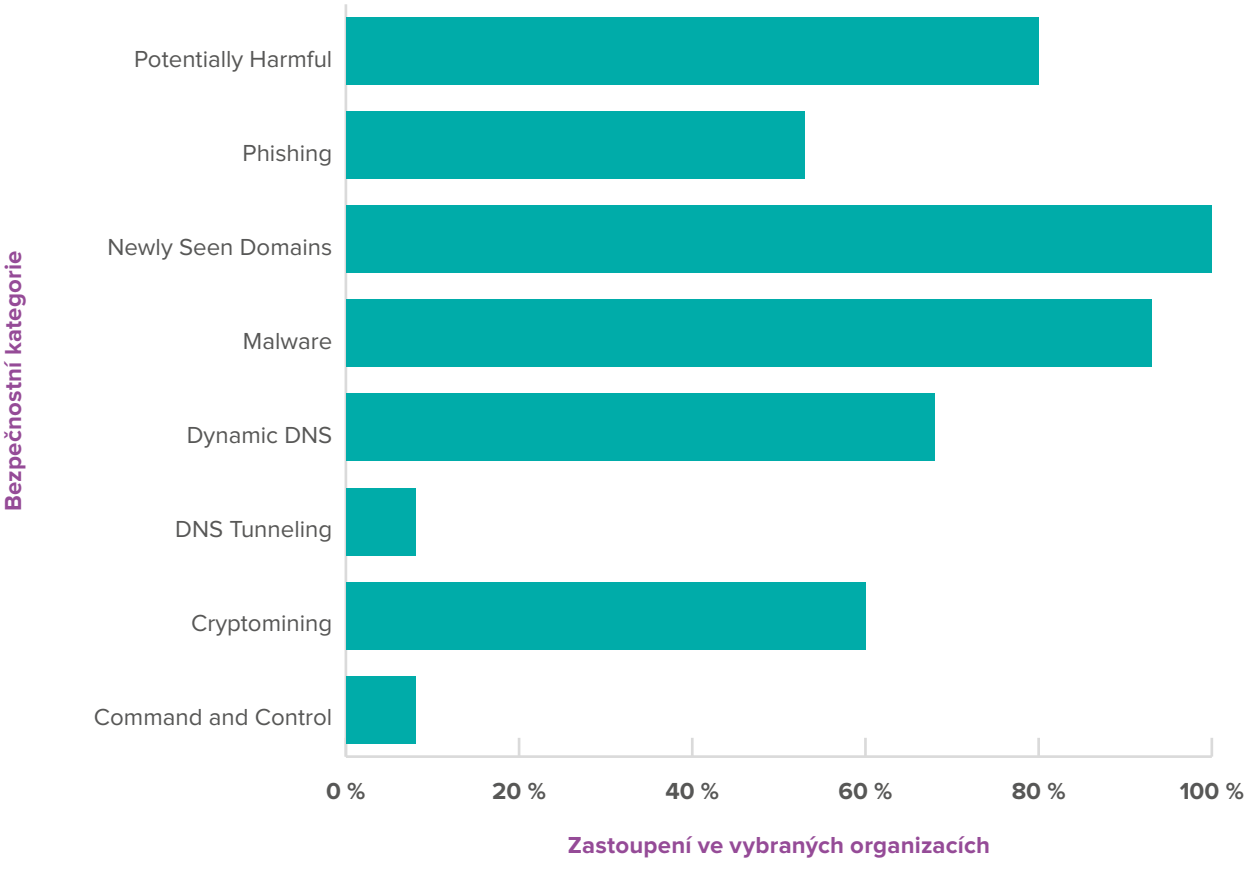
Následující data jsou získána z technologie Cisco Umbrella napříč několika vybranými organizacemi za měsíc listopad. Jako nejčastější se jeví blokace dotazů podezřelých domén vyznačující se nízkým reputačním skóre. Následují nově vytvořené záznamy, které zahrnují jak legitimní záznamy, na které doposud nebyl generován provoz, tak nově vznikající phishingové kampaně a DGA (Domain Generation Algorithms). Za zmínku taktéž stojí množství domén obsahující malware a blokace 1980 dotazů spadající do kategorie Cryptomining, které jsou detekovatelné na základě dotazů do tzv. mining poolů.

Téměř 93% organizací detekovalo ve své infrastruktuře dotazy na domény spojené s malwarem a následně blokovalo komunikaci spojenou s nežádoucími aktivitami. Poměrně vysoký je také výskyt dotazů spadající do kategorie phishingu (53% dotázaných) a cryptominingu (60% dotázaných).

Počet blokovaných dotazů na škodlivé domény, listopad 2021



Objevené škodlivé domény napříč organizacemi, listopad 2021

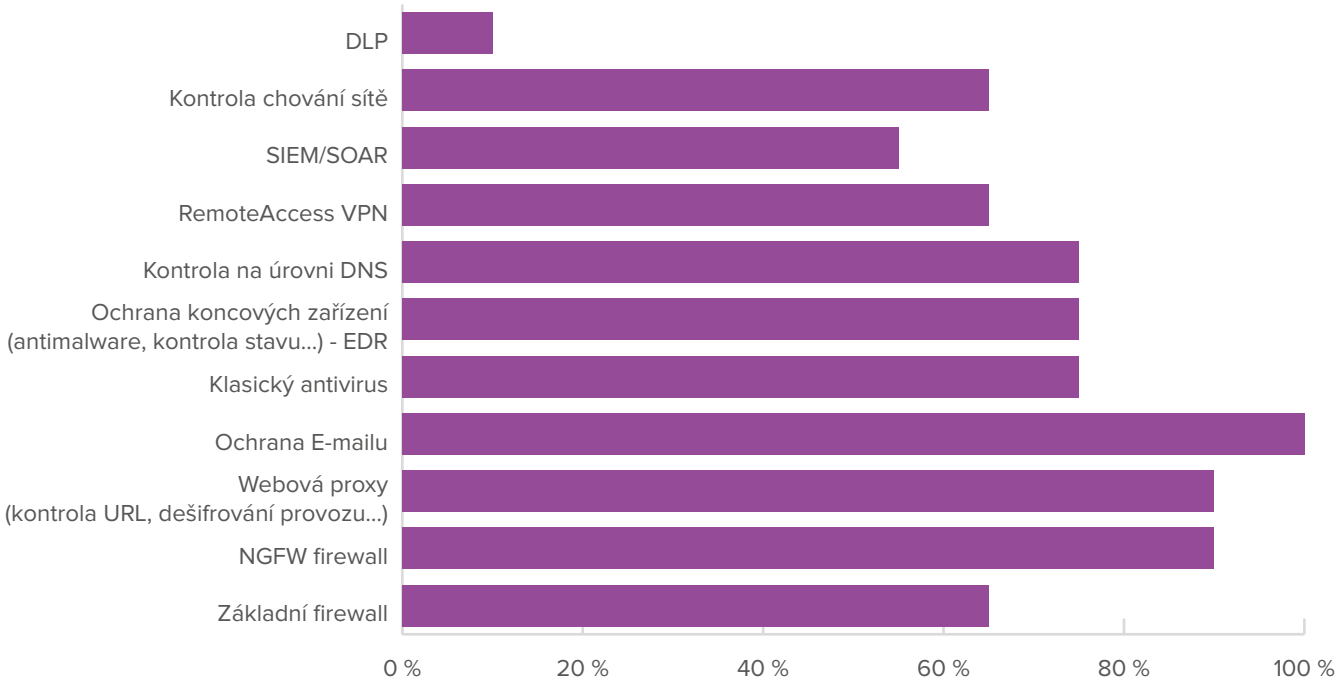


Kyberbezpečnostní technologie používané v reálném světě

Jiří Herzig

Od prvního antivirového softwaru a prvního firewallu uplynula už pěkná řádka let a počet technologií které zajišťují naši bezpečnost v kybersvětě značně narostla. To, že jen malé množství společností řeší každou oblast kyberbezpečnosti, ukazují i odpovědi v našem dotazníku, kde dotazovaní odpovídali na otázky týkající se právě používaných technologií v jejich prostředí. Ruku v ruce s množstvím technologií ale hraje roli i velikost společnosti a citlivost dat, se kterými pracují, stejně jako schopnost financovat nákup těchto nových technologií.

Jaké technologie pro kybernetickou bezpečnost používáte?



V první otázce dotazníkového průzkumu jsme se zajímali o to, jaké technologie jsou nejčastěji využívány. Použití firewallu je dnes již nutností. Je to ta nejzákladnější technologie, která dokáže prostředí uživatele ochránit před útočníky toužícími po datech, nebo těmi, kteří chtějí „jen“ uškodit. Základní stavové firewally již ale dnes nedokáží ochránit sofistikovaný útok moderních hackerů a jejich nástrojů. V tomto případě mohou pomoci tzv. firewally nové generace (NGFW) a jejich schopnost kontrolovat provoz na úrovni aplikací, nebo na základě URL, případně využijí kontrolu na viry a malware. Další funkcí těchto firewallů pak často bývá právě IDS/IPS, tedy pokročilá ochrana proti vniknutí nežádoucích osob. Dle výsledků můžeme vidět, že nějakou verzi firewallu používají všichni dotazovaní, někteří i obě varianty.

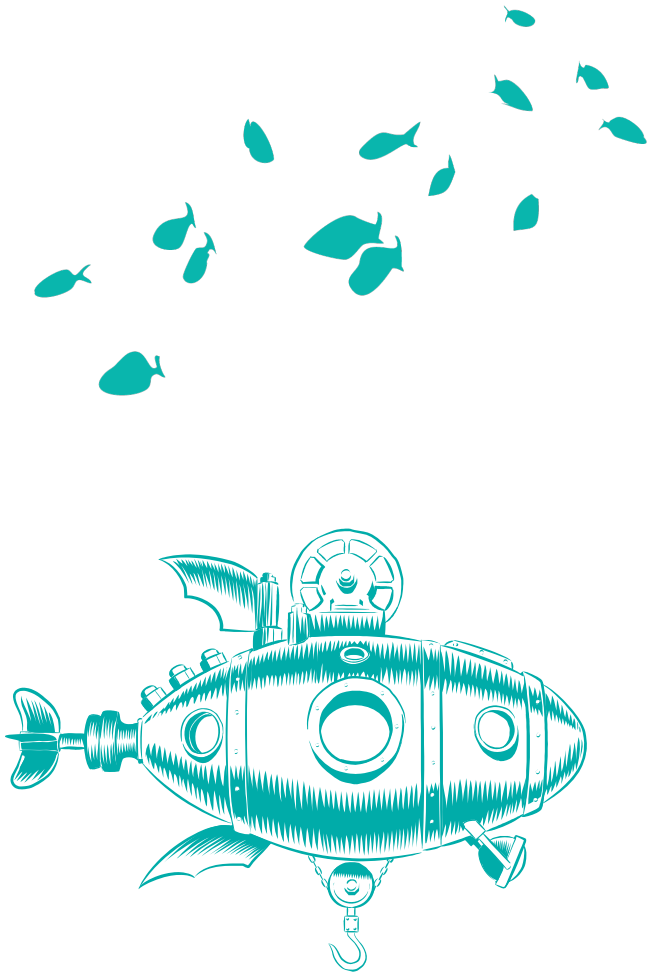
Můžeme zde vidět, že ochranu e-mailu, ať už v jakékoliv podobě, používá 100 % dotazovaných.

A není se čemu divit. I v dnešní době sociálních sítí, chatovacích platforem a sdílených úložišť je e-mail stále nejpoužívanějším způsobem komunikace v podnikovém prostředí. I z tohoto důvodu si útočníci vybírají právě tuto platformu a používají ji k šíření malware, phishingových kampaní a k jiným způsobům získávání informací o Vašem prostředí nebo uživatelích. Je proto namístě tuto platformu chránit alespoň základními nástroji proti spamu, či pokročilými proti malware a phishingu. Statistiky o zneužití e-mailu naleznete v článku na straně 24.

V těsném závěsu za e-mailem se drží kontrola webového provozu, jeho dešifrování či filtrování na úrovni kategorií, případně jako webová proxy. I toto dává smysl, vzhledem k tomu, že většina uživatelů vyhledává informace právě na webu. Někteří uživatelé jej i v pracovním prostředí používají k soukromým účelům a mnohdy k přístupu na pochybné stránky. Právě pomocí webové proxy dokážeme zakázat komunikaci na určité kategorie, případně komunikaci konkrétních aplikací.

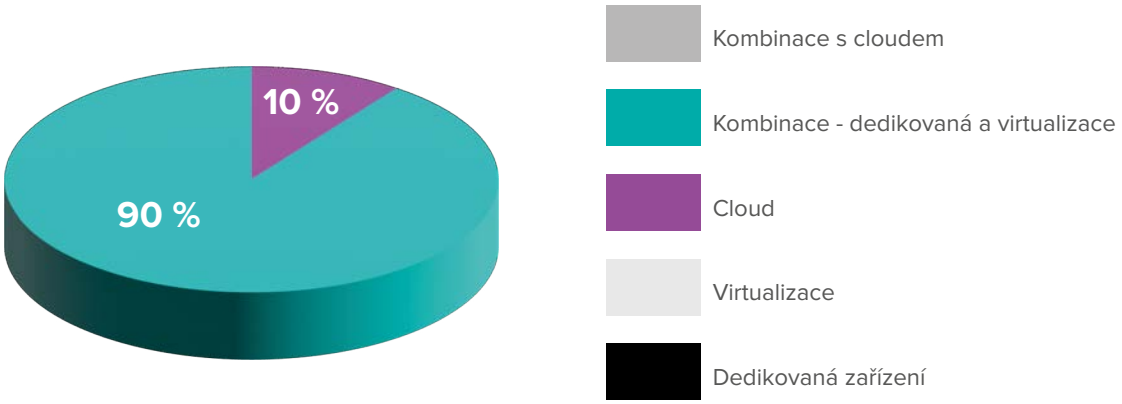
Další kategorie otázek se dá označit souhrnně jako ochrana koncových zařízení. Týká se prostředí podnikové sítě, nebo mimo ni, v domácnostech uživatelů, či na cestách. Velmi často mají uživatelé pracovní zařízení k dispozici i pro soukromé účely. Zde se setkáme s problémem, jak zabezpečit, aby po příchodu do kanceláře nám uživatel nepřinesl do vnitřní sítě různé viry či malware. Základem je antivirus. Ten ale často nedokáže rozeznat vysoce inteligentní malware, nebo „novinky“ v oblasti virů. Z tohoto důvodu se doporučuje používat antimalware software, který dokáže například podezřelé soubory vložit nejen do karantény, ale i do tzv. sandboxu a zkoumat jejich chování. Tímto způsobem je tam možné například odhalit Zero Day útoky (nejsou ještě obecné známé), případně Fileless malware (nacházející se pouze v operační paměti zařízení). Ochrana na úrovni DNS pak dokáže nahradit podnikovou webovou proxy i mimo podnikovou síť a zabránit tak přístupu např. na phishingové stránky. Remote Access VPN se do této kategorie dá jistým způsobem také počítat, zde se ale vytvoří zabezpečené spojení přes Internet do podnikové sítě a ochranu tak zajišťují právě bezpečnostní zařízení v této síti.

Security Information and Event Management (SIEM) nebo Security Orchestration, Automation and Response (SOAR) jsou technologie, které velkou měrou přispívají k ukládání logů, jejich třídění, vyhodnocování a další práci s těmito daty. Stejně jako kontrola chování sítě (např. Secure Network Analytics od Cisco) tak i Data Lost Protection, jsou tyto technologie v našich podnicích vzácnější a ukazují na to, že v tomto případě se to se síťovou bezpečností v podnikovém prostředí myslí opravdu vážně.



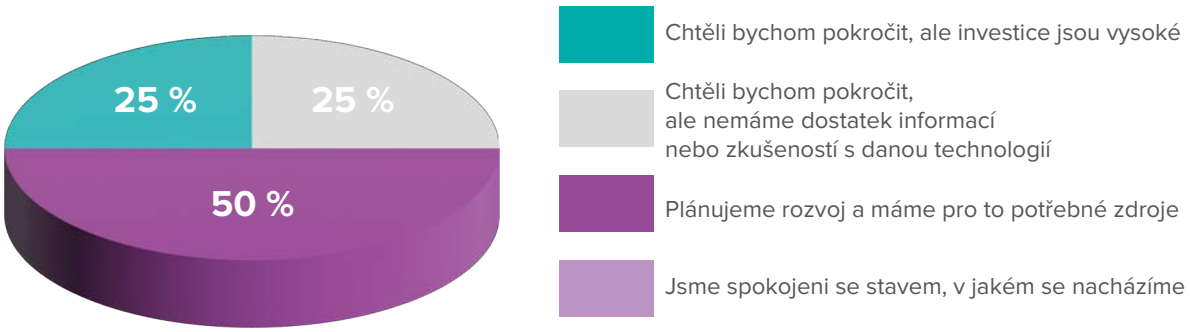
Pokud víte, jakou technologii budete používat, ještě stále není zcela vyhráno. Je totiž několik způsobů, jakým ji ve svém prostředí nasadíte. Pryč jsou časy, kdy bylo potřeba mít pro každou technologii dedikované zařízení, které dodával konkrétní výrobce. I tato možnost je u nás stále častá, ale doplňuje ji tzv. virtualizace, kdy na jednom výkonném serveru můžete provozovat více technologií a lze je i zaměňovat. Z grafu je jasně vidět, že se nejvíce používá právě kombinace těchto dvou způsobů. I u dedikovaného firewallu totiž můžete použít například virtualizovaný management, případně si ve virtuálním prostředí postavit celý lab, kdy se náklady počítají pouze za software, případně licence. Můžeme vidět, že cca 10 % dotazovaných dává přednost instalaci v cloudu. Tak nízké číslo může být dáno nedůvěrou v cizí prostředí, potřebu mít servery pod kontrolou, zákonné předpisy, nebo nedostupnost takové služby. Stále více klasických řešení se ale dostává k velkým poskytovatelům cloudových služeb jako je AWS nebo MS Azure. Výhodou takového řešení může být například pozbytí nutnosti udržovat hardware aktualizovaný a hlavně aktuální vzhledem k technickému pokroku. Jsou ale i služby, které jinak než v cloudu neběží. Tou může být například Cisco Umbrella či Secure Endpoint, sloužící k ochraně koncových zařízení. Můžeme v tom spatřit výhodu rychlého nasazení bez nutnosti vlastnit jakýkoliv hardware.

Pokud je možnost si vybrat, jaké formě instalace kybernetického zabezpečení dáváte přednost?



Tak jako v jakémkoliv jiném odvětví, i v kyberkriminalitě se útočníci snaží přijít každý den s novým řešením, jak se dostat k datům a informacím jednotlivých uživatelů. V tomto odvětví je to ještě umocněno tím, že informace vládnou světu a je to často velmi cenná komodita. Z toho důvodu je dobré, ne-li přímo nutné, držet krok s vývojem zabezpečení podnikového prostředí. Jak bylo uvedeno na začátku tohoto článku, pryč jsou doby, kdy stačil pouze firewall. Tím se zabývala i naše další otázka. Je vidět, že respondenti o rozvoji bezpečnosti uvažují. Pouze čtvrtina je se stavem svého zabezpečení spokojena a já předpokládám, že je to jistě z důvodu nedávného rozšíření bezpečnostních technologií. Další čtvrtina dotazovaných by rozvoj chtěla, ale bohužel je to pro ně finančně náročné, nebo je těžké přesvědčit o investici ty, kteří o ní rozhodují. To je vzhledem k vysokým cenám těchto technologií pochopitelné, ale je třeba si také uvědomit, jaký dopad by pro organizaci představoval úspěšný kybernetický útok, při kterém by došlo například k úniku citlivých dat kvůli chybějící bezpečnostní technologii.

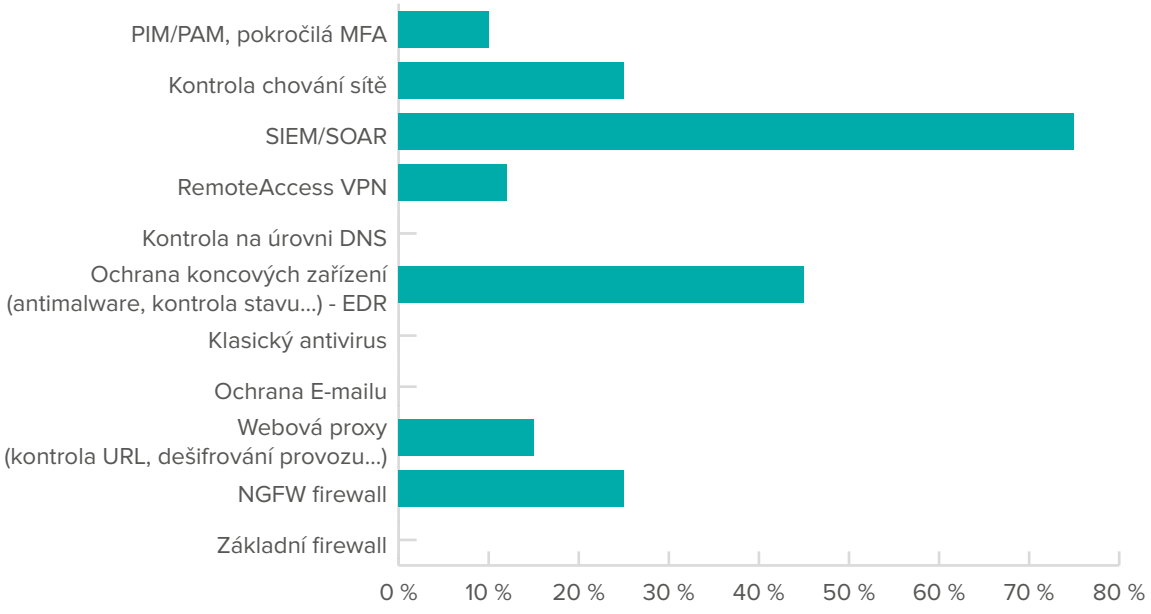
Přemýšlíte nad rozšířením kybernetické bezpečnosti, nebo jste se stávajícím stavem spokojeni?



Většina dotazovaných chce rozšířit stávající technologie o ty chybějící anebo povýšit o nové funkce. Obecně lze říct, že správci chtějí mít větší přehled a snadnější správu. Základní pravidlo v bezpečnosti nejen v oblasti IT je totiž „co nemohu vidět, nebo o čem nevím, proti tomu se nemohu chránit“. Dalším směrem rozvoje je nepochybně ochrana koncových zařízení. Je to dáno právě tím, že stále více lidí pracuje mimo kanceláře a útočníci toho velice rádi využívají. Málokdo má možnost mít domácí síť zabezpečenou tak, jako tu podnikovou. Klasické antiviry také už přestávají stačit na sofistikovaný malware, který je často připraven tak, aby klasickými antiviry prošel. Zde je pak výhodné být připraven a používat pokročilou ochranu proti malware. A jelikož jako správci nemáme často možnost ovlivnit, jak uživatelé chrání svěřená zařízení, je často nutné ověřovat, zda osoba, která žádá o přístup do zabezpečené sítě nebo do kritické aplikace je skutečně tou osobou, kterou tvrdí. Rozšířil se i zájem o multifaktorové ověřování uživatelů a správu přístupu uživatelů.

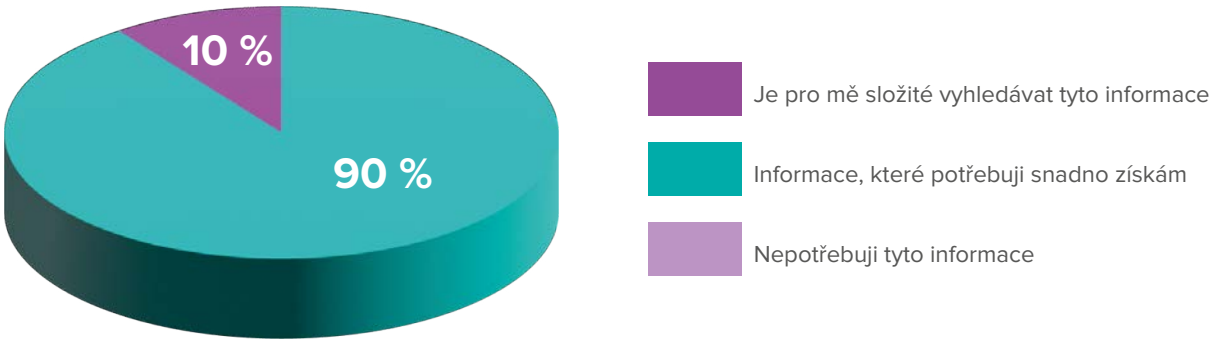
Jako společnost poskytující služby jsme sami zaznamenali i jiný trend. Menší společnosti se stále více zajímají o zabezpečení, ale mnohdy na agendu s tím spojenou nemají vyškolené správce, nebo se jednoduše nechtějí takovými věcmi zabývat. I z tohoto důvodu vznikají tzv. manažované služby, kdy se zákazníkovi poskytne např. ochrana koncových zařízení společně s monitoringem a řešením problémů pomocí lidské síly. I my v Alefu jsme jako odpověď po této poptávce vytvořili službu, díky níž dokážeme zajistit vyšší úroveň zabezpečení i s lidským přístupem v případě řešení problémů.

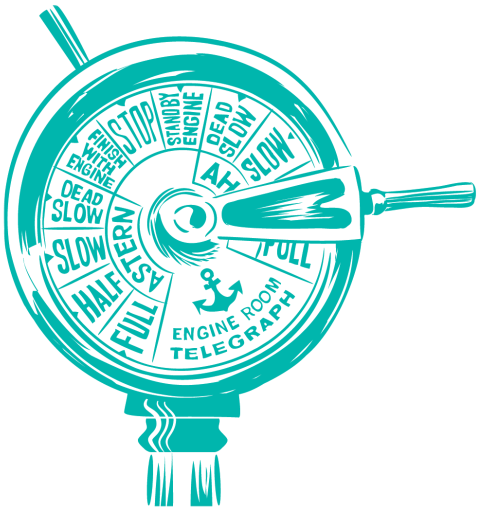
Jakým směrem, případně jakou technologií byste chtěli svou kybernetickou bezpečnost rozšířit?



Na posledním grafu můžeme vidět, že získávání informací o nových technologiích je pro většinu dotazovaných snadné. Důvodem může být dostupnost informací na internetu. Výrobci či vývojáři těchto technologií se často snaží co nejvíce potenciálním zákazníkům zviditelnit, a tak mít před konkurencí navrch. Nezávislé společnosti, jako je například Gartner, je porovnávají a nabízejí objektivní informace o těchto produktech široké veřejnosti.

Je pro vás jednoduché získat informace o novinkách a trendech v kyberbezpečnostních technologiích?





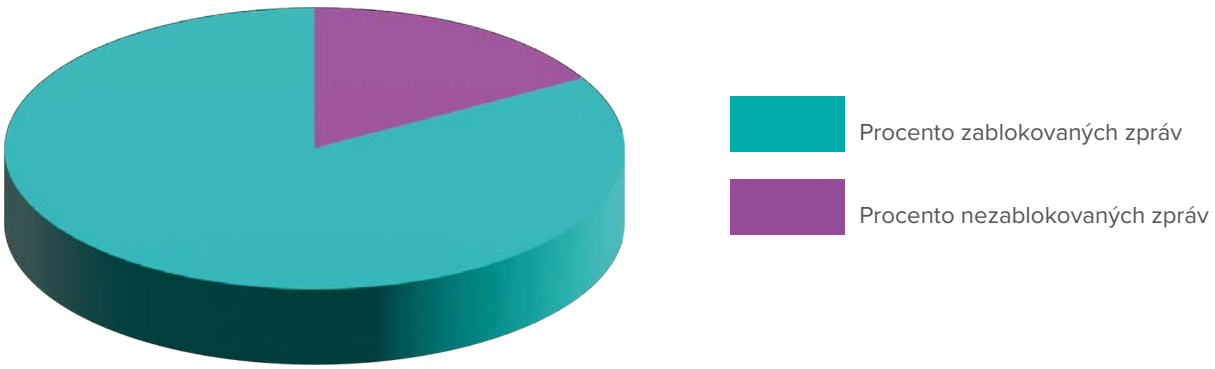
Analýza dat z e-mailových bran

Milan Habrcetl

Tato část analýzy probíhala nad daty příchozích e-mailových zpráv, které byly přijaty vybranými e-mailovými branami v roce 2021.

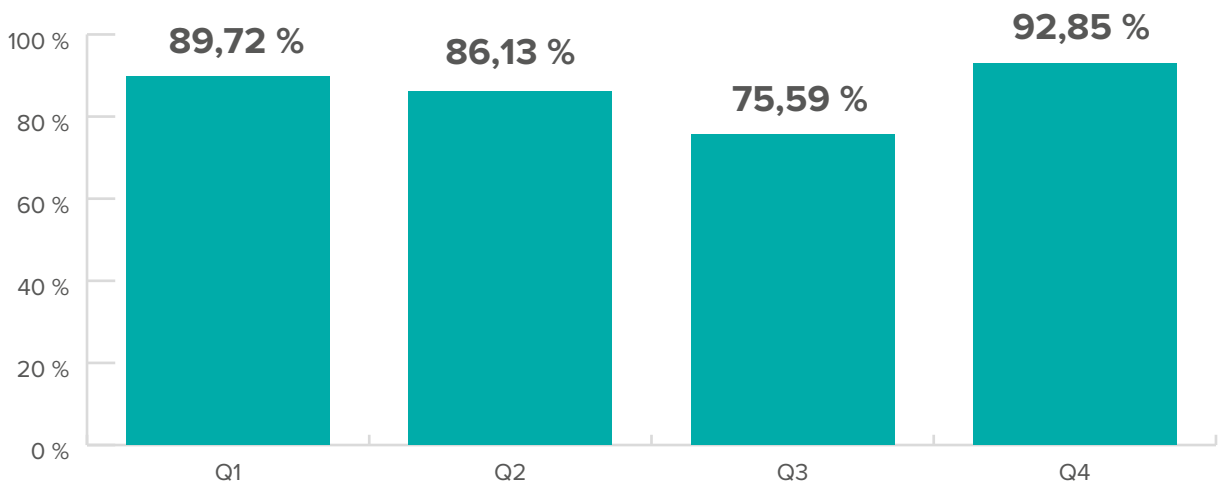
Za celý rok 2021 bylo zablokováno více než 88 procent všech příchozích e-mailových zpráv. Oproti předchozímu roku se jedná o nárůst počtu zablokovaných e-mailových zpráv, avšak jedná se o téměř stejnou hodnotu jako v roce 2019, tedy před situací spojenou s pandemií.

Zablokované vs. nezablokované e-mailové zprávy



V každém čtvrtletí roku 2021 bylo e-mailovými branami zablokováno průměrně 86 procent e-mailových zpráv. Nejvíce e-mailových zpráv bylo blokováno v posledním čtvrtletí (říjen, listopad, prosinec), kdy procento blokovaných zpráv dosáhlo téměř 93 procent.

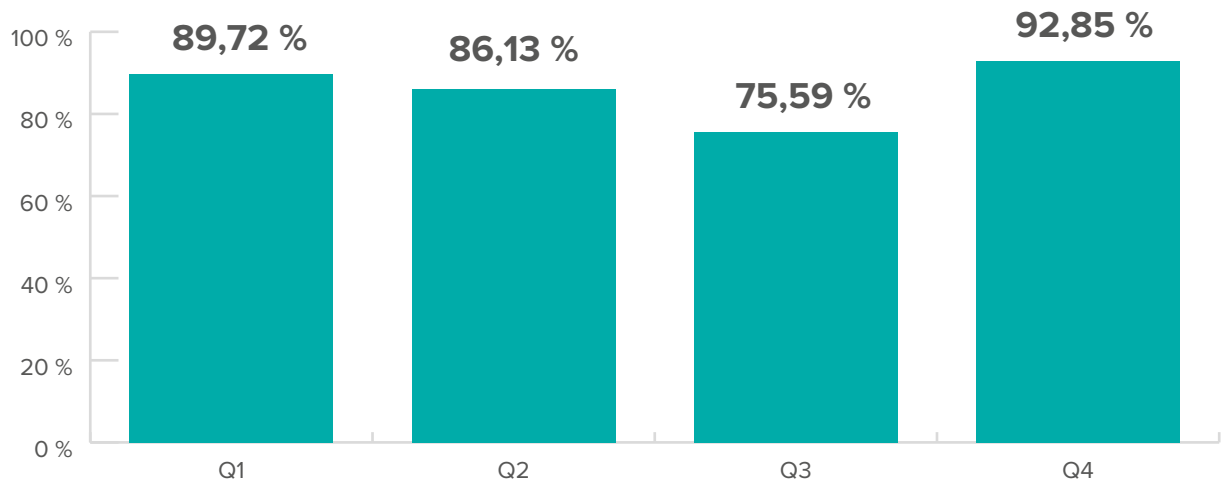
Procento zablokovaných e-mailových zpráv v jednotlivých čtvrtletích



Po agregaci dat do jednotlivých čtvrtletí lze vypozorovat významný nárůst blokovaných e-mailových zpráv mezi třetím a čtvrtým čtvrtletím roku 2021. Důvodem jsou s největší pravděpodobností vánoční svátky a konec roku a všechny přípravy spojené s těmito svátky. V tomto období jsou uživatelé často méně pozorní a také očekávají příchozí balíčky, faktury apod. Útočníci tohoto tedy tradičně využívali tím, že odesílají velké množství škodlivých e-mailových zpráv, aby zvýšili své výdělky.

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

Procentuální rozdělení všech zablokovaných e-mailů do jednotlivých čtvrtletí



Období dovolených a pokles počtu zablokovaných e-mailových zpráv

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

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

Analýza důvodu blokace e-mailových zpráv

Při analýze důvodů blokace e-mailových zpráv na e-mailových branách jsme zjistili, že téměř všechny (přes 98 procent) zablokované e-mailové zprávy byly zablokovány na základě informací z reputační databáze o serveru, ze kterého e-mailová zpráva přišla. V reputační databázi je serverům přiděleno skóre a pokud je serveru přiděleno nízké nebo negativní skóre, pak je komunikace z tohoto serveru zablokována.

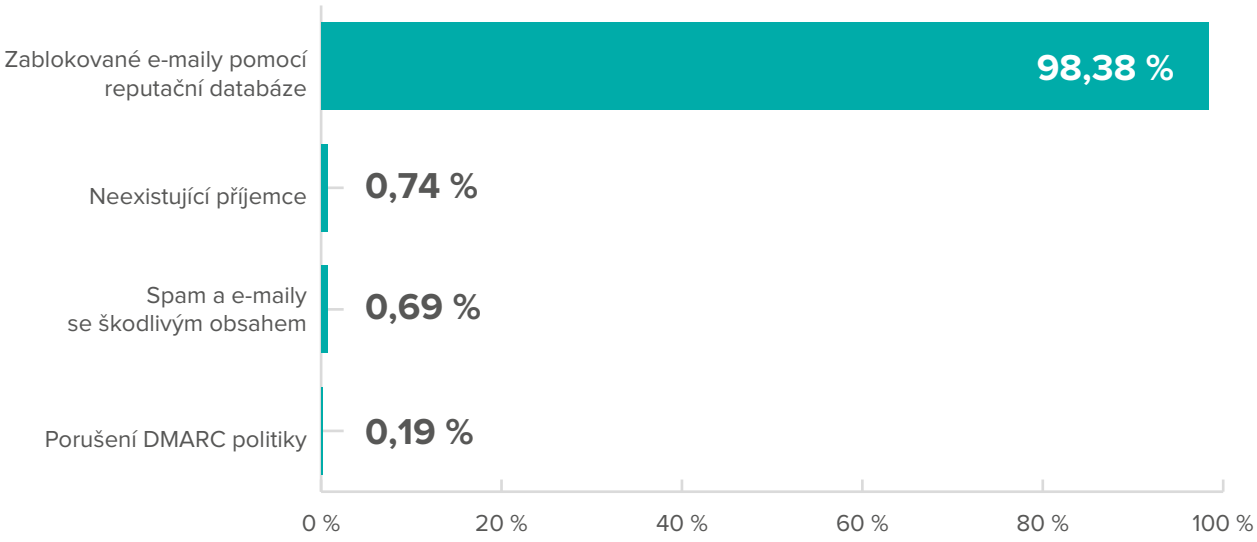
Necelé 1 procento zablokovaných e-mailových zpráv byla zablokováno kvůli tomu, že e-mailové adresy příjemců těchto zpráv neexistují, často se v tomto případě jedná o překlep v zadávání e-mailových adres. Také se může jednat o e-mailovou adresu, která v minulosti existovala, ale byla smazána, a útočníci ji mají stále uloženou v seznamech, případně je již neexistující adresa stále k dispozici na webových stránkách.

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

obsahem měl přílohu, která obsahovala škodlivý software.

Téměř čtvrt procenta zablokovaných e-mailových zpráv bylo blokováno kvůli porušení DMARC politiky, která byla nastavena u doménového jména v adrese odesílatele (legitimní i podvržený) e-mailové zprávy.

Zablokované e-mailové zprávy podle kategorií

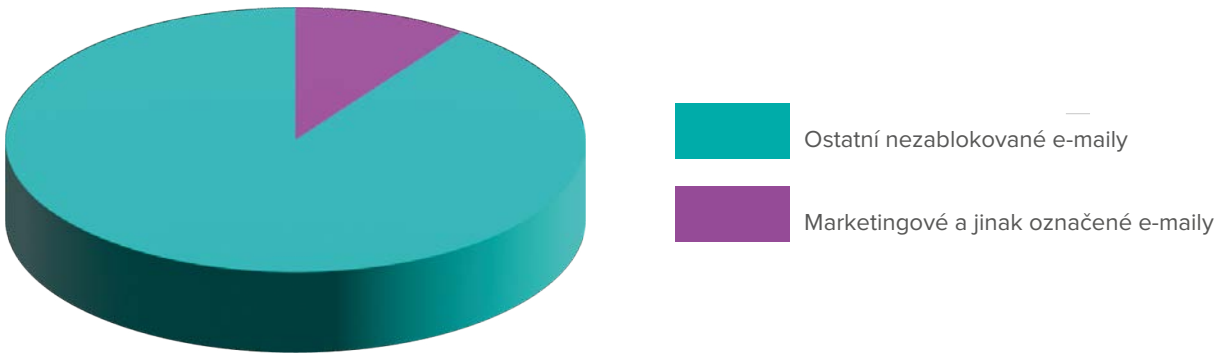


Marketingové a jinak označené e-mailové zprávy (Graymail)

E-mailové brány jsou obvykle také schopny identifikovat a označovat e-mailové zprávy s marketingovým obsahem či zprávy ze sociálních sítí. Často jsou tyto typy e-mailových zpráv nazývané jako „Graymail“, protože někteří uživatelé považují tyto zprávy za nevyžádanou poštu, někteří si ale naopak tuto poštu vyžádali.

Tyto zprávy se tedy pohybují v „šedé zóně“ mezi spamem a legitimním e-mailem. Proto se nedá jednoznačně určit, jestli se jedná o nevyžádanou poštu. Tyto e-mailové zprávy se tak automaticky neblokují, ale jen nějakým způsobem označují, například vložením textu „[Marketing]“ do předmětu e-mailové zprávy. Takto označených e-mailových zpráv bylo v námi získaném vzorku dat z e-mailových bran téměř 10 procent z celkového počtu nezablokovaných e-mailových zpráv.

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



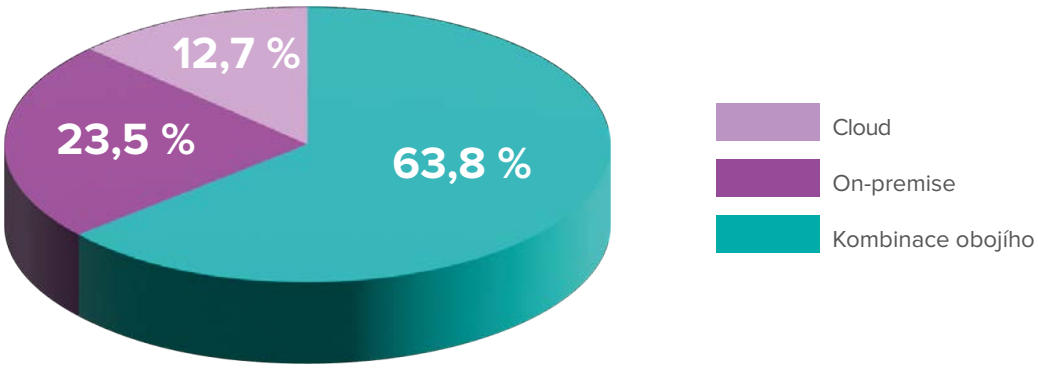
Zabezpečení webových aplikací

Oleksandra Kocyba

Webové aplikace již dlouhá léta nejsou pouze doménou internetových prohlížečů či speciálních „těžkých“ klientů. Webové aplikace nebo HTTP či HTTPS protokol je dnes zastoupen téměř všude. Od klasických webových aplikací, přes mobilní aplikace, streamovací a komunikační služby či komunikace propojující podniky a jejich podnikové aplikace, až po ovládání výrobních linek. Bezpečnost webových aplikací a jejich ochrana před hrozbami se stává pro mnohé organizace kritickou. V tomto reportu se podíváme, jak řeší bezpečnost a ochranu před hrozbami české organizace prostřednictvím dat získaných z dotazníkového šetření mezi klienty Alef Group.

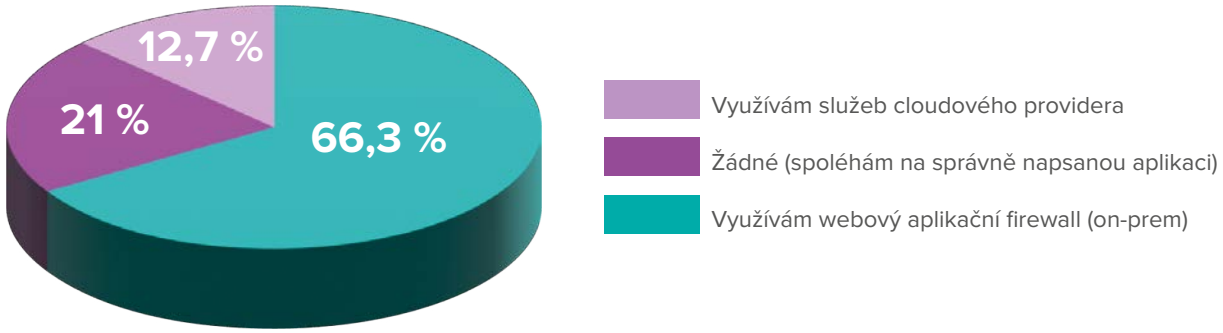
Prostředí, ve kterém aplikace běží, ovlivňuje způsob, jak organizace může zajistit její bezpečnost. V obecné rovině rozlišujeme prostředí, ve kterých běží aplikace, na prostředí tradiční, cloudová a hybridní. V tradičním prostředí běží aplikace ve vlastním datovém centru či pronajatém racku (často označován jako on-premise). Druhé zmíněné prostředí cloudu je specifické tím, že organizace využívá pouze technologické možnosti, které jsou v cloudu dostupné. Posledním prostředím je kombinace obojího, tedy on-premise a cloudu nazývané také jako hybridní prostředí. Téměř dvě třetiny respondentů využívají pro své aplikace hybridní prostředí, přibližně čtvrtina zůstává u klasického modelu on-premise a více než desetina využívá plně cloudového prostředí.

Který model využíváte pro služby a aplikace?



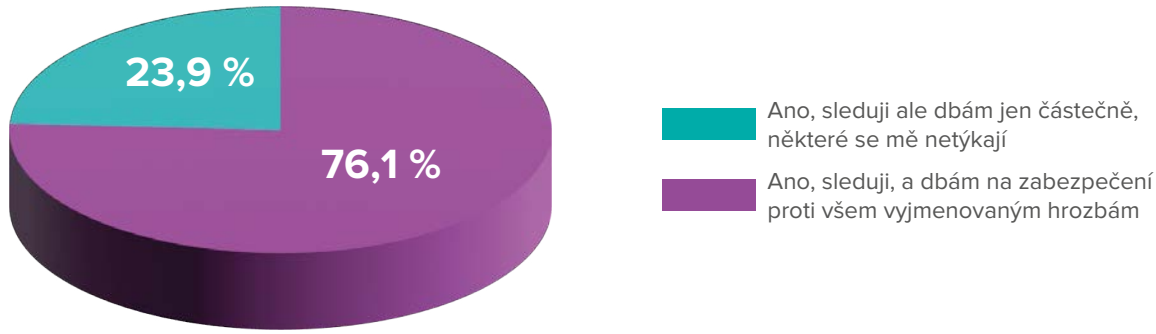
V návaznosti na předchozí dotaz je skladba odpovědí respondentů velmi podobná. Tedy dvě třetiny respondentů využívají webový aplikační firewall, přibližně pětina spoléhá na bezpečný vývoj aplikace a necelých třináct procent využívá pro zabezpečení svých aplikací služeb poskytovatele cloudu. Vyvíjet bezpečné a „neprůstřelné“ aplikace by mělo být vždy cílem. Tomuto cíli se však lze pouze přiblížit, protože aplikace budou vždy obsahovat chyby nebo nebude prostor chyby objevit a opravit. Budou existovat chyby logické, chyby v kódu či chyby v knihovnách třetích stran. Za těmito chybami je vždy lidský faktor. Útoky, které využívají dosud neznámých chyb (zranitelností), se nazývají Zero Day útoky. Vzpomeňme na kritické zranitelnosti a relativně jednoduše proveditelné zranitelnosti HEARTBLEED, SHELLSHOCK nebo čerstvě Log4j zveřejněné v prosinci roku 2021.

Jak řešíte zabezpečení Vašich aplikací?



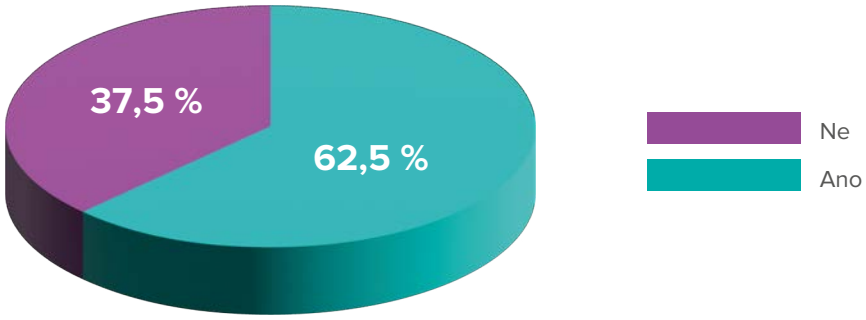
Mluvíme-li o zabezpečení webové aplikace, existuje celá řada metodologií popisujících postupy pro bezpečný vývoj a testování webové aplikace. Jeden z nejznámějších projektů je OWASP (Open Web Application Security Project). Tato nadace sdružuje tisíce vývojářů, kteří se podílí na tvorbě projektů zabývajících se bezpečným vývojem webových aplikací. Jedním z nich je také seznam 10 nejčastějších hrozeb a rizik webových aplikací OWASP Top Ten. Tento seznam hrozeb a rizik je periodicky sestavován a reflektuje aktuální vývoj a trendy. V průběhu času se OWASP Top Ten seznam stal prakticky standardem, podle kterého se může řídit každá organizace a zaměřit se tak na nejdůležitější oblasti v zabezpečení svých aplikací. Data získaná z dotazníkového šetření tomuto nasvědčují, neboť všichni respondenti odpověděli na otázku, zda sledují seznam OWASP Top Ten kladně a dbají na zabezpečení proti všem nebo alespoň části ze zranitelností.

Sledujete pravidelně seznam 10 největších zranitelností aplikací OWASP Top Ten?



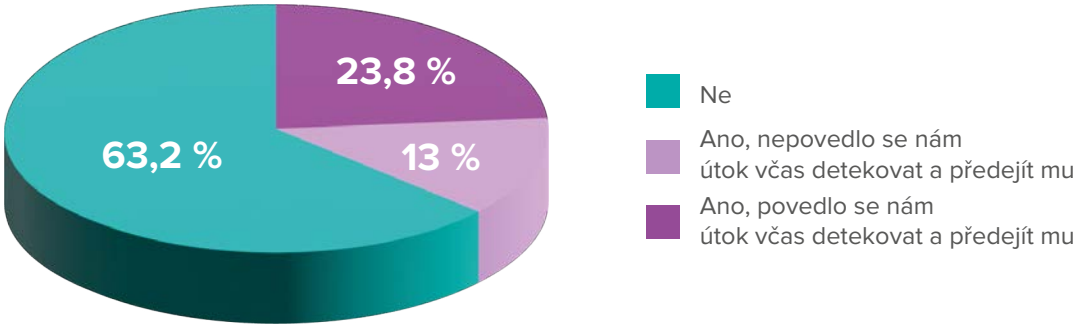
V závěrečné části reportu se zaměříme na útoky proti webovým aplikacím, za kterými ve velkém procentu případů stojí roboti, tedy automatizovaní klienti (označovaní také jako boti). Tyto automatizované klienty můžeme rozdělit do dvou skupin. První z nich jsou neškodné roboty (vyhledávače, srovnávače, marketingové nástroje, SEO apod.), jejichž přínosy jsou pro dnešní elektronické obchodování a konzumaci internetu důležité a mnohdy nepostradatelné. Dalším typem robotů jsou spíše nežádoucí nebo vyložené škodlivé skupiny robotů. Mezi tyto škodlivé můžeme zařadit tzv. DoS boty. Útočník malwarem kompromitované počítače či systémy ovládá za účelem vykonávat zadané instrukce a operace k provedení DoS útoků (Denial of Service). Větší skupině takovýchto botů se říká botnet a jsou často využívány k zahlcení webových aplikací velkým množstvím provozu (distribuovaný DoS útok – DDoS), který může mít za následek výpadek aplikace a její znepřístupnění legitimním uživatelům. Podle výsledků dotazníkového šetření řeší ochranu proti DDoS útokům přibližně 63 % dotazovaných organizací.

Řešíte DDoS ochranu Vašich aplikací?



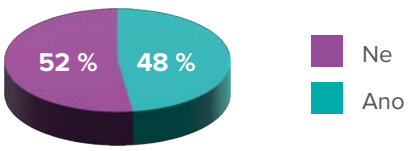
Obdobně 63 % organizací se s DDoS útoky na aplikace v roce 2021 nesetkalo. Kolem 24 % organizací se poté s DDoS útokem setkalo a úspěšně jej detekovaly, naopak 13 % organizací s detekcí a ochranou úspěšných nebylo.

Setkali jste se v posledním roce s DDoS útokem na Vaše aplikace?

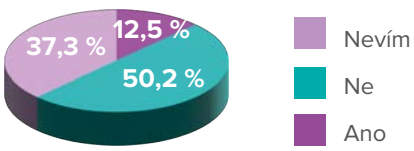


Dalším typem nežádoucích či škodlivých robotů se kterými se organizace často setkávají, jsou boti se schopností interagovat s webovými aplikacemi jako klasický „lidský“ uživatel. Jedná se o automatizované skripty, které se pokouší různými způsoby kopírovat stránky a sbírat informace a ceny z webů (content a price scraping), či zneužít nechráněné přihlašovací formuláře, na kterých testují různé kombinace přihlašovacích jmen a hesel nebo kombinace uniklých přihlašovacích údajů (credential stuffing). Podle průzkumu přibližně polovina organizací rozlišuje, zda s jejich aplikacemi interaguje člověk či robot, polovina se poté s útokem robotů na svou aplikaci nikdy nesetkala, přibližně 13 % naopak ano.

Rozlišujete, zda s Vaší aplikací interaguje člověk či robot?



Setkali jste se někdy s útokem botů na Vaši aplikaci?



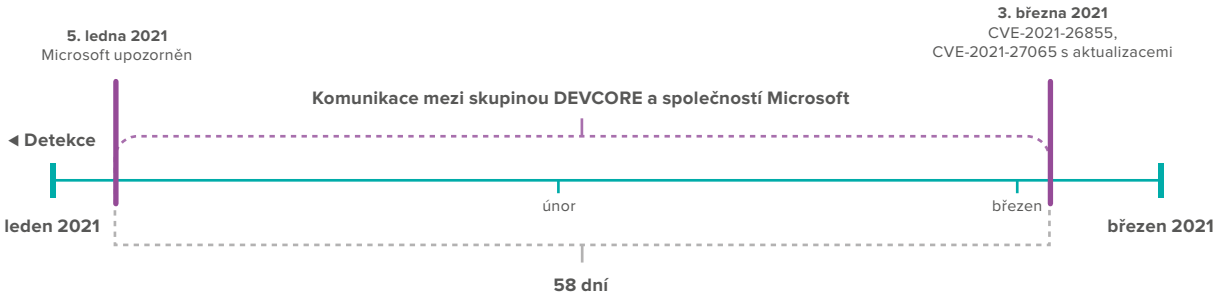
Z šetření jednoznačně plyne fakt, že se respondenti vážně zabývají zabezpečením webových aplikací, neboť význam webových aplikací v posledních téměř dvou dekádách významně vzrostl a stal se nástrojem pro komunikaci a nástrojem obchodní činnosti komerčních organizací.

Zero-Day zranitelnosti ve světě Windows

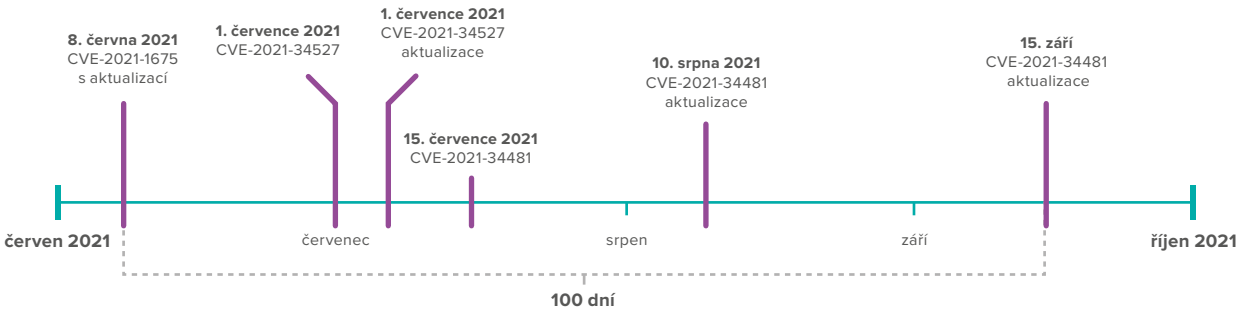
David Horák

Rok 2021 byl z pohledu Zero-Day zranitelností pro společnost Microsoft náročným obdobím, neboť právě v tomto roce jich bylo hned několik. My si v rámci tohoto reportu čtyři z nich blíže popíšeme a zobrazíme si je na časové ose.

Zřejmě největší dosah měla zranitelnost zvaná **ProxyLogon**, která se nacházela v produktu Microsoft Exchange. Tuto zranitelnost objevila skupina DEVCORE a skládala se hned z několika zneužitelných chyb. První z těchto chyb byla objevena už v prosinci roku 2020 s označením **CVE-2021–26855**. Tato chyba umožňovala útočníkovi vzdáleně obejít ověřovací mechanismus a tím získat administrátorská privilegia. V kombinaci s druhou chybou s označením **CVE-2021–27065** objevenou také v prosinci roku 2020 mohl útočník následně zapsat do systému libovolný soubor v podobě například web shellu, skrze který následně bylo možné vzdáleně spouštět libovolné příkazy. Výše uvedené zranitelnosti byly společnosti Microsoft nahlášeny skupinou DEVCORE 5. ledna 2021, následně probíhalo ověřování této zranitelnosti společností Microsoft. K jejímu potvrzení došlo 8. ledna 2021. Aktualizace s potřebnými doporučeními následně společnost Microsoft vydala až 3.března 2021. Náprava této zranitelnosti tedy trvala **58 dní**. Vzhledem k množství serverů Microsoft Exchange dostupných přímo z internetu měla tato zranitelnost pro mnoho společností drtivé následky.

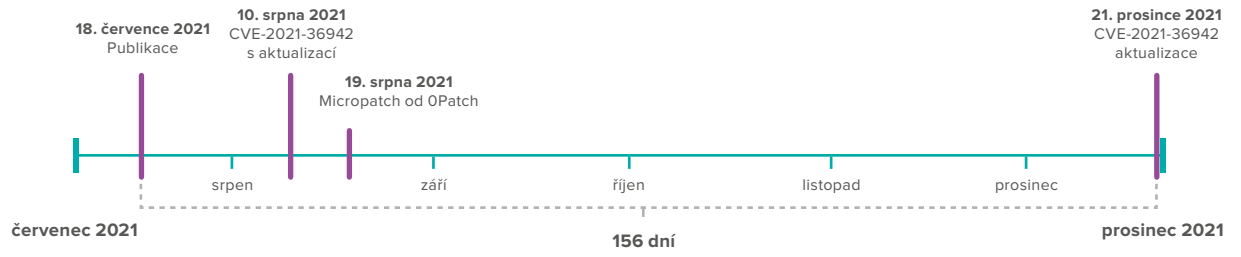


Další zranitelnost zvaná **PrintNightmare** přinesla mnoho strastí pro tiskové služby v rámci Active Directory. Dění okolo této zranitelnosti začalo 8. června 2021, kdy společnost Microsoft vydala **CVE-2021–1675** s aktualizacemi opravujícími zneužitelnou chybu ve službě Print Spooler. Tato chyba umožňovala eskalaci oprávnění na úroveň systému běžnému uživateli za pomocí nahrání maligního ovladače a byla zneužitelná pouze lokálně. Vydaná aktualizace probudila v mnoha výzkumnících zájem o tento typ zranitelnosti. Jedním z nich byl například Benjamin Delpy. Tento zájem vedl k sérii „bojů“ mezi novými aktualizacemi a novými zneužitími. 1. července 2021 společnost Microsoft vydala **CVE-2021–34527** s následnými aktualizacemi 6. července 2021 opravujícími další chybu ve službě Print Spooler, která umožňovala zmíněnou instalaci maligního ovladače a ovládnutí systému vzdáleně. Nicméně ani tato aktualizace dny zranitelnosti neukončila a výzkumníci našli jiné cesty jejího zneužití. To vedlo 15. července 2021 k vydání nového **CVE-2021–34481** upozorňující na tuto chybu. Aktualizace pro **CVE-2021–34481** společnost Microsoft vydala 10. srpna 2021, která bohužel danou chybu plně neopravila. **CVE-2021–34481** byla kompletně opravena až ve vlně pravidelně vydávaných aktualizací 14. září 2021. Kompletní náprava trvala **100 dní** a během těchto procesů aktualizování se mnoho společností potýkalo s problémy s tiskem.



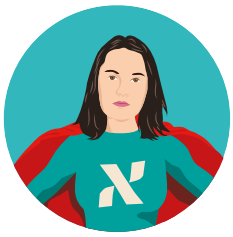
Jednou z menších, ale rozhodně zajímavých byla zranitelnost zvaná **SeriousSam/HiveNightmare**. Tato zranitelnost spočívala v chybně nastaveném Access Control Listu (ACL) na systémové složce Config, která obsahuje například databázi lokálních účtů včetně jejich tajemstvích – Security Account Manager (SAM). Chybně nastavené ACL umožňovalo neprivilegovanému uživateli přistoupit k těmto citlivým souborům v rámci složky Config. Tato zranitelnost byla nalezena výzkumníkem Jonasem Lykem, který na ni narazil náhodou při zkoumání bezpečnosti Windows 11. Tato zranitelnost se v operačních systémech Windows 10 nacházela již od buildu 1809. Zranitelnost byla detekována a publikována 19. července 2021. Společnost Microsoft vydala **CVE-2021–36934** s aktualizací 20. července 2021. U této zranitelnosti byla náprava dodána za pouhý **1 den,** nicméně zde zůstává obrovské riziko v zálohách tzv. Shadow Copy pořízených pomocí Volume Shadow Copy služby před aktualizováním systému. Neboť tyto zálohy v operačním systému zůstanou s chybně nastaveným ACL i po aktualizování a měly by tak být smazány.

Poslední zranitelnost, na kterou se v rámci reportu podíváme je **PetitPotam**. Tuto zranitelnost objevil výzkumník označovaný na Twitteru jako @Topotam77. Zranitelnost umožňovala útočníkovi donutit Encrypting File System Remote Protokol (EFSRPC) na vzdáleném zařízení k ověření vůči cílové službě, kterou byly certifikační služby. Díky tomu si byl útočník schopný vydat certifikát pro zneužité vzdálené zařízení, kterým mohl být i doménový řadič. Zranitelnost byla detekována a publikována 18. července 2021. Společnost Microsoft vydala 10. srpna 2021 **CVE-2021-36942** s aktualizacemi, které nicméně danou zranitelnost kompletně neopravily. Mimo společnost Microsoft se opravou dané zranitelnosti zabývala i platforma 0Patch, která vydala aktualizaci 19. srpna 2021. Finální aktualizaci vydala společnost Microsoft až 21. prosince 2021. Náprava této zranitelnosti tedy trvala **156 dní**.



Z výše uvedených čísel vyplývá, že ačkoliv je základním předpokladem včasná aktualizace systému, tak na Zero-Day zranitelnosti musíme naše prostředí na pravidelné bázi připravovat pomocí aktuálních bezpečnostních principů a praktik.

Úroveň šifrování webserverů na českém internetu

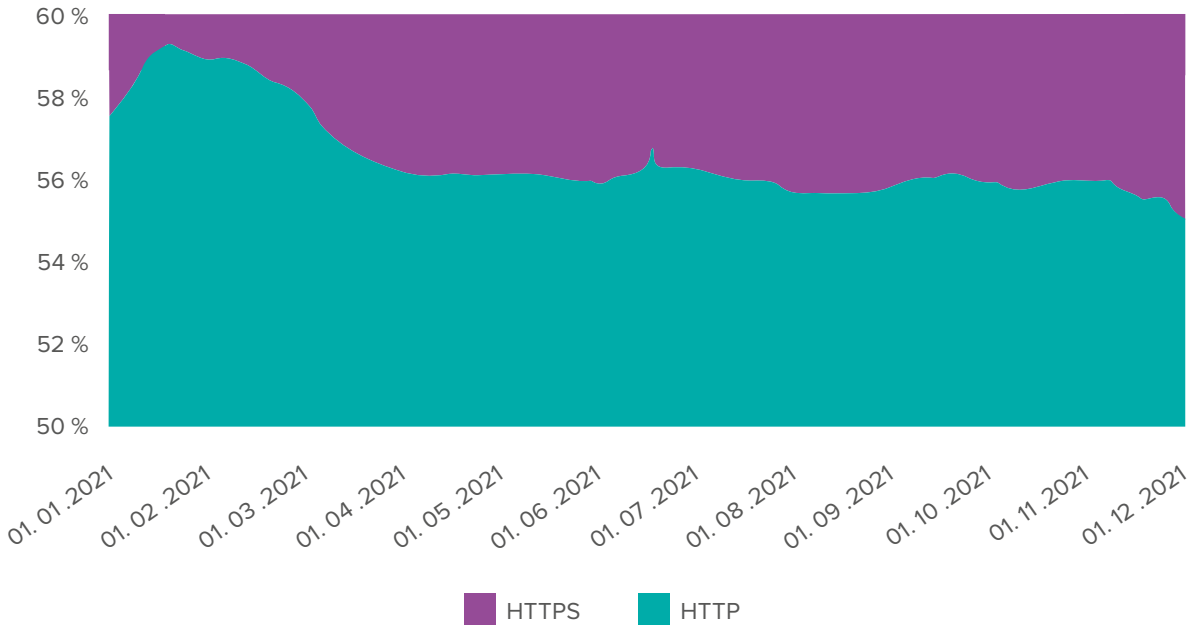


Oleksandra Kocyba

V dnešní době je většina dat, se kterými pracujeme, online. Data k nám pak putují po veřejné síti, kde jsou vystavena riziku odchycení. I z toho důvodu byly vyvinuty protokoly sloužící k šifrování provozu v počítačových sítích. Ve světě webových aplikací se jedná zejména o protokoly TLS (resp. SSL).

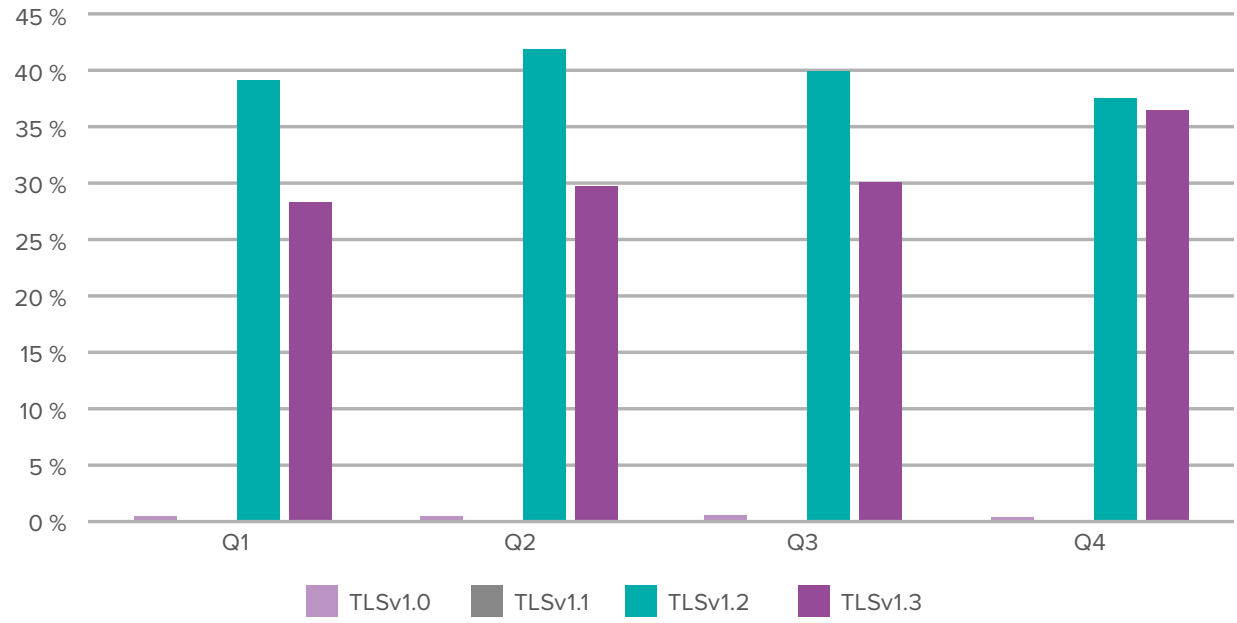
Podle dat nahromaděných za rok 2021 na českém internetu se zaměříme nejprve na poměr webserverů, které podporují šifrovanou či nešifrovanou komunikaci. Je potřeba zmínit, že podpora HTTP i HTTPS není vzájemně exkluzivní. Mnoho webových serverů má otevřený port 80 (HTTP) i port 443 (HTTPS). Port 80 se využívá pro prvotní navázání spojení s klientem, načež je klient přesměrován na port 443, kde následná komunikace probíhá šifrovaně.

Poměr služeb HTTP a HTTPS na českém internetu



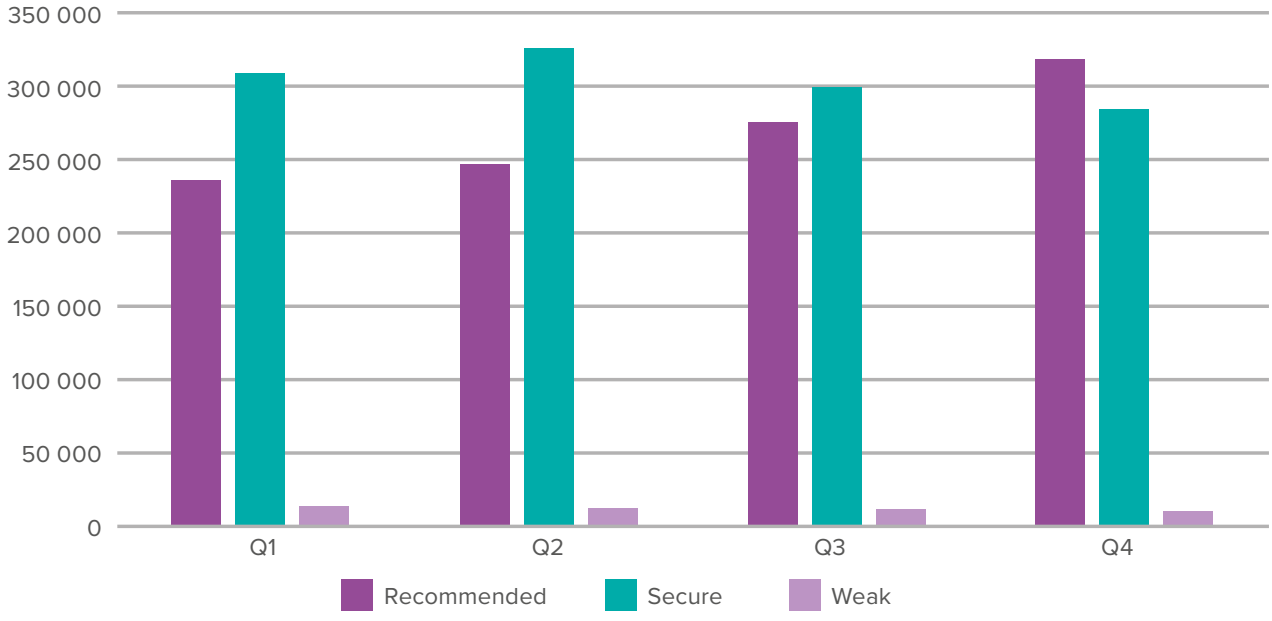
Webová komunikace je šifrovaná pomocí protokolů TLS nebo předchůdce – SSL, jenž obsahuje známé zranitelnosti a z bezpečnostních důvodů by se již neměl používat. Nahradil jej TLS, který prochází vývojem již od roku 1999, od verze TLSv1.0 až po současnou verzi TLSv1.3., přičemž mezi doporučované verze od roku 2020 patří pouze TLSv1.2 a TLSv1.3. Na českém internetu se tato doporučení dle dat nahromaděných za rok 2021 projevují. V průběhu roku docházelo k postupnému snižování webových serverů podporujících TLSv1.0 (na 0,4 % ze všech detekovaných webserverů) a TLSv1.1 (na 0,003 %) a k nárustu serverů podporujících TLSv1.3. Na grafu níže je znázorněn proměnlivý počet dostupných webserverů a podporovaných verzí TLS.

Podpora verzí TLS na webových serverech - 2021



K zajištění šifrované komunikace však nestačí určit jen verzi TLS/SSL. Při navazování komunikace se klient a server musí domluvit na šifrovací sadě, která určuje nejen algoritmus určený k šifrování komunikace, ale i algoritmus pro výměnu klíčů, algoritmus sloužící k autentizaci a MAC algoritmus zajišťující integritu přenášených dat. Tato šifrovací sada poté určuje, jak bezpečná, kompatibilní a rychlá bude komunikace se serverem. Šifrovacích sad je velké množství a pro tento report bylo vybráno 26 nejčastěji používaných sad, rozdělených 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.

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.

Trendy v oblasti bezpečnostního vzdělávání

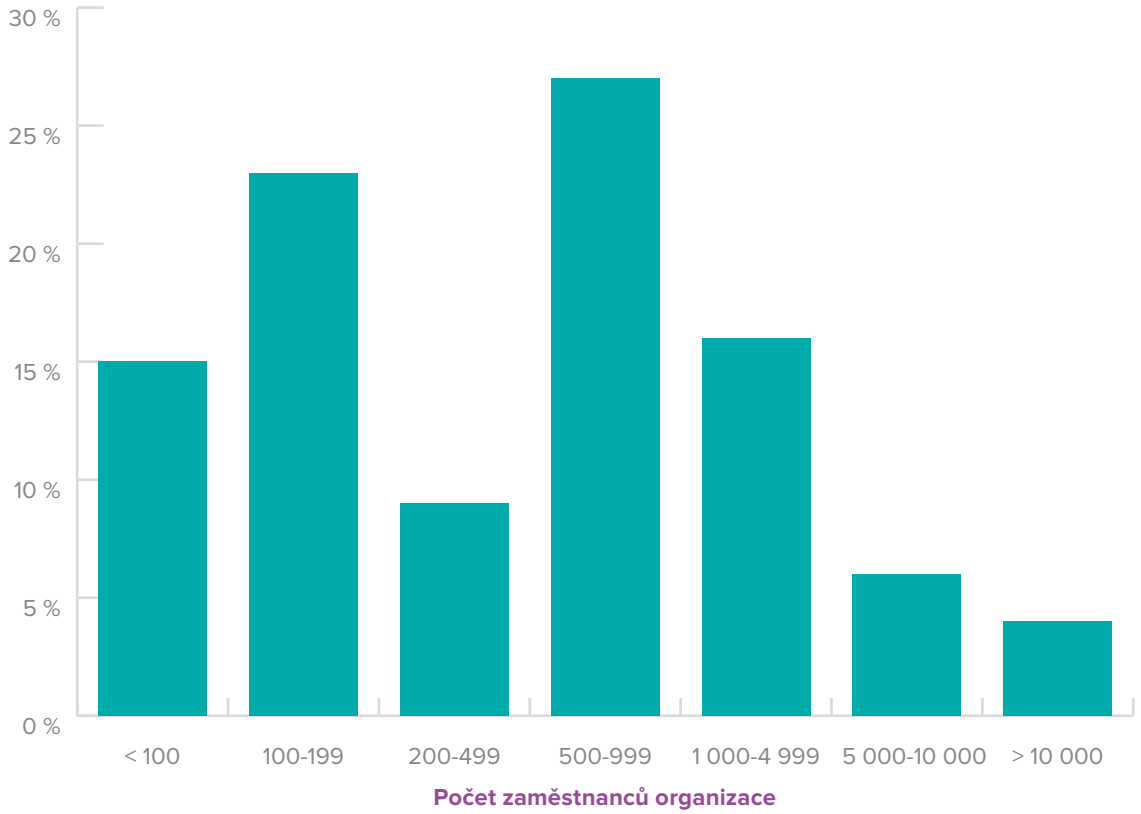
Radek Švadlenka

Vzdělávání zaměstnanců v oblasti kybernetické bezpečnosti se stalo neodmyslitelnou součástí bezpečnostní strategie všech organizací, které si uvědomují rizika související s hrozbami, jež neoddělitelně patří ke kyberprostoru. Stále propracovanější metody útočníků v kombinaci s novými vektory útoků mohou prověřit reálnou odolnost bezpečnostních opatření kteréhokoliv subjektu jak v komerčním prostředí, tak i v oblasti veřejné sféry. Investice do technických bezpečnostních prostředků jsou jistě na místě, nicméně bez odpovídající znalosti zaměstnanců ztrácejí na účinnosti.

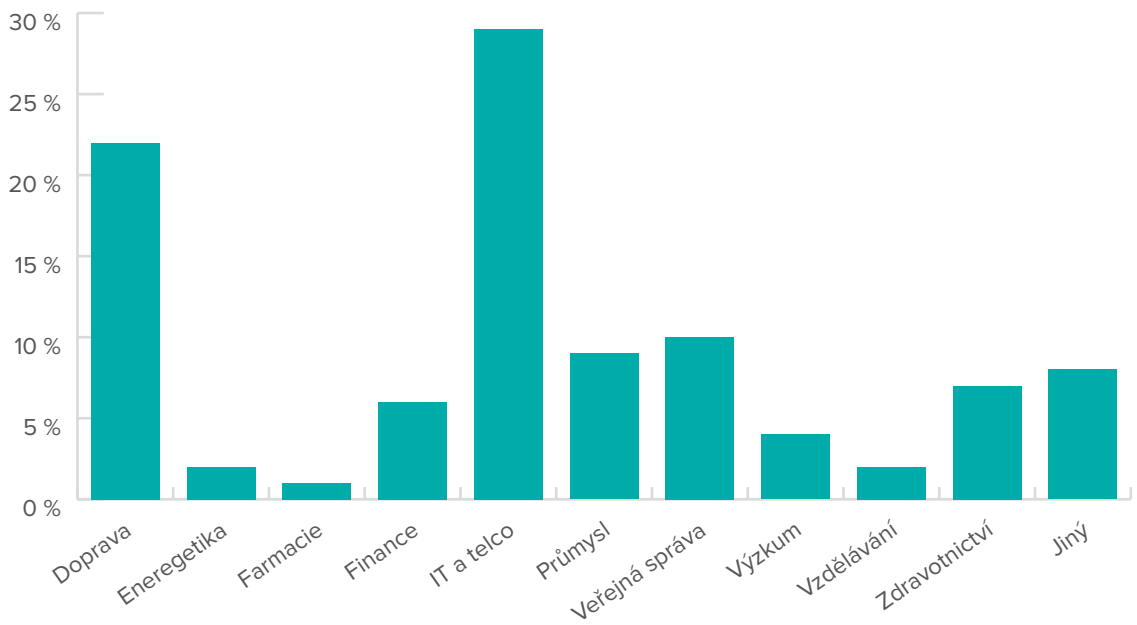
Není tedy žádným překvapením, že zákon o kybernetické bezpečnosti vyžaduje od povinných subjektů realizovat bezpečnostní opatření v podobě stanovení plánu rozvoje bezpečnostního povědomí, jehož cílem je zajistit odpovídající vzdělávání a zlepšování bezpečnostního povědomí uživatelů, administrátorů a osob zastávajících bezpečnostní role.

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 2021 s ohledem na plánovaná opatření pro rok 2022. Do většiny aktivit organizací v loňském roce výrazně zasáhla pandemie Covid-19. O to zajímavější je meziroční srovnání plánovaných a realizovaných aktivit v oblasti vzdělávání v kybernetické bezpečnosti. Průzkumu se zúčastnilo bezmála sto organizací různých zaměření a velikostí, jak je vidět z grafů níže. Výzkumný vzorek je velmi podobný tomu z loňského roku, a to jak s ohledem na počet respondentů, tak i v poměru zastoupení organizací dle oboru a velikosti.

Procentuální zastoupení organizací dle velikosti

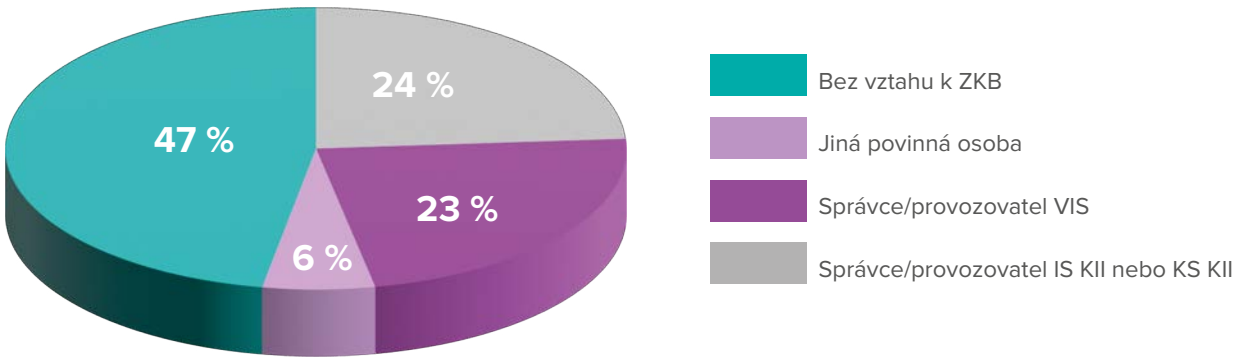


Procentuální zastoupení oragnizací dle oboru

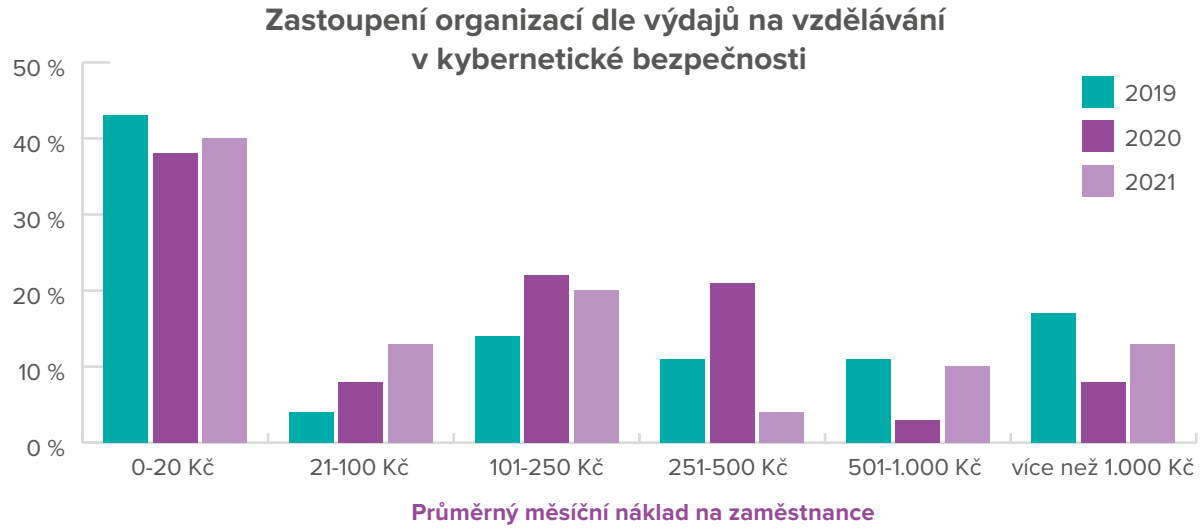


Aby interpretace jednotlivých výstupů nebyla zkreslena, je třeba upřesnit, že více než polovina respondentů průzkumu se řadí mezi povinné subjekty podle zákona o kybernetické bezpečnosti, jak ilustruje následující graf.

Vztah organizací k ZKB



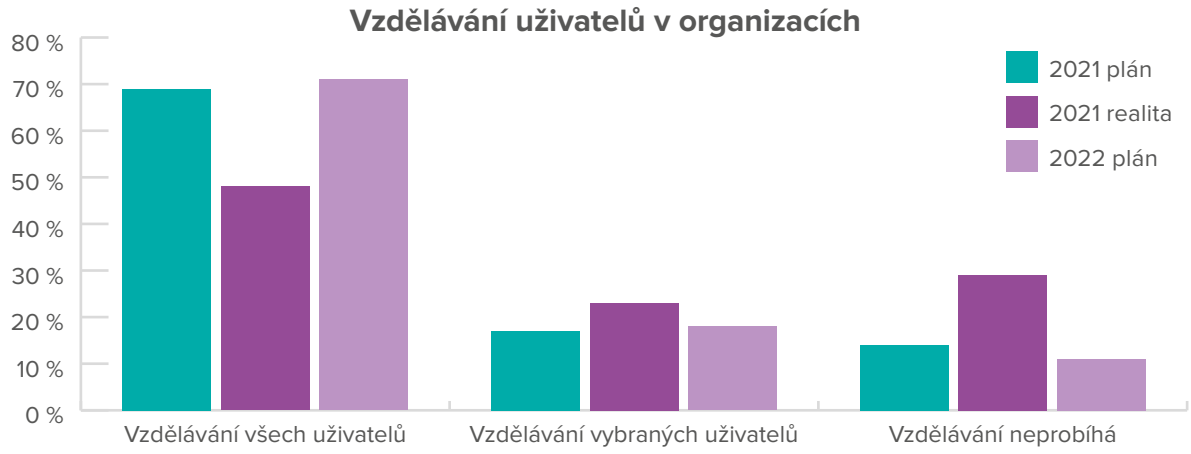
Realizaci vzdělávacích aktivit v oblasti kybernetické bezpečnosti je možné zajistit za pomoci jak interních, tak i externích zdrojů v podobě prezenčních školení či e-learningových nástrojů. Vzhledem k omezením souvisejících s pandemií musela být zejména prezenční školení nahrazena jinou formou např. virtuálních školení pomocí online platforem. V grafu níže je možné sledovat porovnání investovaných prostředků do vzdělávání v letech 2019, 2020 a 2021. Jako pozitivní trend je možné označit postupný návrat organizací do před pandemického stavu, kdy investovaly do vzdělávacích aktivit více nez 500 Kč. Celkem logicky pak meziročně klesl počet firem investujících do vzdělávání mezi 251 Kč až 500 Kč na zaměstnance. Bohužel, množství organizací s ochotou investovat do vzdělávání zaměstnanců minimální nebo dokonce žádné prostředky se meziročně drží stále na vysoké úrovni.



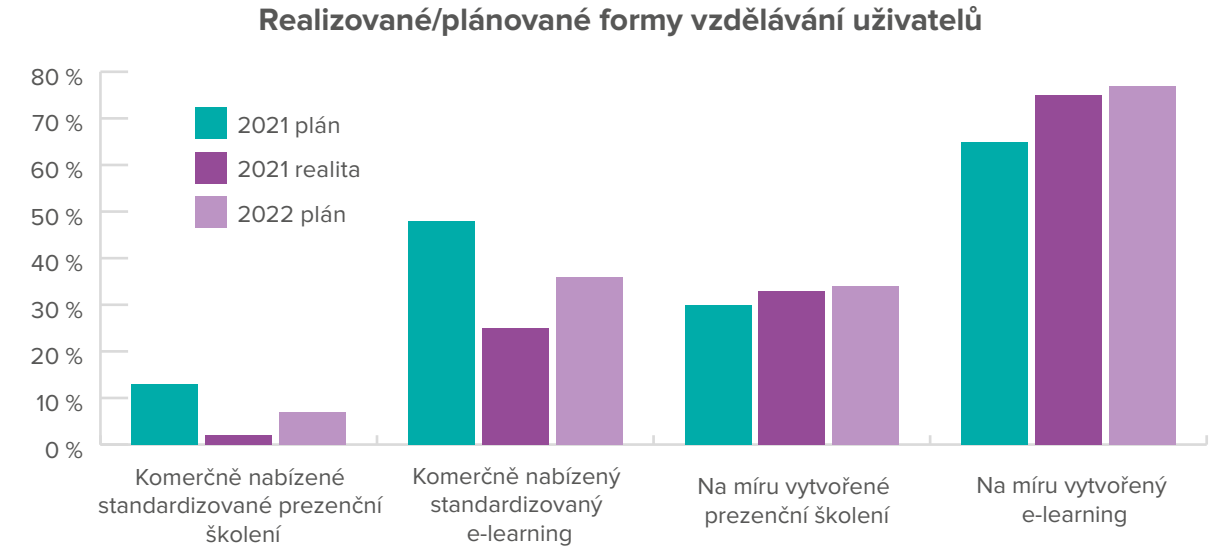
Vzdělávání uživatelů – realita versus plán

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 2020 pro vzdělávání všech uživatelů nebyly v roce 2021 zdaleka naplněny. Naopak počet organizací, kde vzdělávání vůbec neprobíhá je dvojnásobný oproti plánu z předchozího roku.

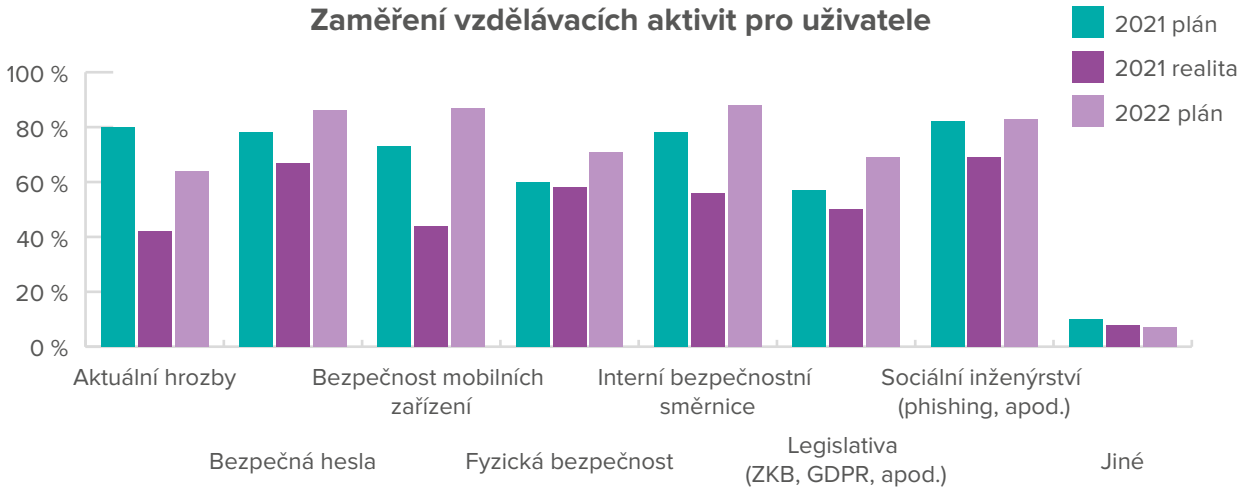
Pozitivní trend je vidět alespoň u vzdělávání vybraných uživatelů, kde realita lehce předčila plán z roku 2020. Co se týče plánu vzdělávacích aktivit pro rok 2022, v podstatě se hodnotově příliš neliší od plánu pro rok 2021 s mírně rostoucím trendem. Jaká však bude realita je těžké predikovat zejména s ohledem na další faktory (např. konflikt na Ukrajině), které mohou významně ovlivnit výsledky.



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, celkem logicky došlo v roce 2021 k omezení prezenčních standardizovaných školení ve prospěch e-learningových řešení oproti plánu stanoveném na konci roku 2020. Naproti tomu na míru vytvořená prezenční školení byla často realizována pomocí online platformy a zde se realita nijak zvlášť neodchýlila od plánu. Z odpovědí týkajících se plánu na rok 2022 je možné predikovat pokračující trend migrace k e-learningovým nástrojům a realizace standardizovaných prezenčních kurzů bude přímo úměrná protiepidemickým opatřením vlády a potenciálnímu riziku nákazy zaměstnanců. Zajímavým fenoménem je také postupný odklon od standardizovaných forem trainingu zaměstnanců směrem k „na míru“ vytvořeným.



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 bezpečných hesel a sociálního inženýrství. Naopak méně organizací se soustředilo na oblast aktuálních hrozeb a bezpečnosti mobilních zařízení. Plán zaměření vzdělávacích aktivit pro uživatele na rok 2022 se příliš neliší od plánu pro rok 2021 s mírně rostoucím trendem téměř ve všech oblastech výzkumu.

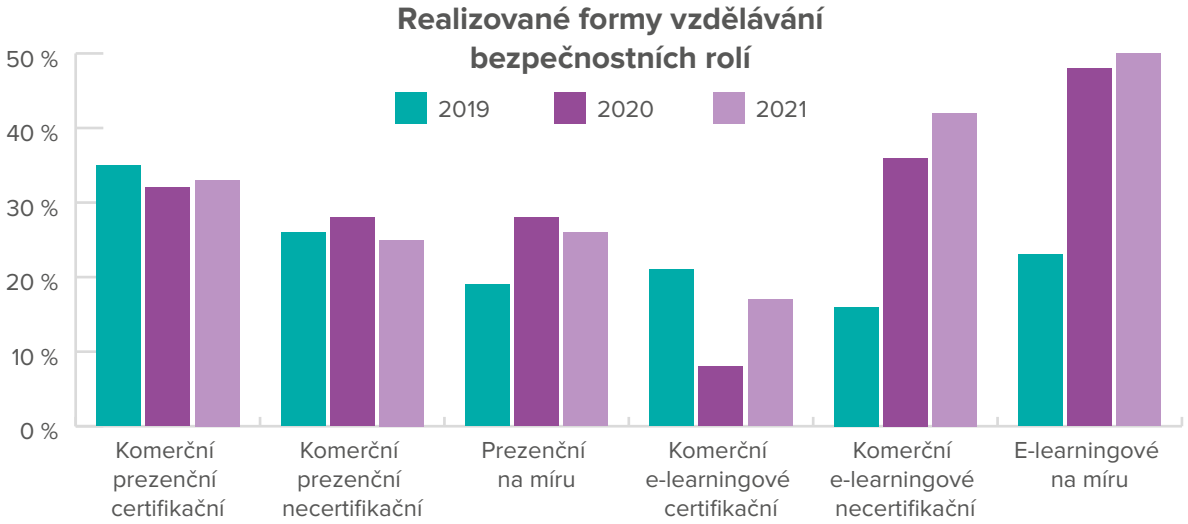


Velice efektivní, ale zároveň také mezi zaměstnanci málo oblíbené, jsou aktivity spojené s ověřováním znalostí a ostražitosti uživatelů v oblasti kybernetické bezpečnosti. Obrázek níže ilustruje aktuální rozložení využívání těchto aktivit u sledovaného vzorku subjektů.

Bohužel celkový trend spojený s těmito aktivitami nevykazuje pozitivní vývoj. Ověřování znalostí formou testů využívá meziročně stále méně organizací, byť rozdíly jsou v řádu jednotek procent. Počet organizací zaměřujících se na ostražitost uživatelů pomocí simulovaných phishingových útoků klesl meziročně o 10 %. Negativní trend je možné pozorovat i na počtu organizací, kde žádné ověřování neprobíhá. Hodnota za rok 2021 dokonce překonala výsledek z roku 2019. Mírný optimismus může být spojen alespoň s výhledem na rok 2022, kdy 76 % organizací plánuje zavést alespoň nějaké aktivity zaměřené na ověřování znalostí uživatelů v oblasti kybernetické bezpečnosti.

Vzdělávání odborných rolí

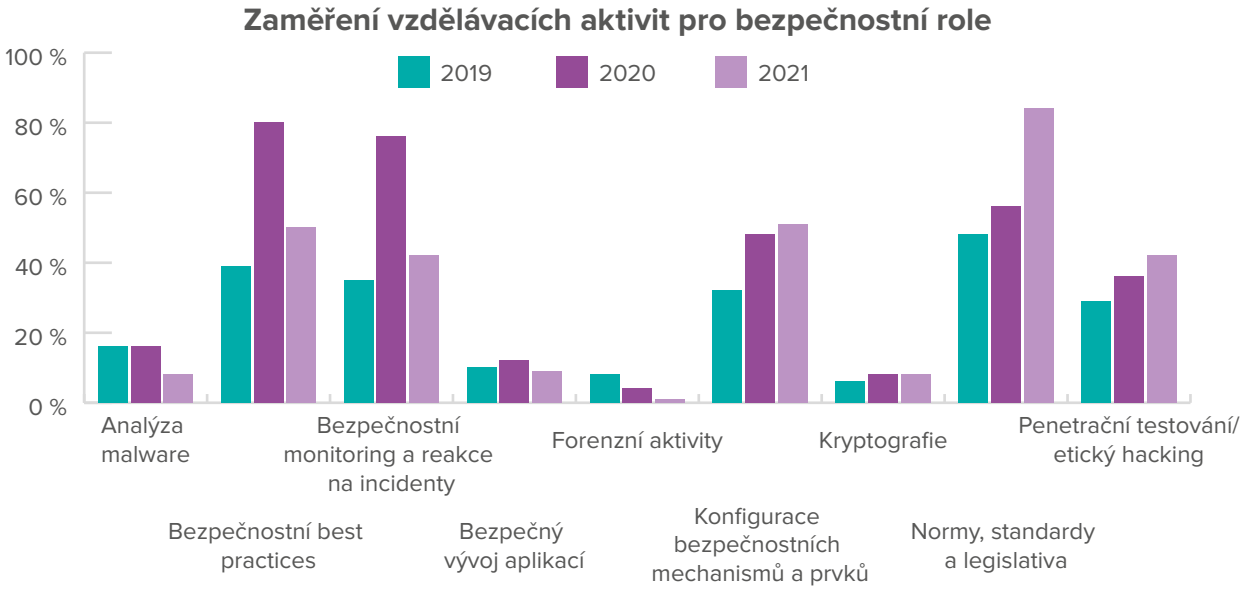
Zaměstnanci na pozicích administrátorů a bezpečnostních expertů jsou klíčoví pro plánování, realizaci a udržitelnost bezpečnostních pravidel v organizaci. Jejich znalosti a dovednosti mohou mít významný dopad na efektivitu zvládání bezpečnostních incidentů. Na grafu níže je zobrazeno meziroční porovnání realizovaných forem vzdělávání bezpečnostních rolí v organizacích. Na první pohled je patrný meziroční růst ve všech kategoriích e-learningových kurzů včetně certifikačních. Naopak prezenční formy vzdělávání bezpečnostních rolí zaznamenaly lehký pokles, s výjimkou kategorie komerčních certifikačních kurzů. Obecně prezenční vzdělávací aktivity v roce 2021 byly tlumeny probíhající epidemií a související legislativou.



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 konfigurace bezpečnostních mechanismů a penetrační testování a etický hacking. Každé z výše vyjmenovaných zaměření vzdělávání bylo využito v roce 2021 téměř polovinou respondentů.

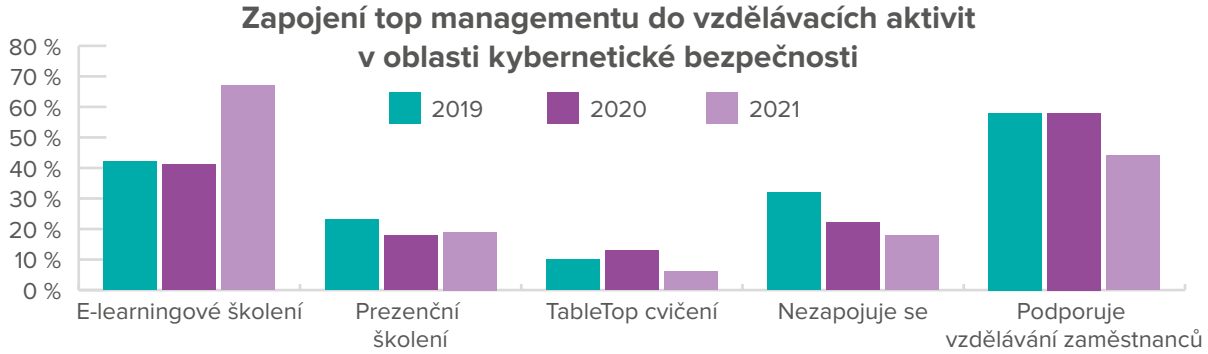
Mezi dlohodobě „slabá“ témata z hlediska vzdělávání bezpečnostních rolí je možné zařadit oblasti kryptografie, forenzních aktivit a bezpečného vývoje aplikací, které nedosáhly z hlediska využití nad testovacím vzorkem hranice deseti procent, jak je patrné z grafu níže.



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. Pozitivní zprávou je, že meziročně klesá počet manažerů, kteří se vůbec nezapojují do vzdělávacích aktivit. Zároveň výrazně vzrostl 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 souvisí s pandemickou situací. Zajímavým jevem je však významný pokles podpory vzdělávání zaměstnanců ze strany top managementu, a to o více než 10 %.



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 97 % 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, což potvrzují závěry interpretované v předchozí kapitole. Přes 20 % respondentů uvádí omezení zdrojů do kybernetické bezpečnosti a přibližně 40 % organizací prozatím nezavedlo změny oproti stavu před epidemií.

Zabezpečení e-mailové komunikace

Martin Šišmiš

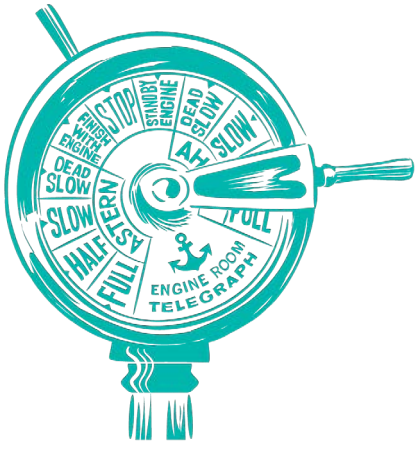
Stejně jako předchozí rok, pojďme se podívat na situaci a data ohledně zabezpečení e-mailové komunikace. Pro přenos dat a zpráv je e-mailovými servery používán aplikační protokol SMTP, který je sám o sobě nešifrovaný. To znamená, že pokud je potencionální útočník schopný kdekoliv po trase zachytávat komunikaci, či spojení přesměrovat přes sebe (on-path útoky), je také schopen si obsah e-mailové komunikace přečíst a dokonce zprávy modifikovat.

Pro ochranu dat při přenosu je možné zvolit dva různé přístupy. První možností je zašifrovat e-mail na počítači odesílatele (**end-to-end šifrování**) za pomocí šifrovacích standardů, které používají asymetrických kryptografických metod (RSA, El Gammal, apod.). Pro příklad lze uvést nejvíce užívané standardy jako PGP, GPG, nebo S/MIME, ale používají se také proprietární standardy. I když end-to-end šifrování, pokud je správně implementováno, nabízí poměrně vysokou úroveň zabezpečení, není úplně jednoduché jej nasadit plošně. Vyžaduje totiž specifické nastavení infrastruktury nebo manuální kroky pro výměnu a nastavení důvěryhodných klíčů. Proto se šifrování na koncových zařízeních využívá spíše sporadicky, nebo pouze v infrastruktuře, která se postará o ověření a distribuci klíčů automaticky. Dalšími nevýhodami této metody je, že SMTP hlavičky jsou stále čitelné a také, že bezpečnostní prvky, jako třeba kontrola obsahu na e-mailovém serveru, nejsou schopné číst samotné tělo e-mailu a najít například škodlivé odkazy.

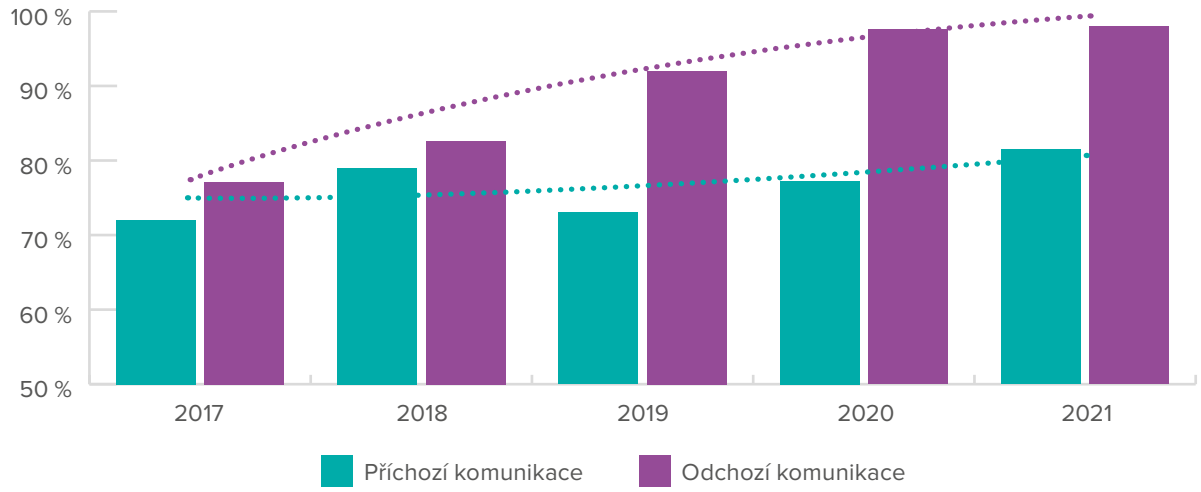
Druhou možností je využití **šifrování na transportní vrstvě,** která funguje v rámci komunikace mezi servery. V tomto případě je nešifrovaná SMTP komunikace zabalena do šifrovaného tunelu. Tento tunel využívá protokolu TLS (Transport Layer Security), a je vytvořený zvlášť pro každou komunikaci mezi 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 nastavené a existuje podpora TLS na serverech po celé trase přenosu dat, pak by měla být zajištěna bezpečnost a důvěryhodnost zprávy při přenosu.
Pokud bychom se chtěli podívat na množství komunikace, která je TLS šifrována u některých globálních poskytovatelů, může nám pomoci například Google. Ten na svých stránkách uvádí procentuální hodnoty šifrování příchozích a odchozích zpráv. Pro rok 2021 je, dle dat společnosti Google, v průměru šifrováno přibližně 92 procent příchozí a 87 procent odchozí e-mailové komunikace.

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 2021 prošlo více jak 100 miliónů zpráv. Následující graf ukazuje, že v rámci použitého vzorku bylo v roce 2021 šifrováno přibližně 95 procent z celkového počtu e-mailové komunikace. Z dat také vyplývá, že přibližně 82 procent příchozí a 98 procent odchozí komunikace je šifrováno.

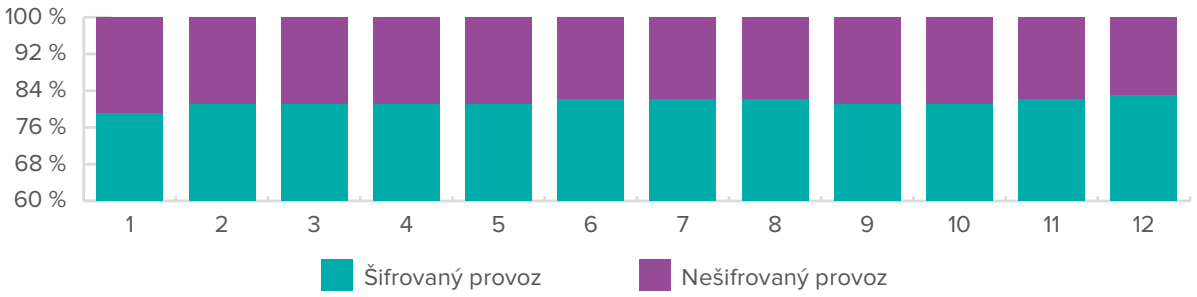


E-mailová komunikace šifrovaná s pomocí TLS

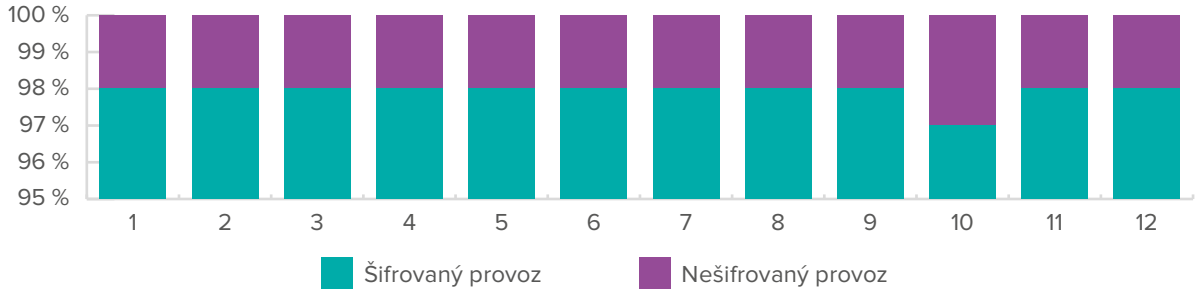


Následující grafy ukazují procentuální zastoupení šifrované a nešifrované komunikace v jednotlivých měsících roku 2021.

Šifrování příchozího e-mailového provozu s pomocí SSL/TLS v roce 2021



Šifrování odchozího e-mailového provozu s pomocí SSL/TLS v roce 2021



V grafech si lze všimnout dlouhodobě stoupajícího trendu, který byl v posledním roce, v porovnání s předchozími, poměrně patrný pro příchozí poštu. V jednotlivých měsících lze i přes kolísání pozorovat lehce stoupající tendenci pro oba směry komunikace. Lze předpokládat, že procento šifrovaného provozu bude i nadále růst, ale je důležité si uvědomit, že se nelze plně spoléhat 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.

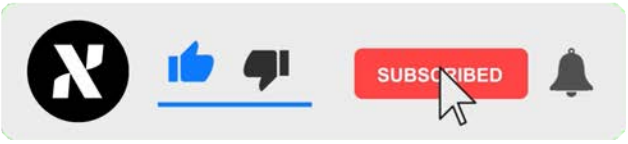
Zdroje:

1: https://transparencyreport.google.com/safer-e-mail/overview

Novinky, rozhovory, doporučení.

Sledujte náš kanál ALEF Security zaměřený na kybernetickou bezpečnost!

YouTube



ALEF

Pro více informací kontaktujte cz-sales@alef.com