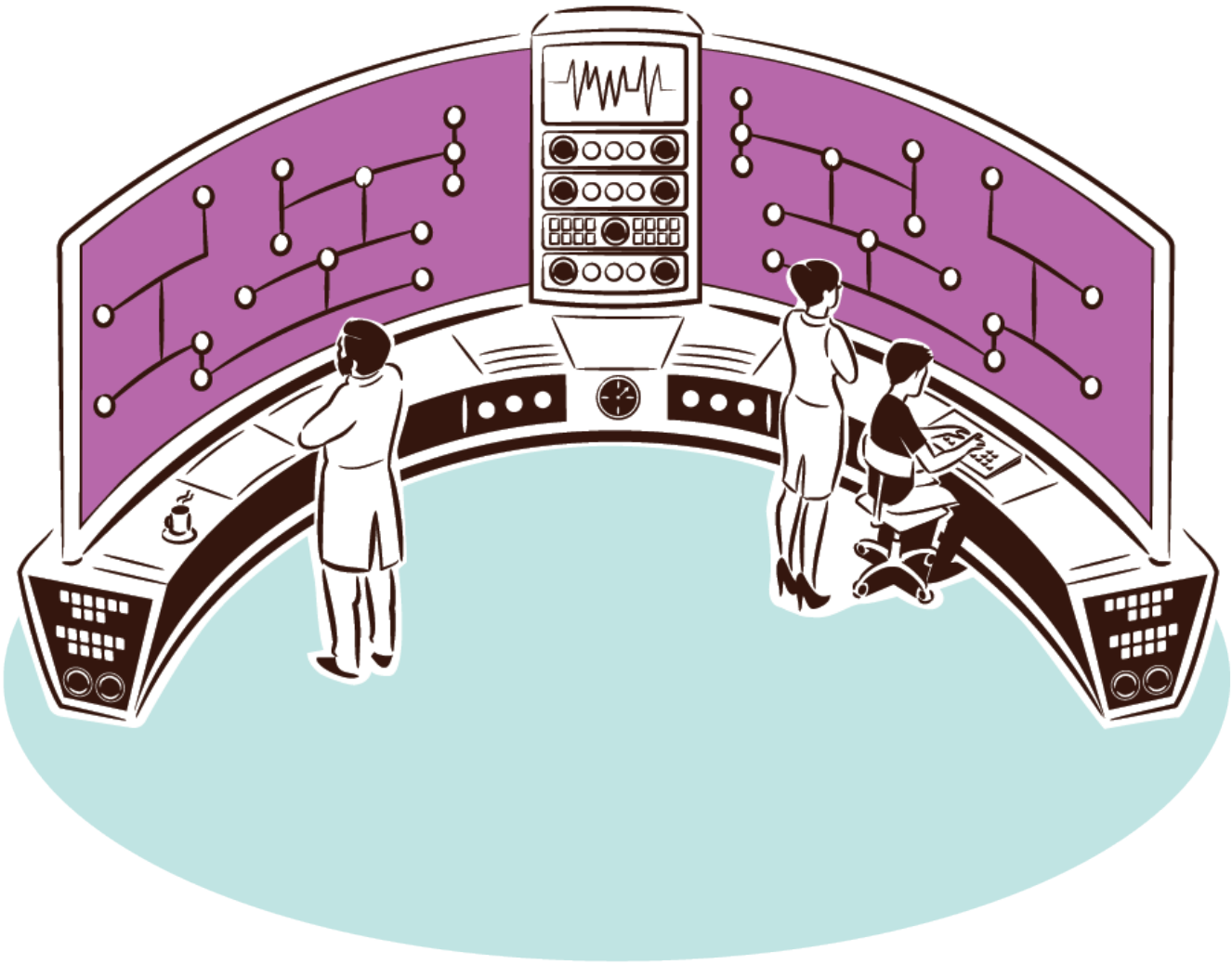
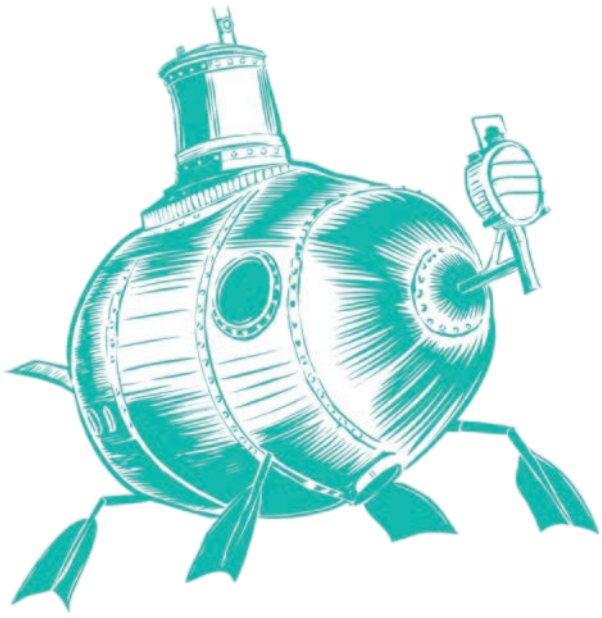
ALEF

Security Report 2020



Trust the Strong
www.alef.com

Obsah



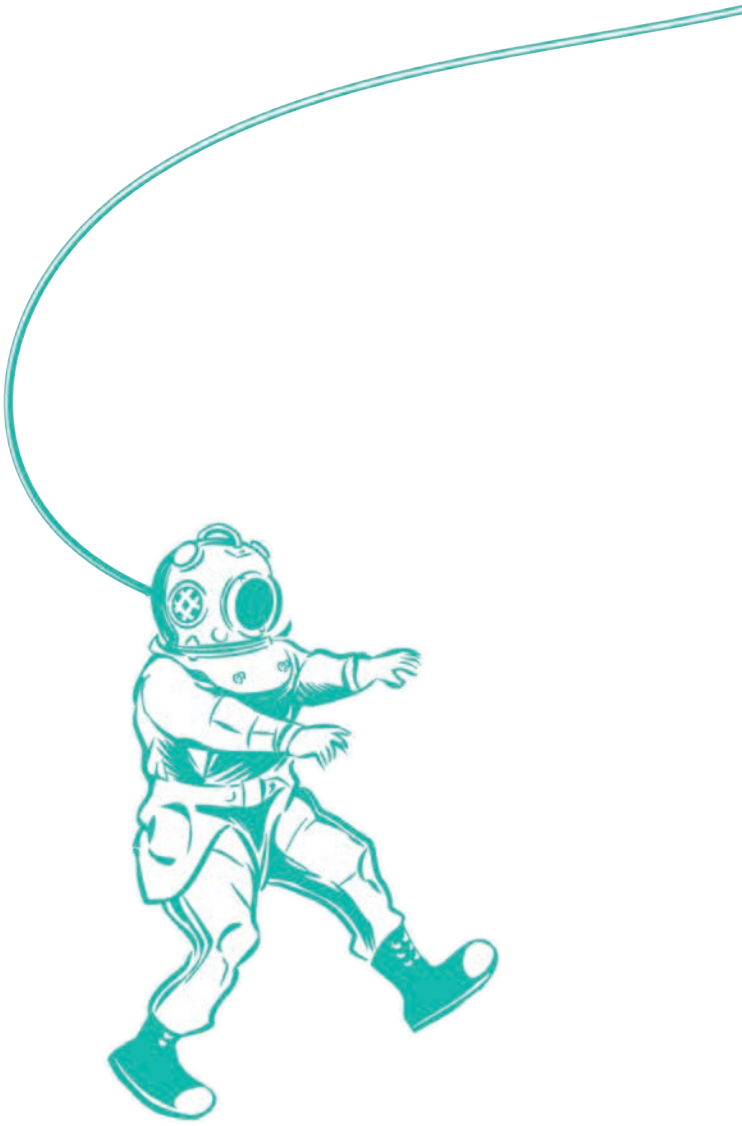
Úvod

Informační technologie si získávají stále citelnější postavení v moderní společnosti a v současnosti snad neexistuje oblast lidského snažení, v níž by nebyly v nějaké podobě užívány. Vedle zvyšování efektivity práce a mnoha jiných pozitiv s sebou však tento vývoj přináší i některé negativní jevy. S narůstajícím počtem počítačových a „chytrých“ zařízení roste rovněž počet systémů, které jsou zranitelné a na něž se mohou útočníci zaměřit. Současně se také zvyšují počty odborně vyspělých škodlivých aktérů i nebezpečnost moderních kybernetických hrozeb.

Abychom měli kontinuální přehled o tom, jak se situace na poli hrozeb, zranitelností a bezpečnostních technologií vyvíjí, sleduje bezpečnostní tým ALEF CSIRT kontinuálně mnoho vlastních i externích datových zdrojů a realizuje výzkumy a analýzy zaměřené na různé aspekty informační a kybernetické bezpečnosti v České republice i v zahraničí. Předložená zpráva, na jejíž přípravě participovali členové tohoto bezpečnostního týmu, ale i další specialisté ALEF Group, obsahuje shrnutí těch nejzajímavějších trendů, které jsme v roce 2019 identifikovali, a analýz, které jsme v jeho průběhu realizovali.

Na následujících stránkách se můžete seznámit s trendy spojenými se šířením škodlivého kódu nebo s vybranými kybernetickými útoky, ale také se situací v oblasti přístupu organizací působících v České republice k bezpečnostnímu monitoringu, penetračním testům nebo vzdělávání uživatelů v problematice kybernetických hrozeb. Můžete se rovněž seznámit s výstupy několika analýz, které jsme v uplynulých 12 měsících realizovali, a zjistit tak, kolik nechráněných průmyslových systémů připojených k internetu se v České republice nacházelo, nebo jak je možné, že některé portály internetového bankovnictví používaly v roce 2019 horší šifrování než pornografické weby.

Tak jako každý rok bychom na tomto místě chtěli poděkovat bezpečnostním týmům CESNET-CERTS a CSIRT.CZ, které nám laskavě poskytly data a statistiky ze svých monitorovacích nástrojů a umožnily nám tak analyzovat a popsat nejen vývoj vybraných aspektů informační bezpečnosti v České republice, ale také na celosvětové úrovni.



Útoky, incidenty, zranitelnosti a šifrování v roce 2019

Jan Kopřiva

Škodlivý kód, průniky do systémů a nové kritické zranitelnosti nás ani v roce 2019 neopustily. Naopak, některé z těchto hrozeb citelně zesílily. Oproti předchozímu roku byl v globálním i českém prostředí citelně častěji detekován ransomware, k němuž se útočníci, po drobném úpadku jeho obliby v průběhu roku 2018, mohutně vraceli. O něco menší zájem byl ze strany útočníků v posledních dvanácti měsících naopak o cryptomining.

Zajímavými trendy v informační bezpečnosti, které se týkají českého prostředí, se zabývá většina příspěvků v tomto reportu. Než se však zaměříme na vývoj hrozeb a útoků, které cílily na Českou republiku, pojďme se alespoň krátce podívat na české trendy v kontextu těch globálních.

Data využitá v této části reportu pochází ze systému PROKI, provozovaného národním bezpečnostním týmem CSIRT.CZ, systému Warden, provozovaného bezpečnostním týmem CESNET-CERTS a z různých bezpečnostních a analytických nástrojů, provozovaných a spravovaných specialisty Alef Nula v rámci vlastních i zákaznických infrastruktur. Oběma výše jmenovaným týmům bychom tímto chtěli ještě jednou poděkovat za to, že nám data ze svých systémů poskytly.

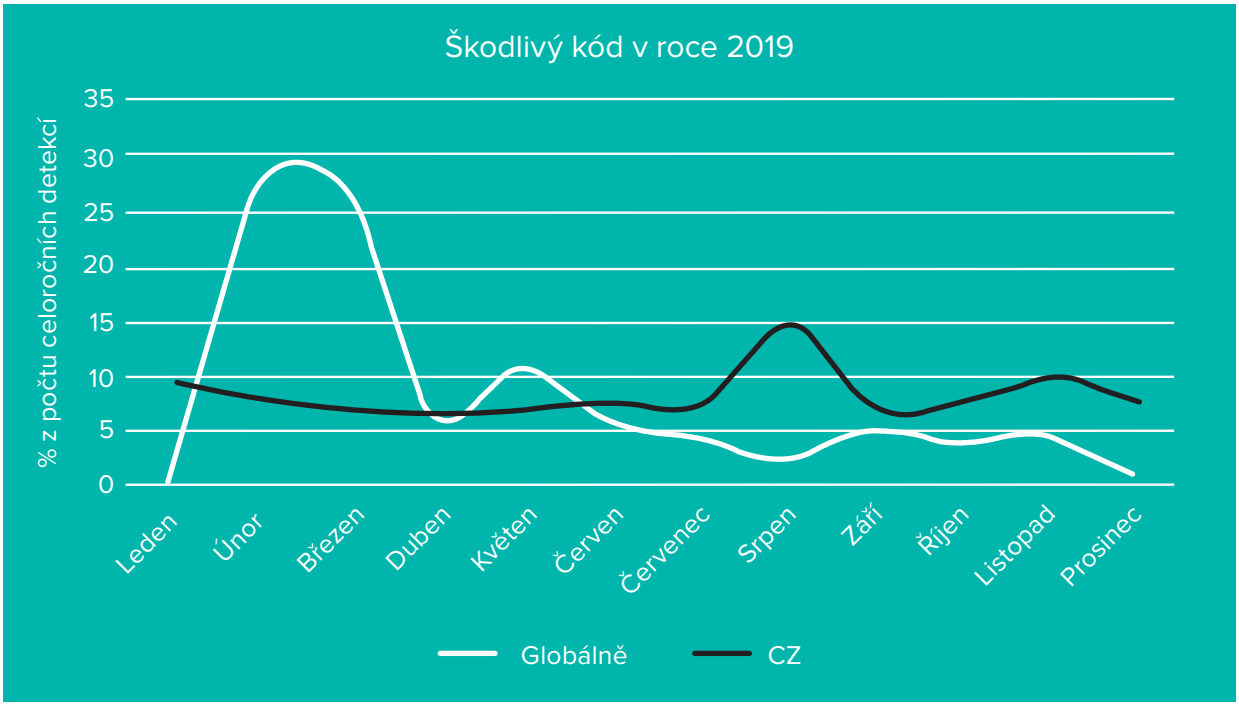
Vzhledem k rozdílu často i mnoha řádů mezi počty evidovaných událostí/útoků pro globální a české prostředí v analyzovaných datech nebylo vhodné porovnávat tyto hodnoty přímo. V rámci všech níže uvedených grafů jsou tak, pokud není uvedeno jinak, namísto absolutních hodnot porovnávána procentuálních rozdělení za rok detekovaných událostí/útoků do jednotlivých měsíců.

Škodlivý kód

Jak bylo zmíněno výše, po krátkém odklonu útočníků od ransomwaru zažíval v roce 2019 právě tento druh škodlivého kódu velmi citelný comeback a to jak na domácí, tak globální scéně. Nešlo ale zdaleka o jedinou hrozbu v podobě malwaru, která nás vloni provázela.

Jak ukazuje následující graf, výskyty detekcí škodlivého kódu v České republice se, s výjimkou posledního čtvrtletí, relativně citelně lišily od globálního trendu. V rámci celosvětových dat je patrný extrémně vysoký nárůst detekcí malwaru v prvním kvartálu. V jeho průběhu bylo, dle analyzovaných dat, detekováno téměř 55 % z veškerého škodlivého kódu identifikovaného v roce 2019. S výjimkou května, na nějž připadlo přes 10,5 % detekcí, byla globální situace po zbytek roku poměrně vyrovnaná. K významným poklesům detekcí došlo pouze v srpnu a na úplném konci roku.

V českém prostředí byl překvapivě právě globálně slabý srpen na detekce škodlivého kódu nejbohatší – v jeho průběhu bylo evidováno přes 14,5 % z celoročního počtu vzorků malwaru. S výjimkou této špičky byla situace v rámci detekcí škodlivého kódu v České republice relativně vyrovnaná v průběhu celého roku.

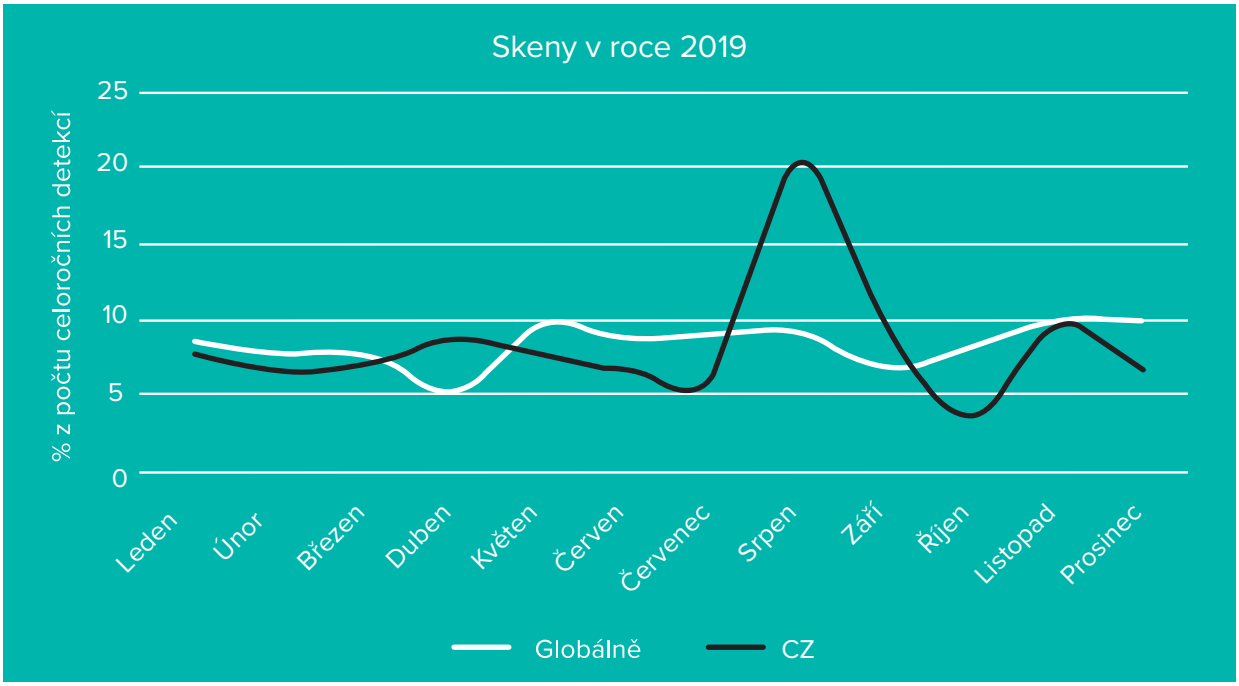


Skeny

Pokud jde o výskyt špiček, byla situace v oblasti skenů pravým opakem výše popsaného vývoje detekcí škodlivého kódu. Zatímco na globální úrovni byly, s výjimkou drobných výkyvů, počty detekcí skenů více méně vyrovnané v průběhu celého roku, v českém prostředí byly patrné dvě citelné špičky v jeho druhé půlce.

V rámci první z nich, v srpnu, bylo detekováno přes 20 % všech skenů evidovaných v průběhu roku, při druhé z nich, v listopadu, pak necelých 10 % skenů.

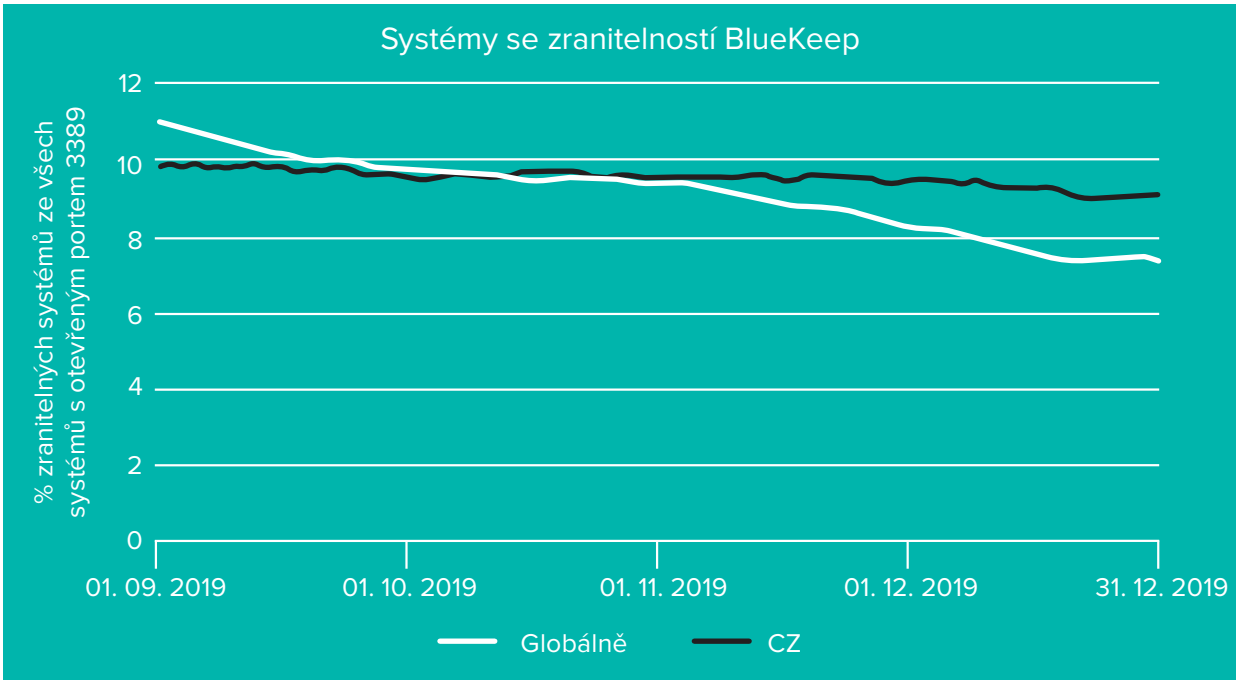
Zajímavou skutečností při tom je, že trendy v oblasti detekovaných skenů v druhé půlce roku kopírují trendy detekcí škodlivého kódu. Lze se tak domnívat, že v grafech je zachycena jedna (či více) ze škodlivých kampaní, v rámci nichž útočníci cílili na systémy dostupné přímo z internetu a šířili na ně malware s pomocí v nich přítomných zranitelností, které odhalovali s pomocí vzdálených skenů.



Zranitelné systémy

Počty detekovaných zranitelných systémů měly, dle dostupných dat, na globální i české úrovni v průběhu roku v průměru snižující se tendenci. Zvláštní zmínku v této oblasti však zaslouží vývoj situace spojené se zranitelností CVE-2019–0708, známou též jako BlueKeep. Tuto kritickou zranitelnost, postihující některé verze operačních systémů Microsoft Windows, detekoval ALEF CSIRT v průběhu roku na více než 780 tisících systémech dostupných přímo z internetu [1,2].

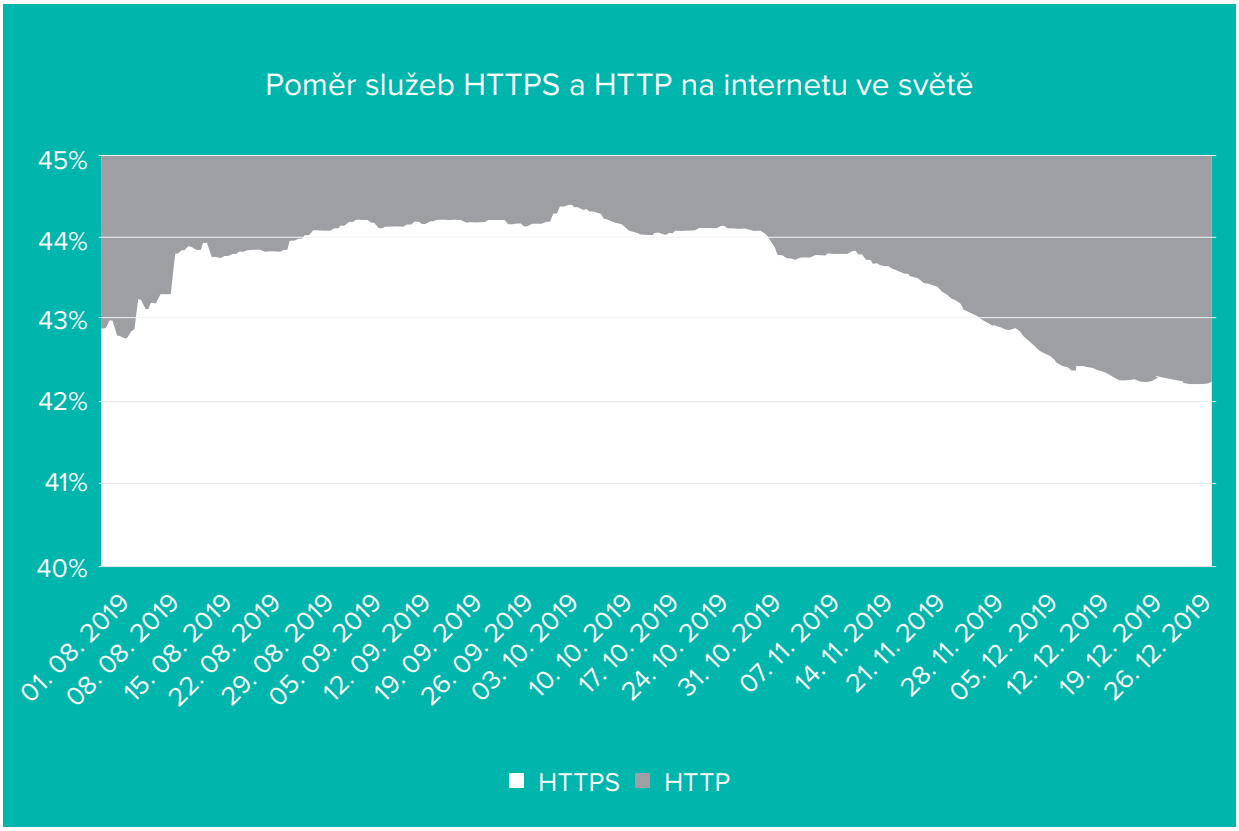
Počátkem listopadu byla odhalena škodlivá kampaň, v rámci níž útočníci zmiňovanou zranitelnost masivně využívali.[3] Jak však ilustruje následující graf, ani přes citelnou mediální pozornost, která byla této kampani věnována, nedošlo v reakci na ní k citelnějšímu snížení počtů zranitelných systémů. V prostředí české části internetu pak byly úbytky zranitelných systémů ještě nižší, než na globální úrovni, a na konci roku tak bylo v České republice z internetu stále volně dostupných téměř 1600 zranitelných systémů.

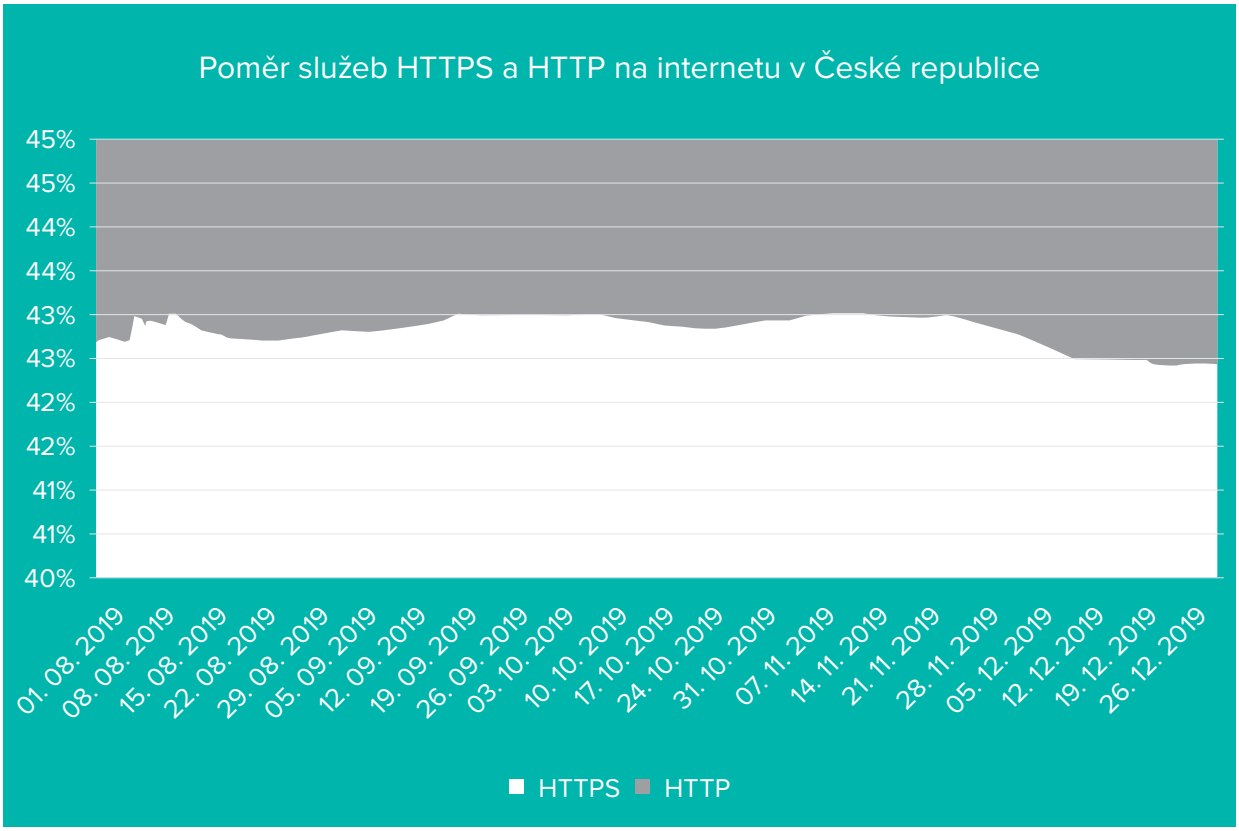


Šifrovaná komunikace v ČR a ve světě

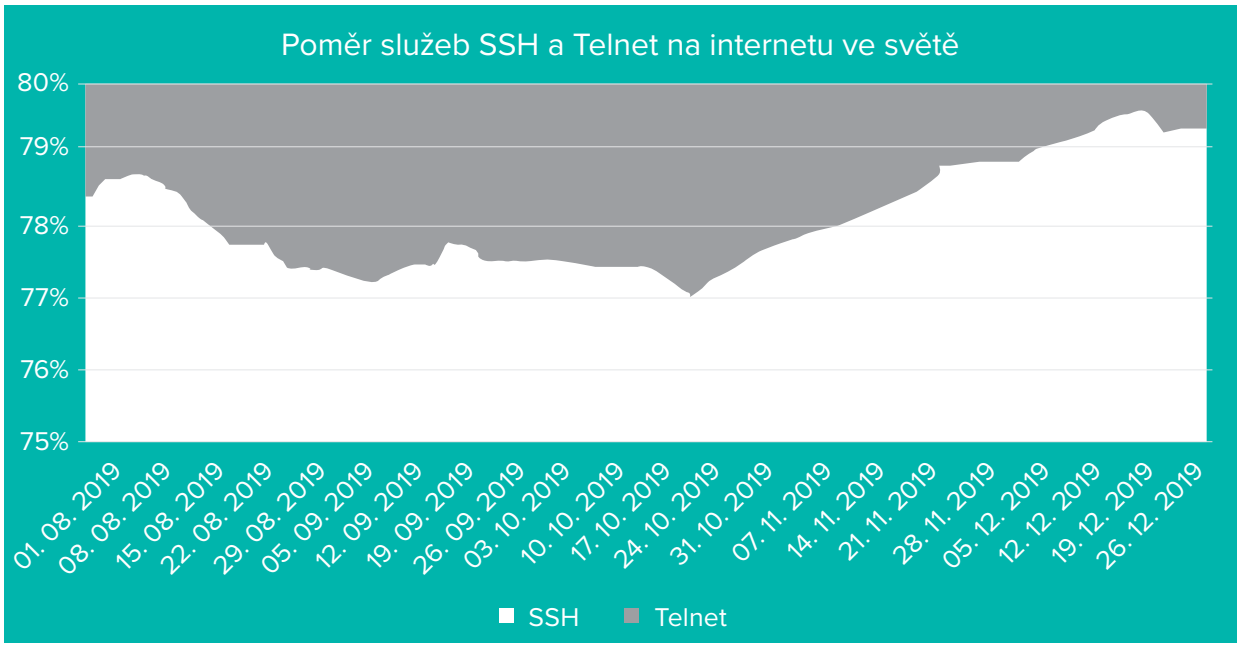
Pro šifrování provozu na počítačových sítích je užíván velký počet mechanismů a protokolů. Těmi zřejmě nejpodstatnějšími jsou SSH a TLS (resp. historicky SSL). Na úrovni webového provozu je pro zajištění kryptografické ochrany komunikace mezi klienty a servery před odposlechem a modifikací užíván právě protokol TLS, resp. protokol HTTPS, který prvně jmenovaný protokol využívá. Protokol SSH pak (mimo jiné) zajišťuje ochranu vzdáleného terminálového přístupu k různým systémům. Oba dva výše zmíněné protokoly byly vytvořeny jako bezpečnější alternativa ke starším protokolům HTTP a Telnet, které sloužily stejným účelům, ale kryptografickou ochranu přenášeným datům neposkytovaly. Přes zjevné výhody modernějších alternativ jsou oba výše zmíněné historické cleartextové protokoly stále široce užívány a to i v prostředí internetu, což může představovat citelné bezpečnostní riziko.

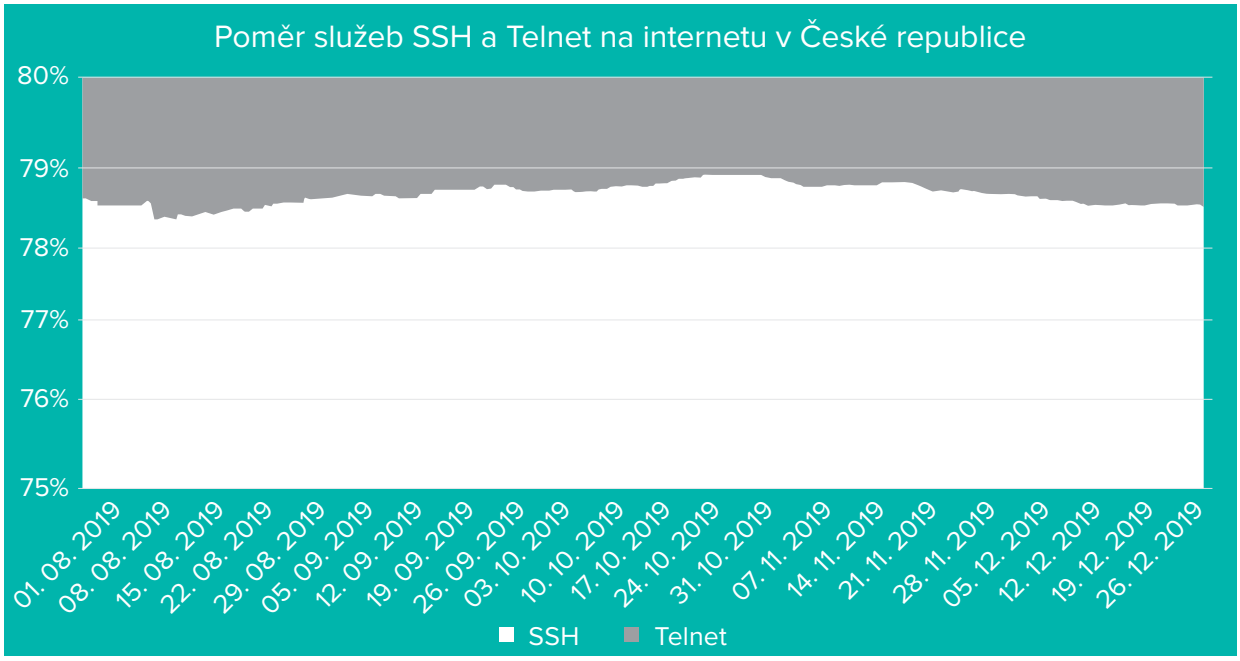
V případě webových serverů nemusí být podpora HTTP nutně nevhodná, vzhledem k tomu, že mnoho serverů nešifrovaný protokol užívá pouze pro prvotní připojení klientů a pro následnou komunikaci s nimi používá HTTPS. Znamená to však, že v ideálním případě by měl počet serverů poskytujících HTTPS buď převyšovat počet těch nabízejících HTTP, nebo by jejich počty měly být maximálně vyrovnané. Jak ale ukazují následující grafy, v českém i globálním prostředí měl v průběhu konce roku poměr mezi servery nabízejícími protokoly pro webový přístup tendenci zvyšovat se ve prospěch nešifrovaného HTTP. Z absolutních čísel vyplývá, že tato změna byla způsobena snížením počtu serverů užívajících protokol HTTPS, spíše než citelnějším nárůstem počtu serverů podporujících HTTP.


Poměr služeb HTTPS a HTTP na internetu ve světě
45%
44%
43%
42%
41%
40%
01. 08. 2019
08. 08. 2019
15. 08. 2019
22. 08. 2019
29. 08. 2019
05. 09. 2019
12. 09. 2019
19. 09. 2019
26. 09. 2019
03. 10. 2019
10. 10. 2019
17. 10. 2019
24. 10. 2019
31. 10. 2019
07. 11. 2019
14. 11. 2019
21. 11. 2019
28. 11. 2019
05. 12. 2019
12. 12. 2019
19. 12. 2019
26. 12. 2019
HTTPS
HTTP


Poměr služeb HTTPS a HTTP na internetu v České republice
45%
45%
44%
44%
43%
43%
42%
42%
41%
41%
40%
01. 08. 2019
08. 08. 2019
15. 08. 2019
22. 08. 2019
29. 08. 2019
05. 09. 2019
12. 09. 2019
19. 09. 2019
26. 09. 2019
03. 10. 2019
10. 10. 2019
17. 10. 2019
24. 10. 2019
31. 10. 2019
07. 11. 2019
14. 11. 2019
21. 11. 2019
28. 11. 2019
05. 12. 2019
12. 12. 2019
19. 12. 2019
26. 12. 2019
HTTPS
HTTP

V případě protokolů pro vzdálené terminálové připojení neexistuje na rozdíl od výše diskutovaných protokolů pro přenos webového provozu významnější důvod pro používání nešifrovaného přenosu dat. Proto lze považovat za pozitivní, že na globální úrovni bylo možné koncem roku 2019 pozorovat citelnou změnu v poměru mezi servery poskytujícími služby s pomocí protokolu SSH a Telnet ve prospěch šifrované varianty. V rámci českých IP adresních rozsahů se tento trend citelněji neprojevil a situace v posledních 4 měsících loňského roku byla v této oblasti relativně vyrovnaná.





[1] https://untrustednetwork.net/en/2019/08/01/where-are-all-the-machines-affected-by-blue-keep-hiding/
[2] https://www.untrustednetwork.net/en/2019/08/10/where-are-all-the-machines-affected-by-bluekeep-hiding-part-2/
[3] https://isc.sans.edu/forums/diary/Did+the+recent+malicious+BlueKeep+campaign+have+any+positive+impact+when+it+comes+to+patching/25506/

CSIRT.CZ

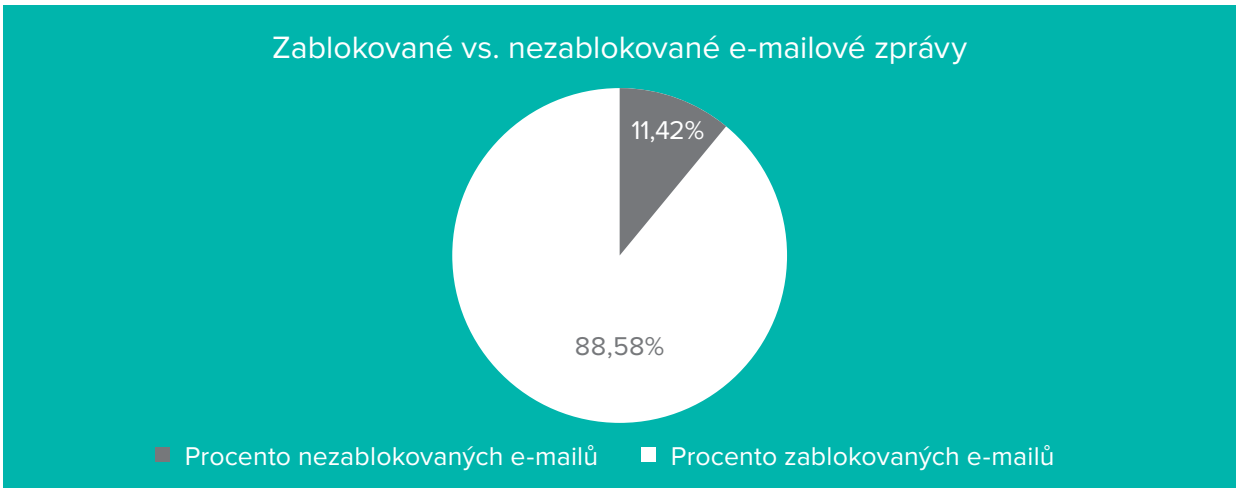
cesnet certs

Analýza dat z e-mailových bran

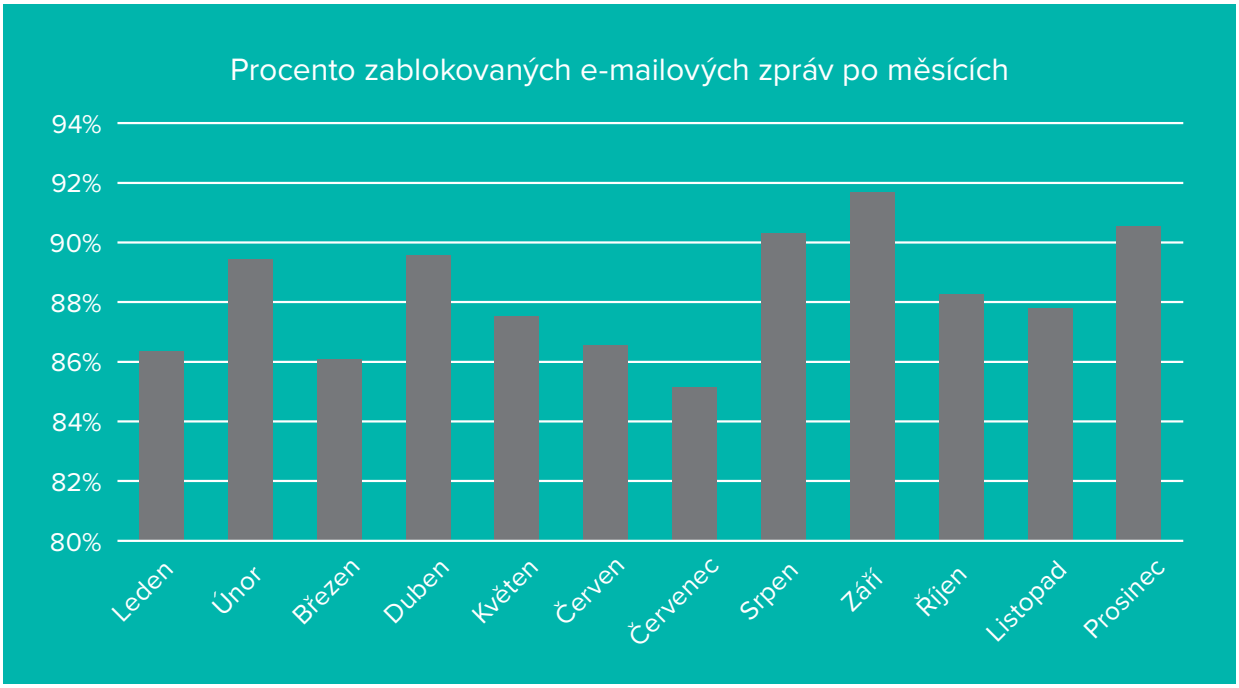
Milan Habrcetl

Tato část analýzy probíhala nad daty příchozích e-mailových zpráv, které byly přijaty vybranými e-mailovými branami v roce 2019. Celkový počet příchozích e-mailových zpráv, které byly zpracovány v těchto nástrojích, byl téměř 16 milionů.

Za celý rok 2019 bylo zablokováno více než 88,5 procenta všech příchozích e-mailových zpráv. Oproti roku předtím se jedná o více než procentní nárůst zablokovaných e-mailových zpráv.

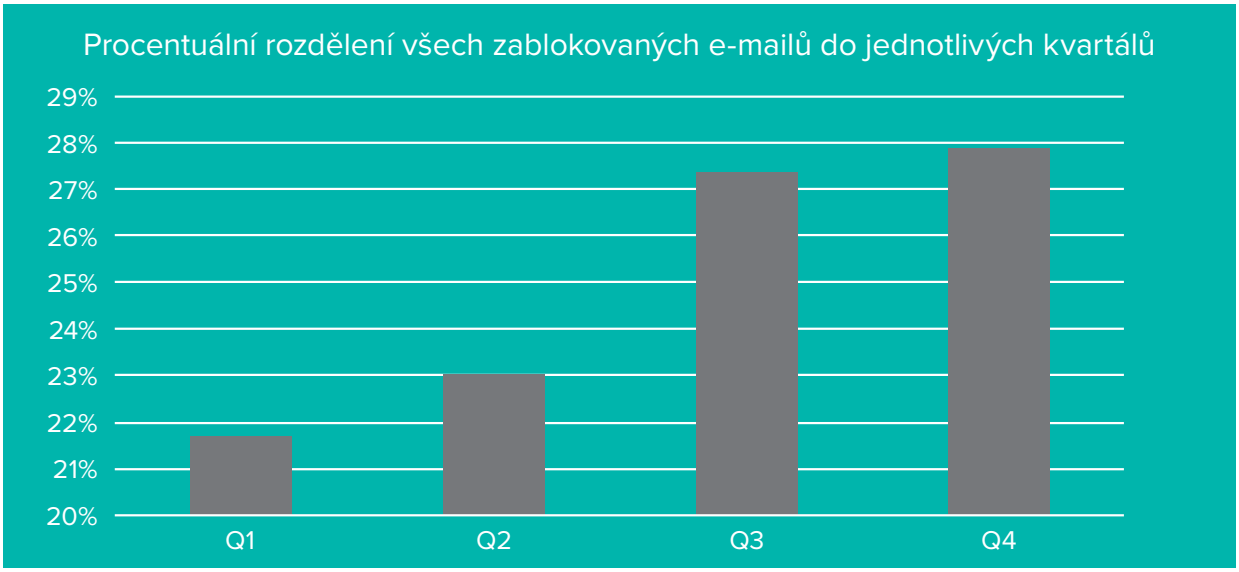


V každém měsíci roku 2019 bylo e-mailovými branami zablokováno průměrně 88 procent e-mailových zpráv. Nejvíce e-mailových zpráv bylo blokováno v srpnu, září a prosinci, kdy procento blokovaných zpráv přesáhlo 90 procent.



Po agregaci dat na jednotlivá čtvrtletí lze také vypozorovat významný nárůst blokovaných e-mailových zpráv mezi druhým a třetím čtvrtletím roku 2019. Důvodem může být například konec dovolených ve třetím čtvrtletí a tím i zvýšený počet škodlivých e-mailových zpráv.

Nejvyšší počet zablokovaných zpráv byl, tak jako tradičně, pozorován ve čtvrtém čtvrtletí roku 2019. Jedním z hlavních důvodů pro to jsou svátky (Vánoce) a oslava příchodu nového roku. V těchto obdobích je totiž uživatel nejméně pozorný a také očekává příchozí balíčky, faktury apod. Útočníci této skutečnosti využívají a odesílají e-mailové zprávy se škodlivým obsahem co největšímu počtu uživatelů, aby zvýšili své výdělky.

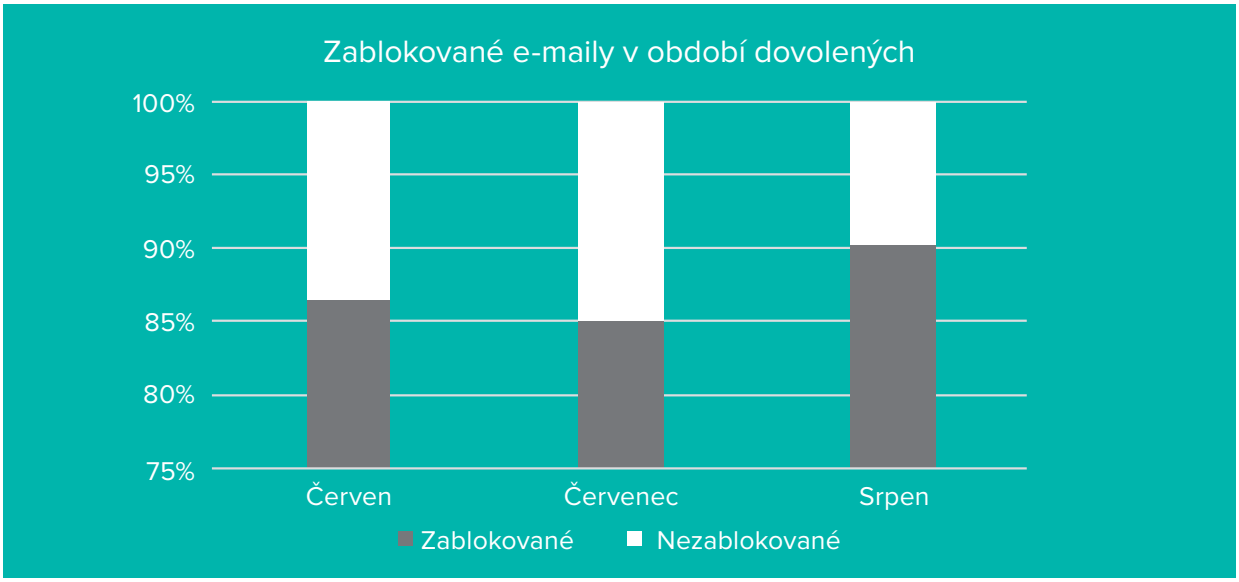


Období dovolených a pokles počtu zablokovaných e-mailových zpráv

V průběhu měsíců června a července, ve kterých obvykle bývá větší počet dovolených, lze vypozorovat pokles zablokovaných e-mailových zpráv. S největší pravděpodobností z toho důvodu, že by se útočníkům nevyplatilo odesílat e-mailové zprávy se škodlivým obsahem, protože s nimi uživatelé neinteragují (jsou na dovolené).

Naopak v srpnu lze pozorovat velký nárůst zablokovaných e-mailových zpráv. V srpnu většinou dovolené končí a útočníci chtějí využít nepozornosti uživatelů, kteří se vracejí do práce a kteří musejí zkontrolovat zameškané e-mailové zprávy.

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



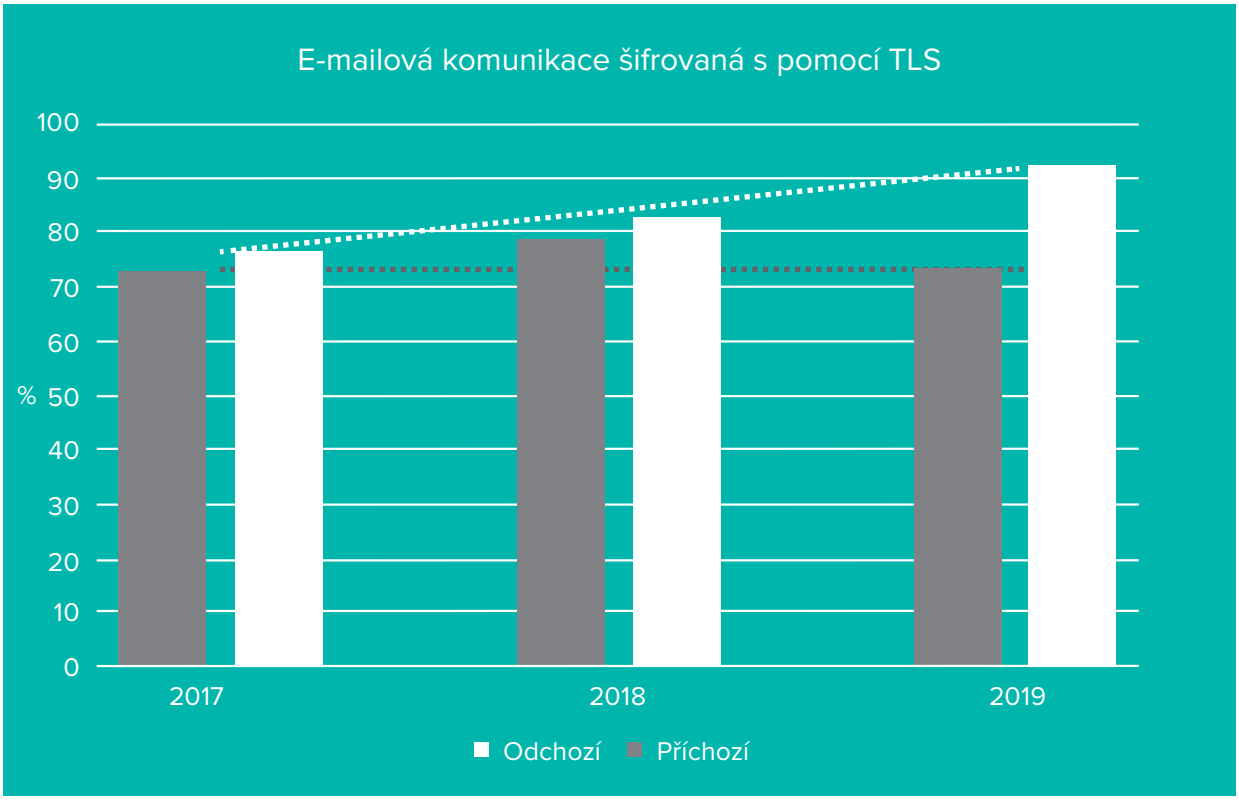
Zabezpečení e-mailové komunikace

Jan Kopřiva

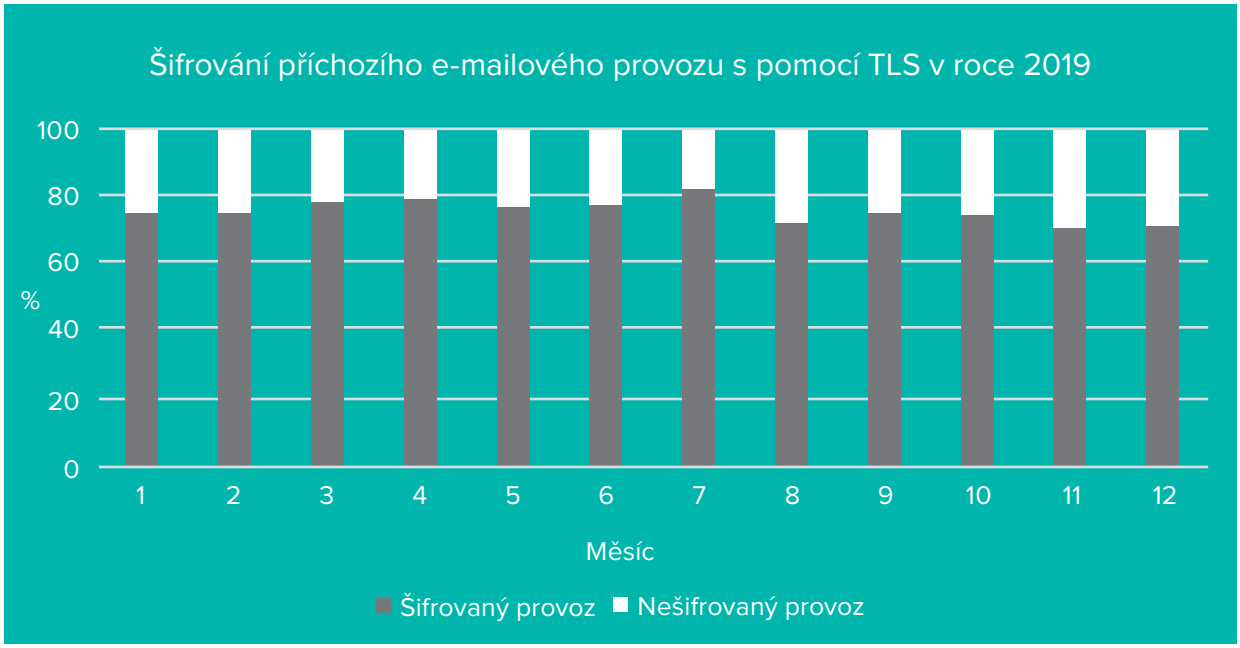
Jak ukazuje předchozí kapitola, na nevyžádané a škodlivé e-mailové zprávy byl rok 2019 velmi bohatý. Vedle stavu na poli hrozeb si však krátký popis zaslouží také vývoj v oblasti zabezpečení e-mailové komunikace, resp. v používání protokolu TLS k šifrování elektronické pošty při přenosu mezi servery.

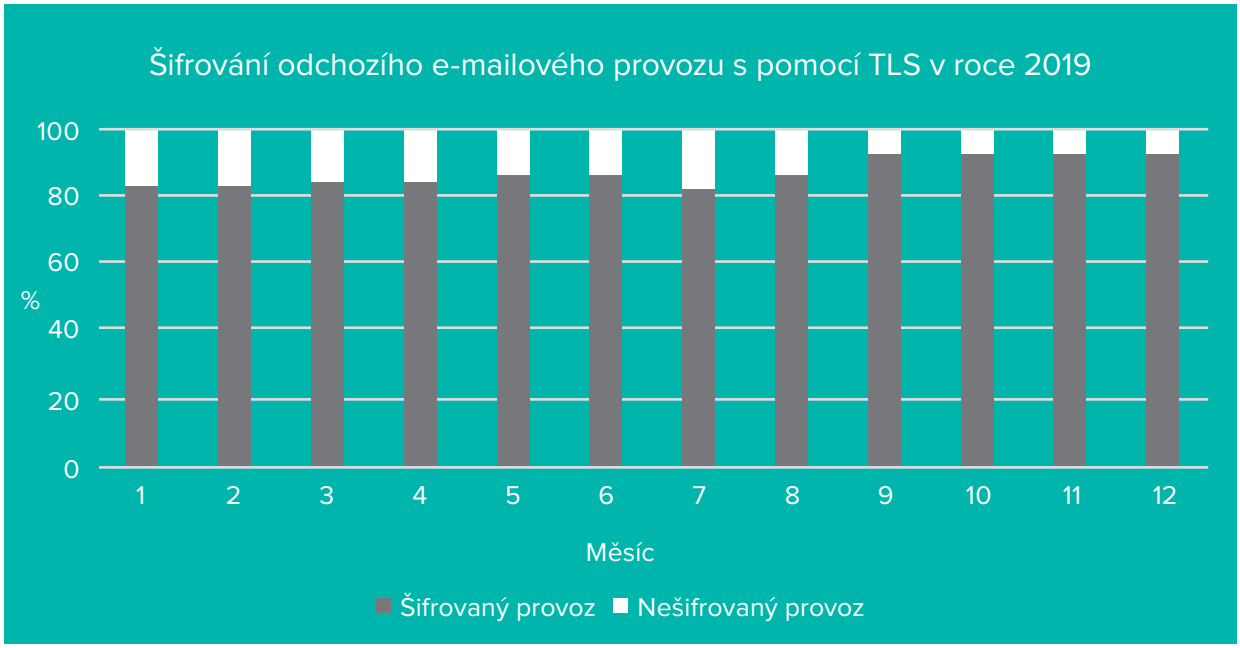
Kryptografický protokol Transport Layer Security (TLS) je spolu s mechanismem STARTTLS často užíván pro zajištění důvěrnosti obsahu e-mailových zpráv při jejich přenosu mezi servery. Na rozdíl od S/MIME a PGP, tedy bezpečnostních mechanismů pro end-to-end šifrování zpráv, zajišťuje TLS pouze šifrování kanálu, jímž je e-mailová komunikace přenášena. Poskytuje tak sice ochranu dat výhradně při jejich přenosu (a tedy ne například ochranu zpráv uložených ve schránce), nicméně z pohledu uživatelů je zcela transparentní. Při komunikaci mezi e-mailovými servery se navíc šifrování s pomocí TLS/STARTTLS aplikuje automaticky, pokud jej obě strany podporují.

Počet e-mailových serverů, které popsaný mechanismus automatického šifrování komunikace podporují, v posledních letech roste, a jak ilustruje následující graf, tento trend je patrný i v prostředí českého internetu.



Následující grafy ukazují procentuální zastoupení e-mailové komunikace šifrované, resp. nešifrované, s pomocí TLS v prostředí České republiky v roce 2019. Data, na základě nichž byly grafy vytvořeny, pocházejí z mnoha různých systémů (viz první kapitola). Zmínku však zaslouží, že od srpna roku 2019 byl mezi sledované systémy přidán další masivní datový zdroj, což je důvodem pro relativně citelný posun v hodnotách vyobrazených v grafech počínaje tímto měsícem.


Šifrování příchozího e-mailového provozu s pomocí TLS v roce 2019
100
80
60
%
40
20
0
1
2
3
4
5
6
7
8
9
10
11
12
Měsíc
Šifrovaný provoz
Nešifrovaný provoz

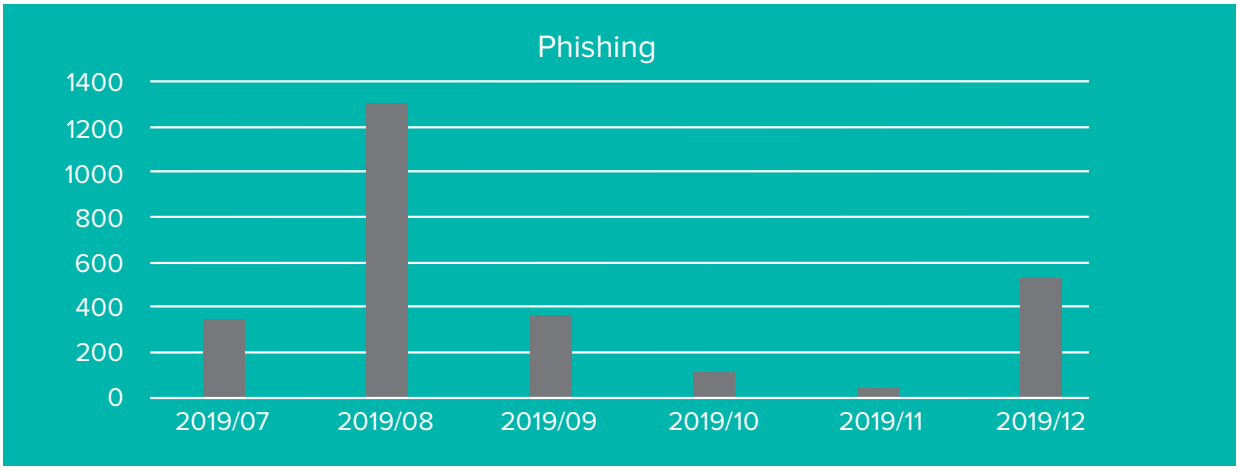

Šifrování odchozího e-mailového provozu s pomocí TLS v roce 2019
100
80
60
%
40
20
0
1
2
3
4
5
6
7
8
9
10
11
12
Měsíc
Šifrovaný provoz
Nešifrovaný provoz

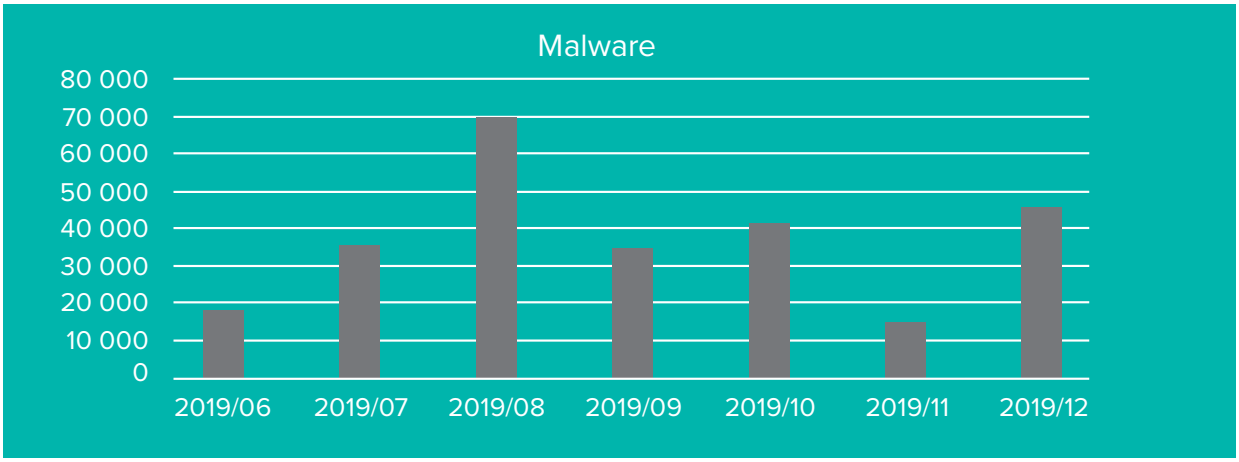
Analýza událostí zachycených IPS sondami

Stanislav Techlovský

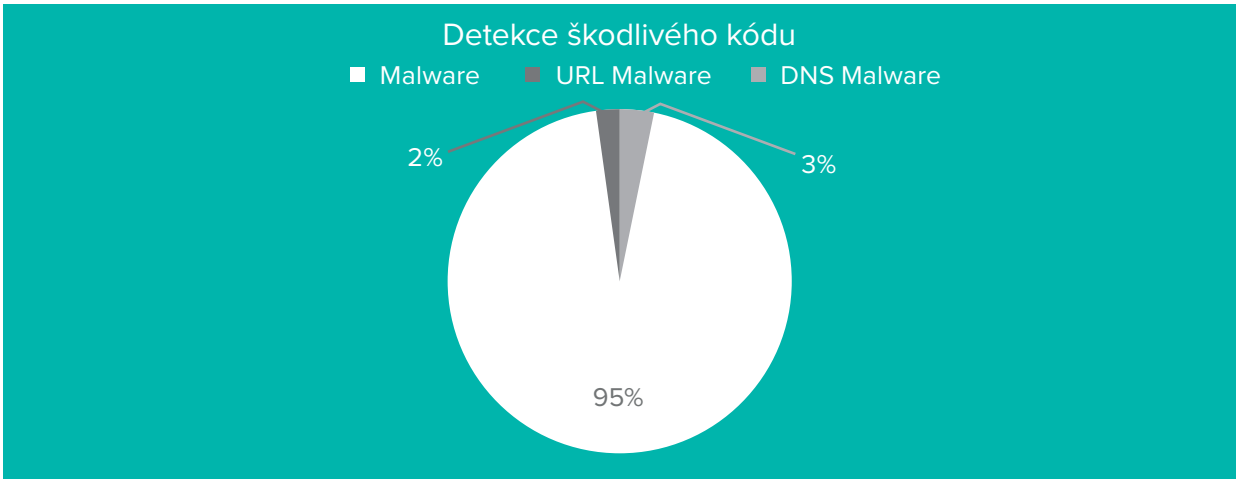
Následující část reportu se zabývá analýzou dat z IPS (Intrusion Prevention System) sond pod správou společnosti ALEF NULA a. s. Analýza se zaměřuje na data z období posledních dvou kvartálů roku 2019.

V první části analýzy se nejprve podíváme na phishing. IPS sondy detekovaly incident tohoto typu vždy, když se uživatel pokusil navštívit blokované phishingové stránky. Nejvíce incidentů z minulého roku bylo detekováno v měsíci srpnu v množství 1306 incidentů. Ke konci roku 2019 došlo, obdobně jako v minulém roce, k růstu incidentů. Za měsíc prosinec bylo detekováno 524 incidentů, oproti předchozímu měsíci listopadu to byl nárůst o 1200 %.





Za poslední dva kvartály roku 2019 bylo největší množství incidentů spojených s malwarem zachyceno IPS systémy v měsíci srpnu – šlo o téměř 70 tisíc událostí. V prosinci bylo detekováno 45 849 incidentů, oproti předchozímu měsíci listopadu jde o 307 % 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 v loňském reportu.

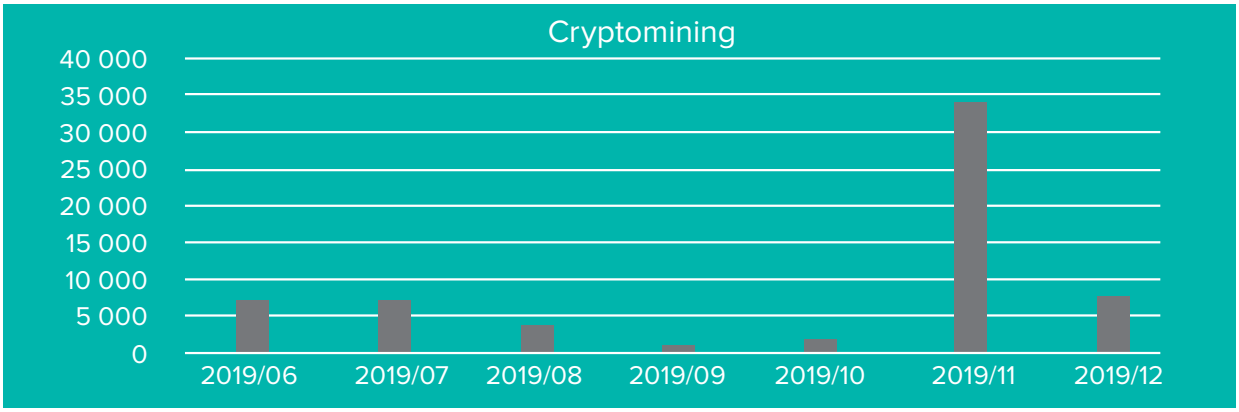


Detekce spojené se škodlivým kódem člení sledované IPS systémy do tří základních kategorií. V kategorii malware se nacházejí události, při kterých byla identifikována shoda s reputační databází IPS, která obsahuje IP adresy, na nichž se vyskytuje nebo vyskytoval malware. Porovnává se přitom jak zdrojová, tak cílová IP adresa.

Kategorie URL malware obsahuje pouze adresy, na nichž byl zaznamenán výskyt malwaru. Samotnou detekci provádí sondy na základě analýzy webového provozu s pomocí kontroly URL.

Poslední kategorií je DNS malware, reputační databáze v tomto případě obsahuje seznam domén, u kterých byl detekován malware. Událostmi jsou v takovém případě detekované DNS dotazy na škodlivé domény, o jejichž překlad se pokusil malware nacházející se uvnitř chráněných sítí.

Za sledované období posledních dvou kvartálů roku 2019 byla struktura detekcí malwaru následující: z 95 % byly detekce výskytu malware realizovány s pomocí reputační databáze, pouze ze 3 % se jednalo o detekce s pomocí kontroly DNS a zbylá 2 % byla odhalena s využitím URL kontroly (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, blacklistovaných domén a SSL certifikátů.

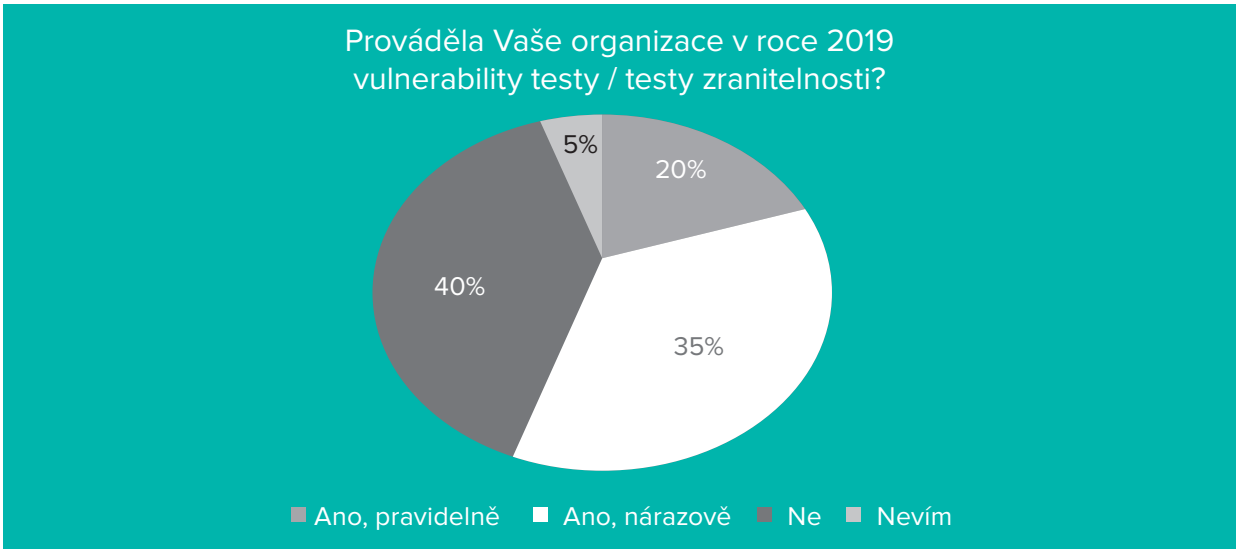
V listopadu 2019 byl zachycen nejvyšší počet pokusů o těžbu kryptoměn, celkem šlo o téměř 34 tisíc detekcí. Oproti předchozímu měsíci říjnu se jednalo o 1844% nárůst. V prosinci došlo k následnému poklesu pokusů o těžbu kryptoměn o 441% oproti předchozímu měsíci (viz. graf Cryptomining). Obdobný trend byl patrný i na konci roku 2018, kdy však pokles pokusů o těžbu kryptoměn nebyl tak výrazný.

Bezpečnostní testování v roce 2019

Jana Little

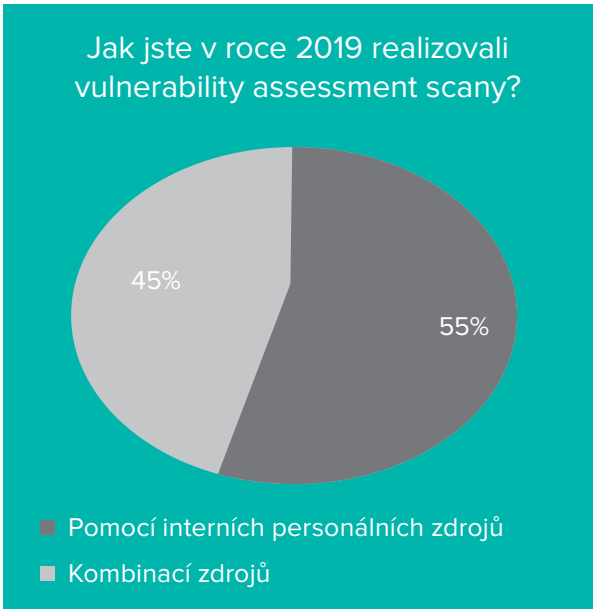
Vulnerability testy v roce 2019

V této části reportu se dozvíme více o bezpečnostním testování. Podíváme se na to, jak si stál rok 2019 z pohledu bezpečnostního testování a také nahlédneme do plánů pro rok 2020. V rámci analýzy nás zajímalo, jak se různé organizace staví k vulnerability testům / testům zranitelností a k penetračnímu testování. Dotkneme se také red team cvičení a rozebereme si, jakým směrem uchylují pozornost organizace v rámci bezpečnostního testování.



Jak je z výše uvedeného grafu patrné, vulnerability testy / testy zranitelností provádělo v roce 2019 55 % dotázaných organizací. Celkem 20 % organizací provádělo testy pravidelně a větší část společností (35 %) uvedla, že tyto testy provádí pouze nárazově. V celkovém souhrnu vyšlo najevo, že 40 % dotázaných organizací tyto testy vůbec neprovádí.

Jaký je vůbec přínos testů zranitelností a proč by se jim organizace měly alespoň nárazově věnovat? Jak ukazuje část první kapitoly věnovaná zranitelnosti BlueKeep, i mnoho měsíců po publikaci kritických zranitelností existují stále v českém i globálním prostředí systémy připojené k internetu, které jsou vůči nim náchylné. Totéž platí i v rámci lokálních sítí. Aby byla organizace schopná spolehlivě eliminovat tyto zranitelnosti ze svých systémů, potřebuje vedle standardizovaného patch management plánu také provádět verifikaci vlastního nasazení záplat.

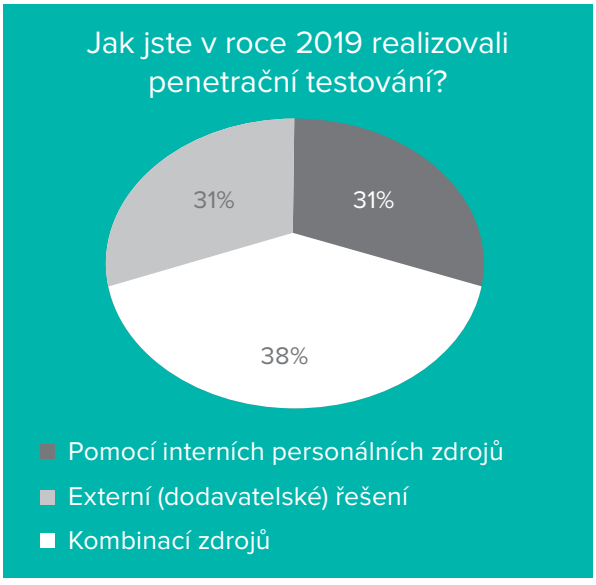


Pokud organizace v rámci dotazníku uvedla, že se vulnerability testy / testy zranitelností zabývá, zajímalo nás, jakým způsobem testy realizovala. Žádná z organizací v roce 2019 nepřenechala realizaci testů pouze externím dodavatelům. Většina dotázaných uvedla, že testy uskutečňovali s pomocí svých interních personálních zdrojů. Zbylých 45 % společností uvedlo, že testy řeší za pomocí kombinace zdrojů. Využívají tedy zkušeností dodavatelů, ale zapojují do realizace také své interní zdroje.

Penetrační testování v roce 2019

Jak to bylo v případě penetračního testování? Tento typ bezpečnostních testů představuje způsob, jak nejen identifikovat přítomnost zranitelností v systémech organizace, ale také prokázat, že jejich zneužití je reálně možné, a demonstrovat míru rizika, kterou skutečně představují pro organizaci.

Velká část dotázaných (65 %) uvedla, že se v roce 2019 penetračnímu testování věnovala. To je skvělá zpráva, jelikož penetrační testy jsou jednou z nejlepších možností, jak verifikovat, že bezpečnostní opatření jsou korektně nastavena a implementována.

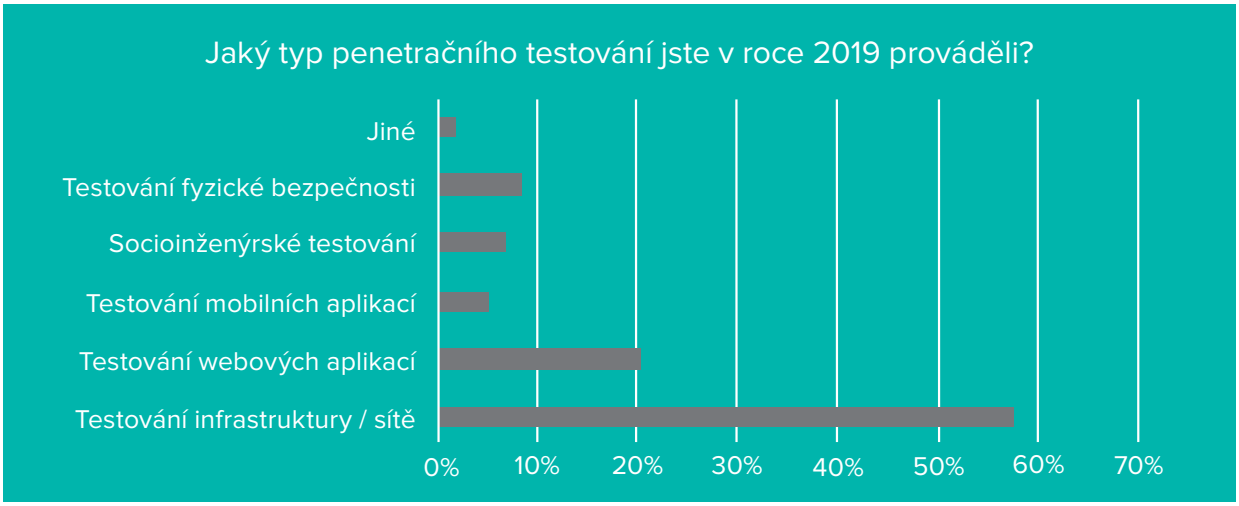


Jak z dotazníku vyplynulo, nejvíce organizací provádělo penetrační testování za pomoci externí dodávky služeb. 31% organizací, které se penetračnímu testování věnují, pak využilo interní personální zdroje a stejné procento organizací řešilo realizaci penetračních testů pomocí kombinace interních a externích zdrojů.

Celých 45% organizací provádělo v roce 2019 penetrační testování pouze nárazově. Zbylých 20% realizovalo v průběhu posledních 12 měsíců penetrační testy pravidelně, a to v souladu s bezpečnostními potřebami a plány. Ze vzorku dotázaných se 35% organizací v roce 2019 problematice penetračního testování vůbec nevěnovalo.

O jaké typy penetračního testování šlo? Nejvíce organizací testovalo v roce 2019 webové aplikace, infrastrukturu, případně sítě. Zájem byl také o testování fyzické bezpečnosti. Organizace realizovaly též penetrační testování mobilních aplikací a prováděly také socioinženýrské testy. Pouze 5 % organizací uvedlo, že v roce 2019 realizovaly také red team cvičení.

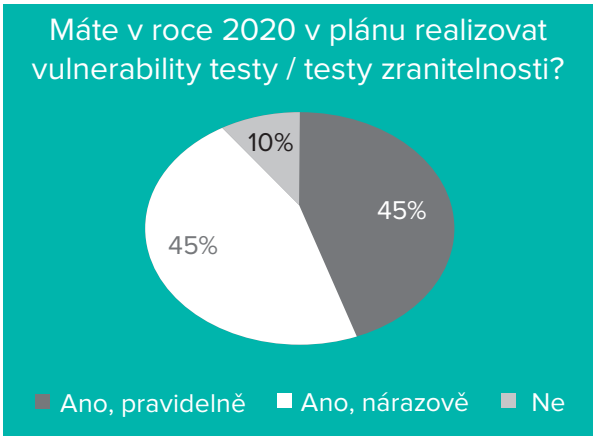
Red team cvičení představují simulaci reálných útoků s pomocí technik, taktik a procedur užívaných skutečnými útočníky (včetně APT aktérů). Vzhledem k tomu, že tato forma bezpečnostního testování klade extrémně vysoké nároky na vyspělost bezpečnostního systému, není pro většinu organizací v jejich současné podobě vhodná. Jak ukazují výše zmíněné výsledky našeho šetření, organizace jsou si toho vědomy a red teamingu se tak věnují pouze ty, pro něž představuje jeho realizace skutečný přínos.

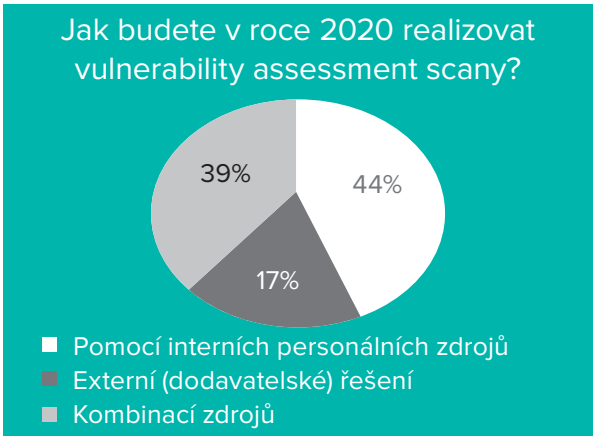


Bezpečnostní testování v roce 2020

Zajímali jsme se rovněž o to, zda dotazované organizace budou věnovat pozornost vulnerability testům i v roce 2020. V plánu to má 90 % z nich. Organizace mají zájem o pravidelné i nárazové testování.

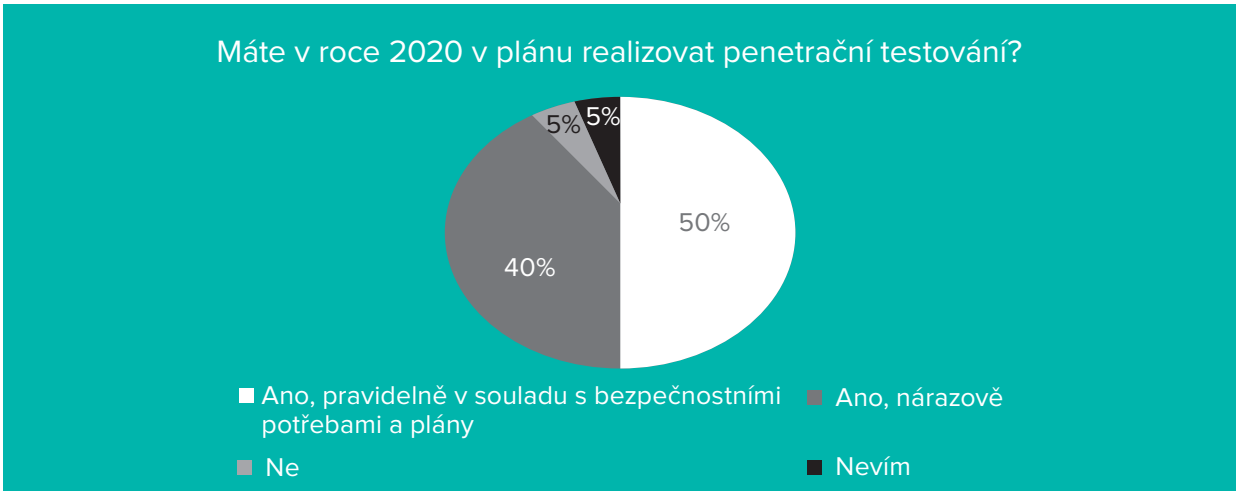
Důsledkem většího zájmu o tento typ bezpečnostních testů může být uvědomování si rizik spojených s přítomností technických zranitelností, potažmo zvyšující se bezpečnostní povědomí. Pouze 10 % organizací se vyjádřilo, že v roce 2020 nemá v plánu tyto testy realizovat. Největší procento organizací má v plánu testování zranitelností realizovat s pomocí interních personálních zdrojů či využití interních zdrojů spolu s externí dodavatelskou firmou. Pouze malá část dotázaných (17 %) plánovala realizovat testy jen prostřednictvím dodavatelského řešení.





Penetrační testování v roce 2020

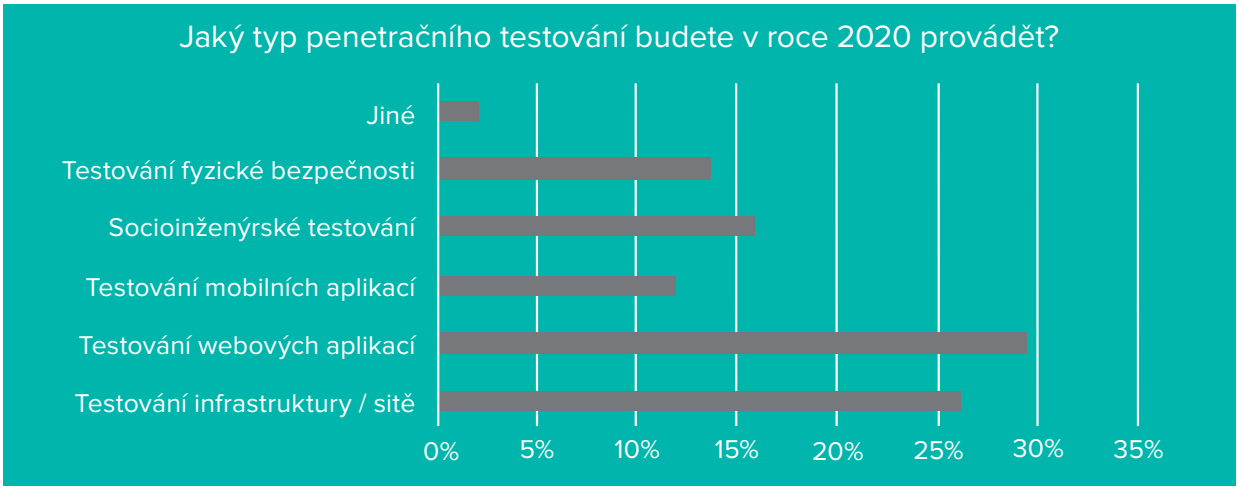
V roce 2020 má 90 % dotázaných organizací zájem o provádění penetračního testování, což je citelný nárůst oproti roku 2019. Nejvíce mají organizace v plánu věnovat se pravidelnému testování v souladu s bezpečnostními potřebami a plány, případně hodlají využívat nárazové penetrační testy. Pouze 5 % organizací ze stejného vzorku dotázaných uvedlo, že se v roce 2020 penetračnímu testování věnovat nebudou.

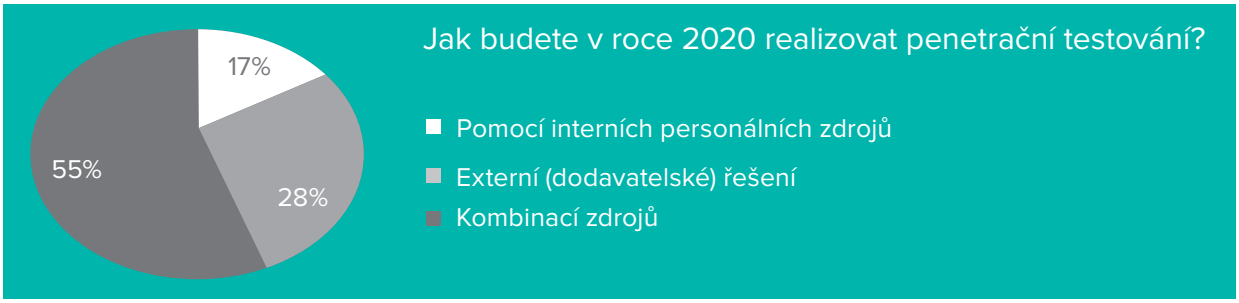


Jak je z níže uvedeného grafu patrné, zaměření testů bude mít obdobný charakter jako v roce 2019. Největší zájem mají organizace o testování webových aplikací, testování infrastruktury / sítí a o socioinženýrské testy.

Organizace mají také v plánu věnovat se testování fyzické bezpečnosti a testovat mobilní aplikace.

Celých 55 % dotázaných organizací má v plánu využít k tomu interní personální zdroje spolu s externí dodavatelskou firmou. Celých 28 % dotázaných bude realizovat penetrační testy pouze pomocí dodavatelského řešení a zbylých 17 % využije pouze interní personální zdroje.





Bezpečnostní dohled a stav Security Operations v roce 2019

Daniel Neumann

Bezpečnostní incidenty jsou pro moderní IT organizace nevyhnutelnou součástí denní reality a jejich včasná detekce je nezbytná pro zajištění bezpečnosti interních systémů a v nich obsažených dat. Řada společností má implementováno množství technologií sloužících k zajištění bezpečnosti infrastruktury, avšak mohou mít potíže s obsluhou těchto řešení.

Problémy mohou spočívat v rozdílnosti jednotlivých technologických řešení, jejich uživatelských rozhraní a absenci centrálního vyhodnocovacího mechanismu. Neméně podstatnou překážkou je často výrazná fluktuace pracovníků IT oddělení, kteří se na své pozici musejí „seznámit“ s technologiemi, se kterými budou na denní bázi pracovat. Mnohdy se s nimi setkávají poprvé a vzniká tudíž potřeba pravidelného školení.

Vhodným řešením se zdá být centralizace bezpečnostní operativy do jednoho bodu – Security Operations Centra (SOC). V případě, že se organizace rozhodne pro vybudování vlastního SOC, bude s největší pravděpodobností čelit několika výzvám. Zároveň si jistě položí některou z uvedených otázek či dospěje k níže uvedeným závěrům:

1.) Budeme mít dostatečné množství analytiků pro zajištění vysoké dostupnosti služby?

2.) Je náš analytik dostatečně kvalifikovaný? Nebude kvůli nízkému výskytu a omezeným typům incidentů ztrácet své „know-how“? Nebo naopak z důvodu nízké úrovně odbornosti bude mít problémy se správnou analýzou hrozeb?

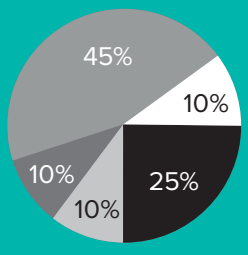
3.) Jak časově náročný bude samotný bezpečnostní dohled? Stihne jej zodpovědná osoba vykonávat na 100 % či jí zabere jen zlomek pracovní náplně? Pokud dotyčný bude vytížen jen minimálně, zaměstnáme jej jinými doplňkovými činnostmi. Ty nicméně postupem času mohou vytěsnit čas na aktivity spjaté se SOC a původní náplň konkrétního analytika tak plně vytěsní.

4.) Finanční náklady na plně funkční SOC jsou značné a tudíž mimo možnosti běžné organizace. Máme na plnohodnotný SOC dostatek prostředků?

Vzhledem k těmto a dalším relevantním otázkám jsme v průběhu prvního kvartálu 2020 realizovali analýzu potřeb a možností organizací v oblasti budování a provozu SOC. Analýza byla založená na datech získaných prostřednictvím dotazníkového šetření mezi klienty ALEF Group, kterým tímto velice děkujeme.

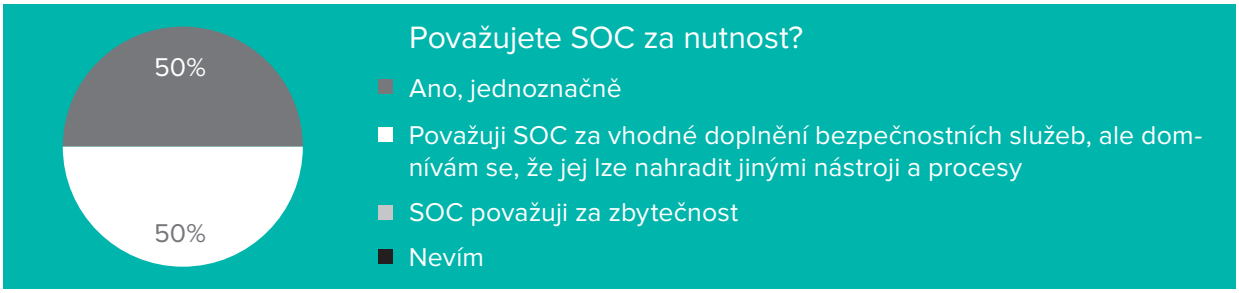
Privátním plně vyhovujícím SOC se může pochlubit přesně čtvrtina dotazovaných společností. Každá desátá sice provozuje vlastní SOC, ale zároveň přiznává, že přesně neodpovídá interním potřebám. Stejný počet klientů volí řešení ve formě externího SOC. Téměř polovina oslovených o SOC uvažuje do budoucna.

Využíváte služeb SOC (Security Operations Center)?

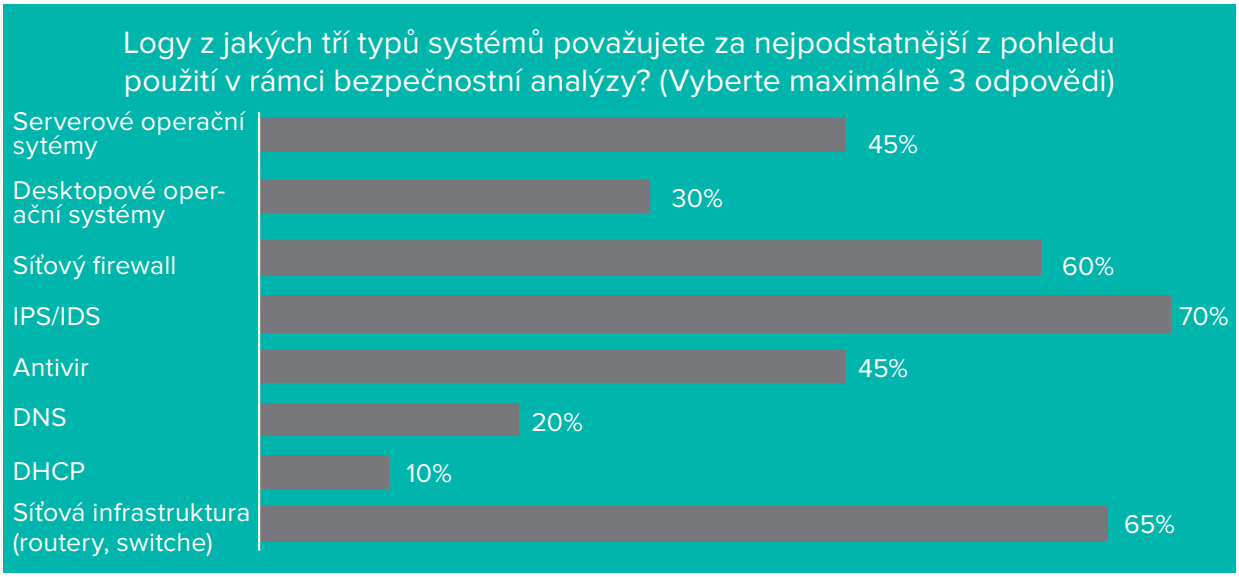


- Ano, máme vlastní SOC a plně pokrývá naše potřeby
- Ano, máme vlastní SOC, ale plně neodpovídá našim potřebám
- Ano, využíváme externí SOC
- Ne, SOC nemáme, ale uvažujeme o něm
- Ne, SOC nemáme a ani o něm do budoucna v žádné formě neuvažujeme
- Nevím

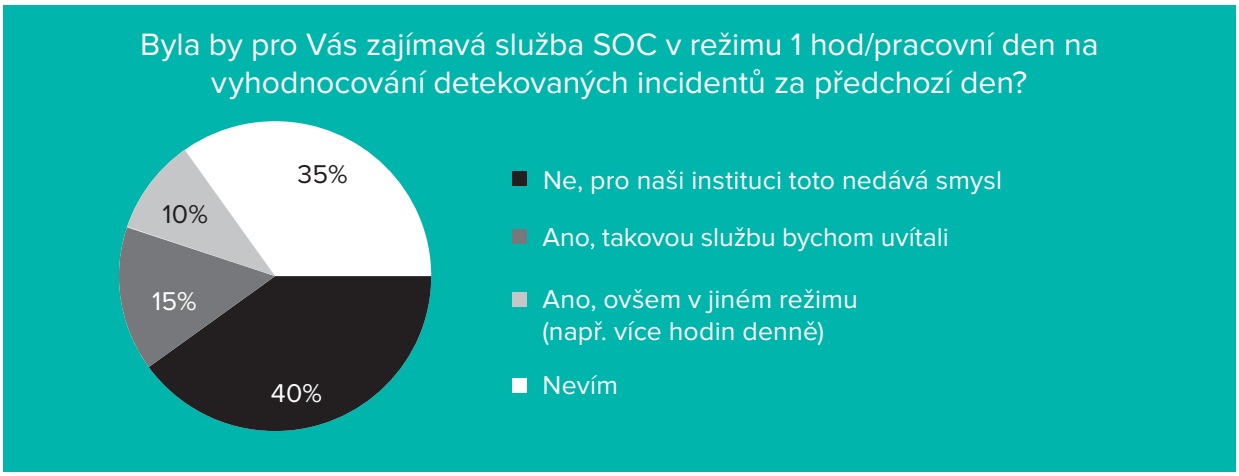
SOC je bezesporu vnímán jako vhodný prostředek pro zajištění bezpečnosti IT prostředí, v očích poloviny dotázaných jej lze nicméně vhodnými nástroji nahradit.



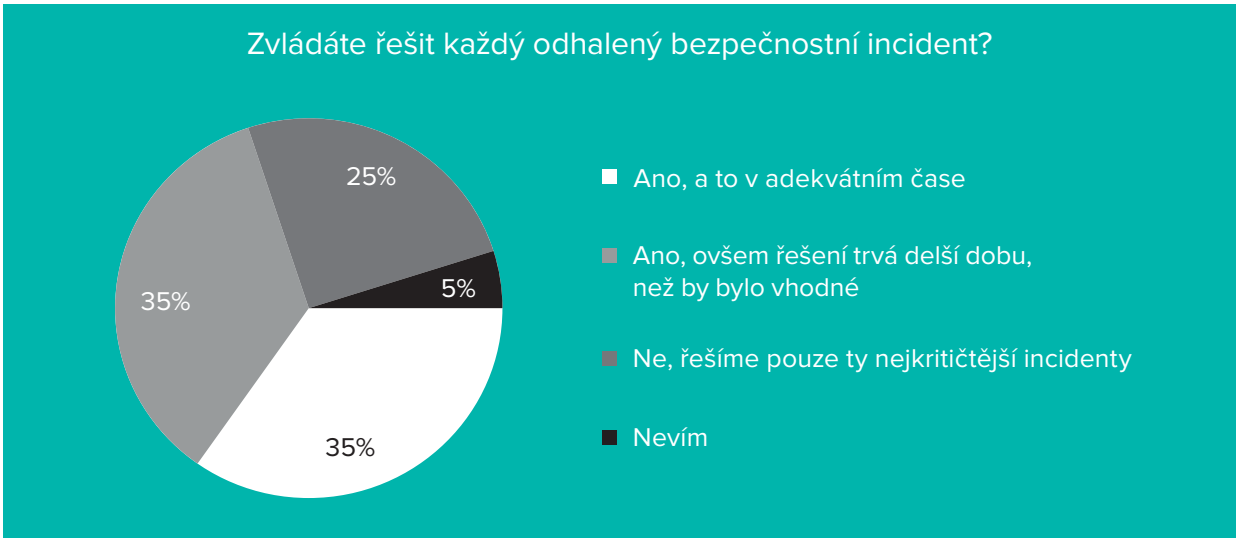
Zaznamenávání dat za účelem jejich analýzy (logování) patří mezi základní činnosti nezbytné k ověření zabezpečení IT prostředí organizace. Za nejpřínosnější pro tuto oblast považuje většina dotázaných logy z IPS/IDS, těsně následovanými logy ze síťové infrastruktury a síťového firewallu. Necelá polovina považuje za významná data generovaná serverovými operačními systémy a antiviry.



Vyhodnocování detekovaných anomálií a poplachů v reálném čase v režimu 24x7 nebo 8x5 nemusí představovat nejvhodnější variantu pro každou instituci, a to z mnoha důvodů. Dávalo by smysl poskytovat variantu SOC „šitou na míru“? Čtvrtina respondentů by takovou variantu uvítala.



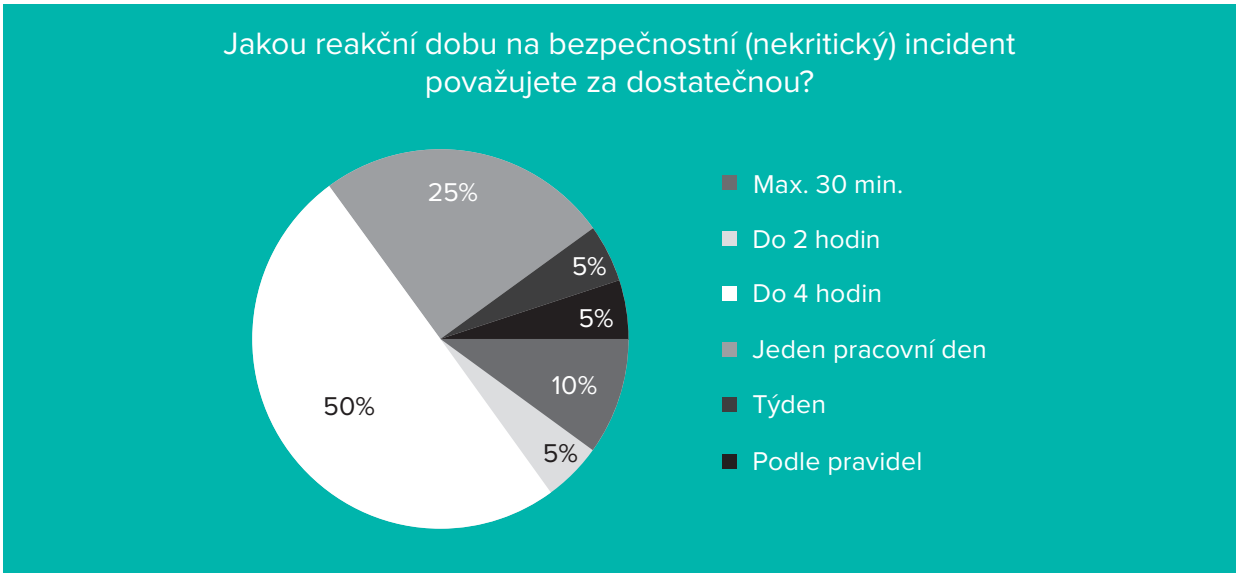
Kybernetické bezpečnostní incidenty představují „denní chleba“ každého, kdo se stará o bezpečnost podnikového IT prostředí. Přibližně třetina z oslovených dle svého vyjádření zvládá řešit každý detekovaný bezpečnostní incident, což je třeba ocenit. Stejný počet respondentů odpověděl, že sice zvládají řešit každý odhalený bezpečnostní incident, ovšem jeho řešení trvá delší dobu, než by bylo vhodné. Čtvrtina dotázaných se zabývá pouze nejkritičtějšími incidenty.



V posledních letech pokračuje nepříznivý trend růstu počtu kybernetických útoků. Jedním z hlavních důvodů k tomu je zvyšující se počet zranitelných zařízení připojených k internetu. Zranitelností využívají útočníci k napadení firemních počítačových sítí, které ochromí ransomwarem nebo odcizí podniková data či IT infrastrukturu poškodí jinými způsoby.

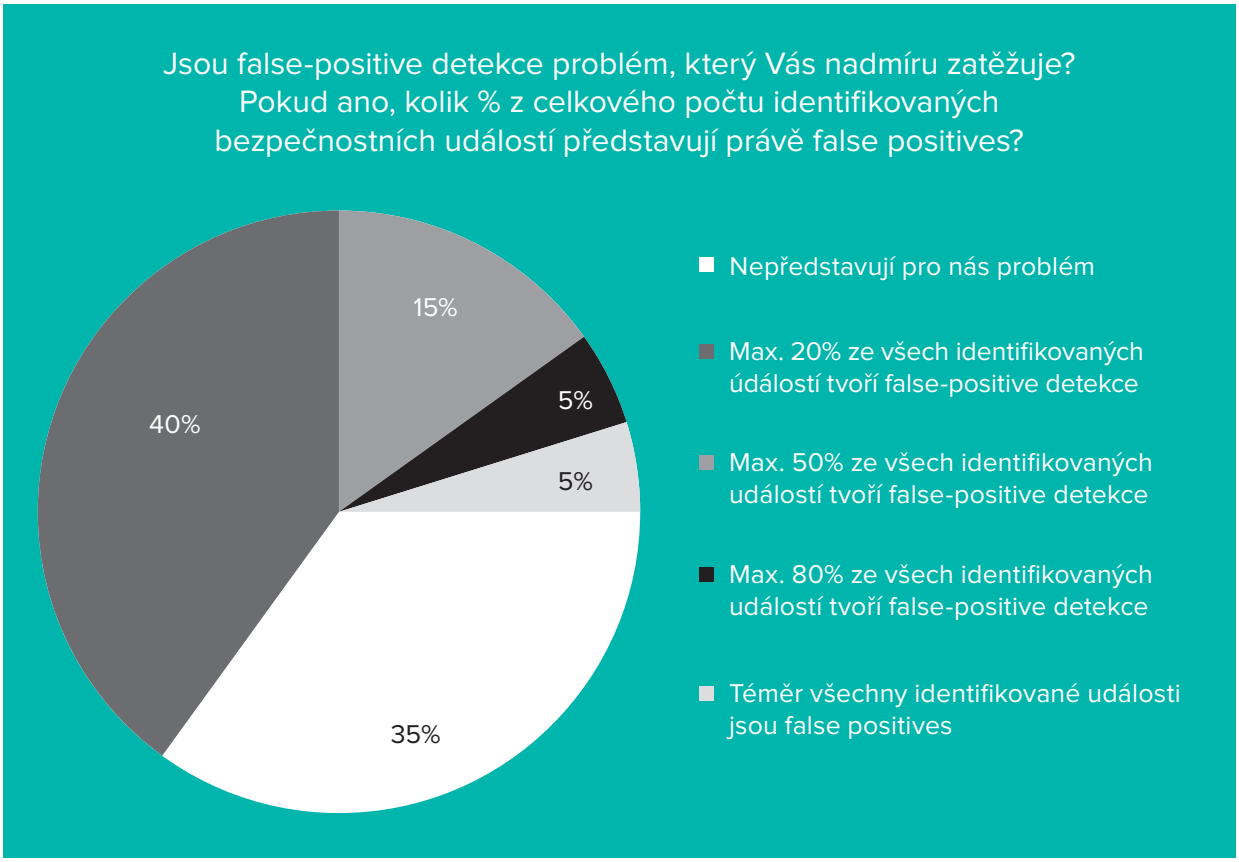
Pravidelné skenování zranitelností infrastruktury by proto měla provádět každá organizace. S tím souhlasí polovina účastníků průzkumu. Ta za optimální přístup ke zvládání zranitelností považuje implementaci kontinuálního vulnerability managementu. Naproti tomu si 15 % institucí vystačí s jedním skenem zranitelností měsíčně.

Včasné řešení kybernetických bezpečnostních incidentů může být klíčovým faktorem, který nakonec rozhodne, jaká bude konečná škoda daného incidentu. Prioritizace incidentů dle jejich závažnosti je proto nezbytná. Dostatečná doba pro řešení nekritického bezpečnostního incidentu odpovídá dle poloviny dotázaných max. 4 hodinám.



Chybné detekce zranitelností a bezpečnostních slabin a incidentů, tzv. „false-positive“ detekce, mohou tvořit velkou část výstupů z automatizovaných skenů sítě, IPS, SIEM a dalších systémů. Jejich následná analýza tak představuje plýtvání časem a zdroji organizace. Jsou tedy false-positive detekce problém, který pracovníky IT nadměrně zatěžuje?

Pro třetinu společností false-positive detekce nepředstavují žádný problém, u obdobného počtu společností se nejedná o více jak 20 % ze všech identifikovaných událostí.



V okamžiku, kdy dojde k objevení kybernetického bezpečnostního incidentu, je třeba se jím zabývat. Reakce na incidenty musí být vždy řízena konkrétním pracovníkem či celým týmem zodpovědných osob. Kolik lidí je v organizacích oficiálně zodpovědných za reakci na incidenty? V našem průzkumu odpověděla čtvrtina dotázaných, že zodpovědní jsou 2 pracovníci, v pětině organizací to jsou 3 zaměstnanci, 30 % institucí si zvolilo tým 4 lidí.

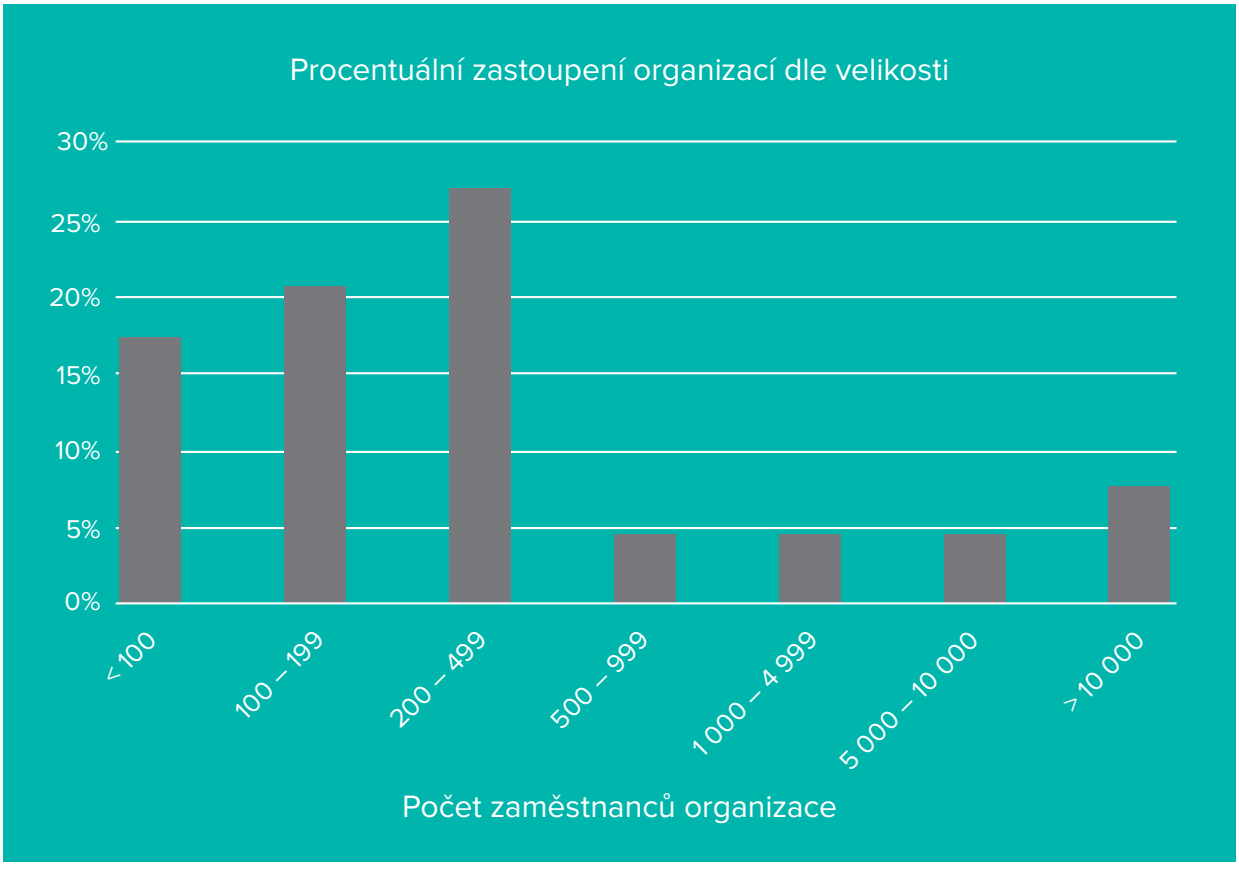
Trendy v oblasti bezpečnostního vzdělávání

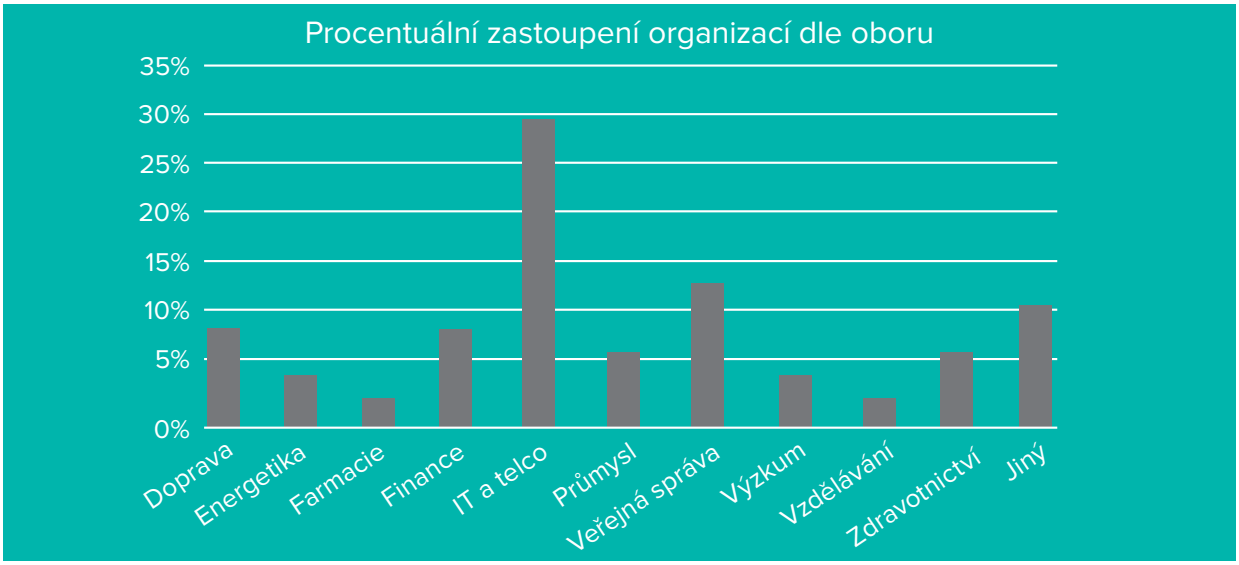
Radek Švadlenka

Vzdělávání zaměstnanců v oblasti kybernetické bezpečnosti se stává 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.

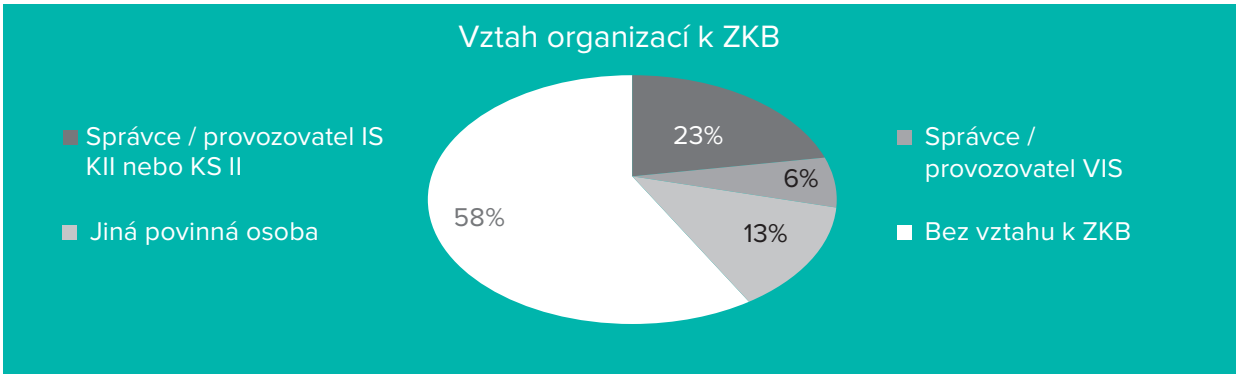
Není tedy žádným překvapením, že zákon o kybernetické bezpečnosti vyžaduje od povinných subjektů realizovat bezpečnostní opatření v podobě stanovení plánu rozvoje bezpečnostního povědomí, jehož cílem je zajistit odpovídající vzdělávání a zlepšování bezpečnostního povědomí uživatelů, administrátorů a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

Už v loňském roce jsme uveřejnili výsledky průzkumu zaměřeného na realizované a plánované vzdělávací programy a aktivity organizací s velmi zajímavými výstupy. Abychom byli schopni sledovat trendy ve vývoji těchto aktivit, připravili jsme pro Vás nový průzkum za rok 2019 s ohledem na plánovaná opatření pro rok 2020. Jistě bude zajímavé i porovnání hodnot před rokem plánovaných vzdělávacích aktivit s reálným výstupem za rok 2019. Průzkumu se zúčastnilo bezmála sto subjektů různých zaměření a velikostí, jak je vidět z grafů níže.



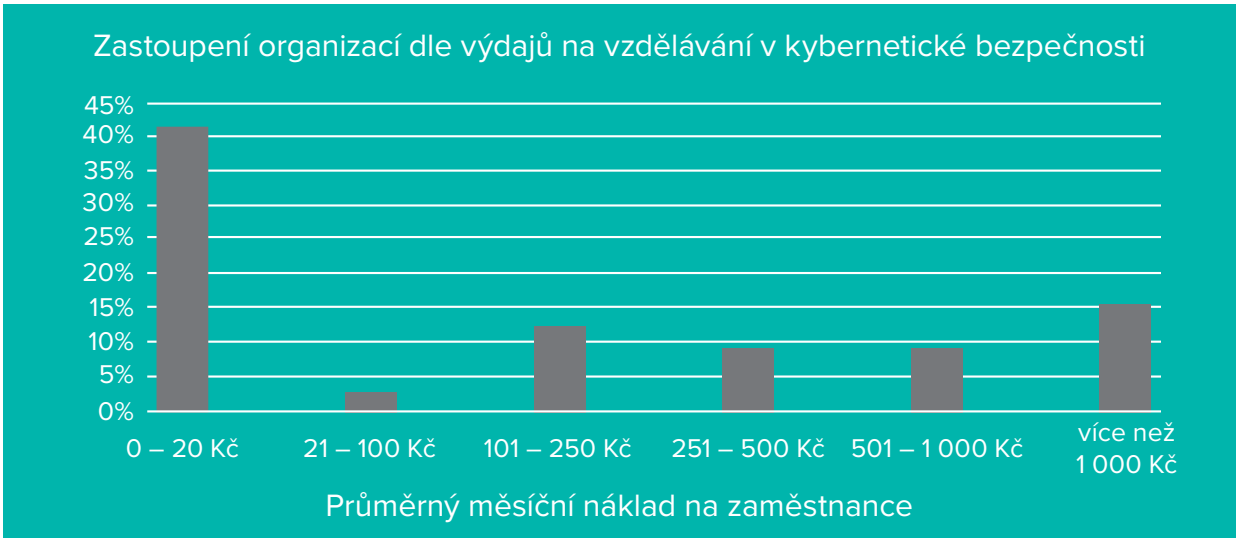


Aby interpretace jednotlivých výstupů nebyla zkreslena, je třeba upřesnit, že necelá polovina respondentů průzkumu se řadí mezi povinné subjekty podle zákona o kybernetické bezpečnosti, jak ilustruje následující graf.



Vzdělávání v oblasti kybernetické bezpečnosti může být řešeno pomocí interních aktivit, často je však spojeno s investicemi do externích zdrojů, jako jsou prezenční školení nebo e-learningové nástroje.

Kolik prostředků vynaložily jednotlivé organizace na vzdělávání zaměstnanců v roce 2019, je možné pozorovat v níže uvedeném grafu. Výstup naznačuje, že poměrně velké množství subjektů se nachází na úrovni minimálních investic, zároveň je však patrné, že 16 % respondentů investuje v průměru více než 1000 Kč měsíčně na zaměstnance do vzdělávání v oblasti kybernetické bezpečnosti.

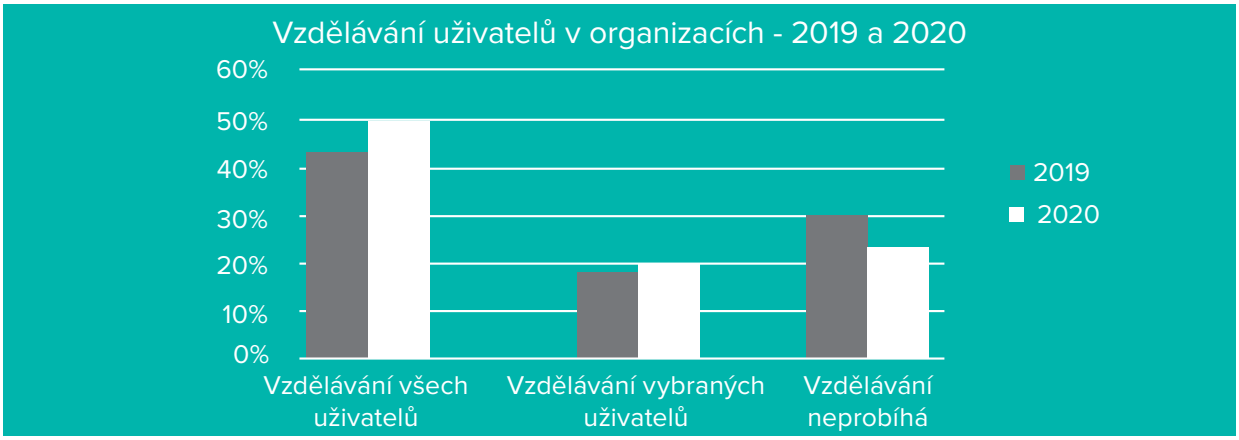


Vzdělávání uživatelů - realita versus plán

V této části průzkumu se zástupci organizací vyjadřovali k realizovaným a plánovaným aktivitám v oblasti vzdělávání uživatelů s výjimkou bezpečnostních rolí. Zatímco přibližně 34 % respondentů uvedlo, že v roce 2019 žádné vzdělávání nerealizovalo, ve výhledu pro rok 2020 byla tato hodnota již o 8 % nižší, což lze jednoznačně hodnotit pozitivně.

Tento trend by se měl promítnout zejména ve zvýšení počtu organizací, které chtějí investovat do vzdělávání všech uživatelů, a to až na 52 % sledovaného počtu respondentů v roce 2020.

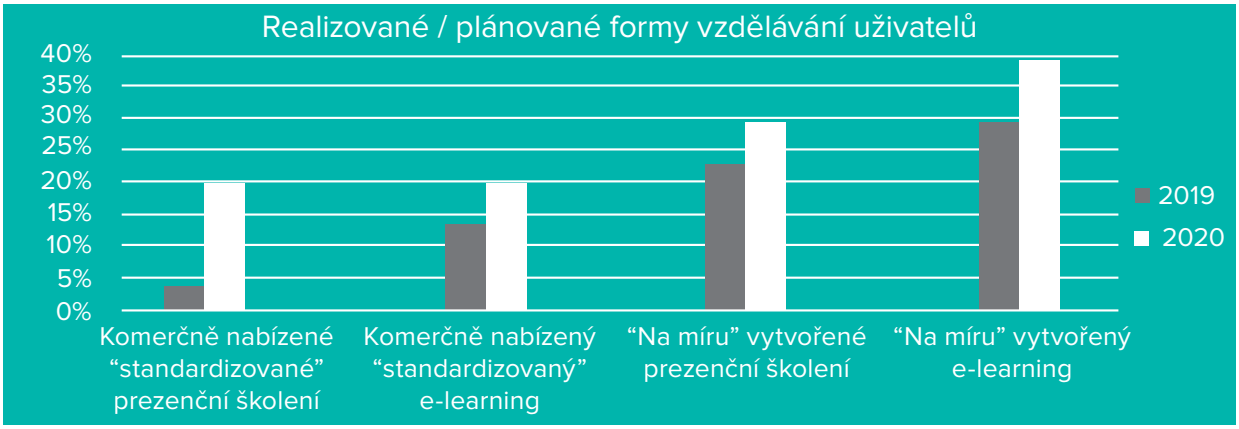
Mírný nárůst hodnot se dá očekávat i v kategorii vzdělávání vybraných uživatelů. Zajímavé výsledky také poskytuje srovnání loňských výstupů za rok 2018 s hodnotami aktuálního průzkumu. Počet organizací, u kterých vzdělávání vůbec neprobíhá, se s odstupem času v podstatě nezměnil, a to i přestože část respondentů plánovala alespoň nějaká opatření zavést. Pro úplnost je třeba uvést, že průzkumy byly realizovány nad odlišnými vzorky respondentů, tedy výsledky srovnání mohou být zkresleny.



Za velmi optimistický je možné označit výhled na rok 2020 z hlediska využití různých forem vzdělávání uživatelů. Z odpovědí respondentů je patrný téměř dvacetiprocentní nárůst v plánu oproti reálně provedeným komerčně nabízeným prezenčním školením. Ani další formy vzdělávání však pravděpodobně nepřijdou zkrátka. V grafu níže je možné sledovat plánovaný nárůst ve všech kategoriích vzdělávání uživatelů, což opět potvrzuje pozitivní trend ve vývoji vzdělávacích aktivit. Pokud však porovnáme plánovaný rozvoj z průzkumu loňského roku s aktuálními výstupy, čísla už tak optimisticky nevypadají.

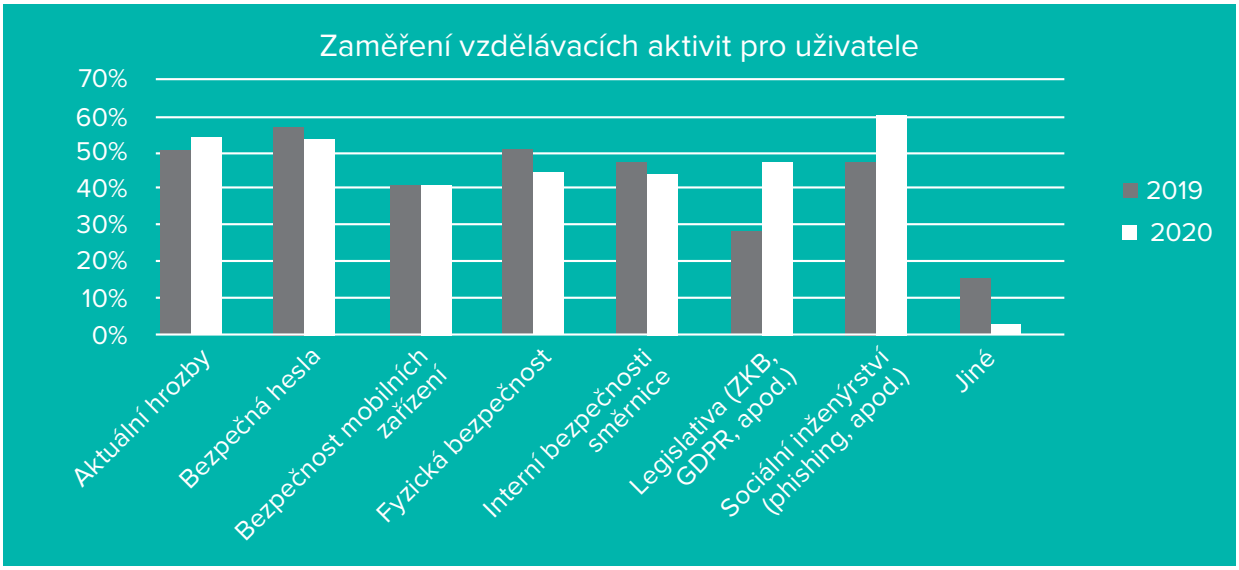
Například v kategorii komerčně nabízených e-learningových nástrojů zůstal reálný výsledek za rok 2019 téměř 10 % pod plány definovanými na počátku tohoto období. Tento fakt vede k závěru, že mnohé organizace plánují významný nárůst ve vzdělávacích aktivitách uživatelů, nicméně z různých důvodů pak tyto plány nebývají naplněny.

Nutno však znovu připomenout, že z důvodu různých výzkumných vzorků v jednotlivých letech nemají tyto výstupy vysokou vypovídající hodnotu.



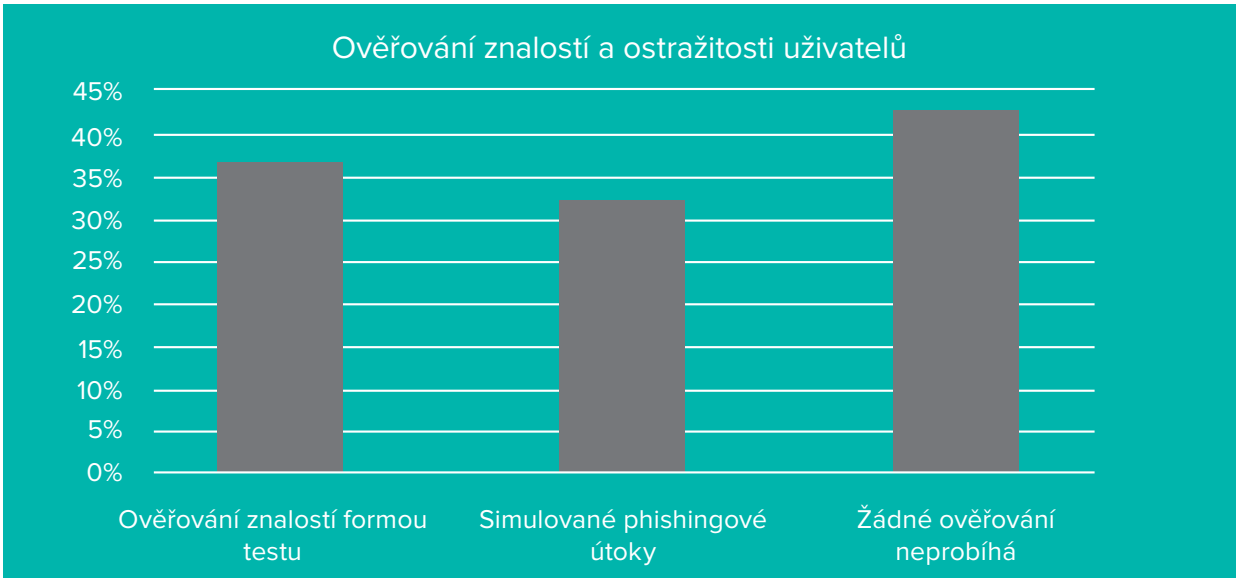
Cílení vzdělávání uživatelů na speciální oblasti neukazuje markantní rozdíly mezi již realizovanými aktivitami a plánem na rok 2020. Mírné výkyvy je možné sledovat v oblasti fyzické bezpečnosti, která pro rok 2020 pravděpodobně mírně zaostane oproti realitě roku 2019 se ztrátou sedmi procentních bodů, naopak růst vzdělávání uživatelů je plánovaný v problematice legislativy a také v oblasti sociálního inženýrství.

Tento výsledek koresponduje s předpokladem, že stále více organizací si uvědomuje rostoucí intenzitu hrozeb spojených s phishingovými útoky a potřebou zvládat základní povinnosti v souladu s aktuální právní úpravou.



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.

Překvapením může být poměrně vysoký počet organizací (45 %), které nerealizují žádné metody ověření znalostí a ostražitosti uživatelů. Zároveň pouze 35 % respondentů realizovalo v roce 2019 simulované phishingové útoky. Pro úplnost je třeba doplnit, že provádět alespoň nějakou formu ověřování v roce 2020 je rozhodnuto bezmála 68 % organizací, které se zúčastnily výzkumu.

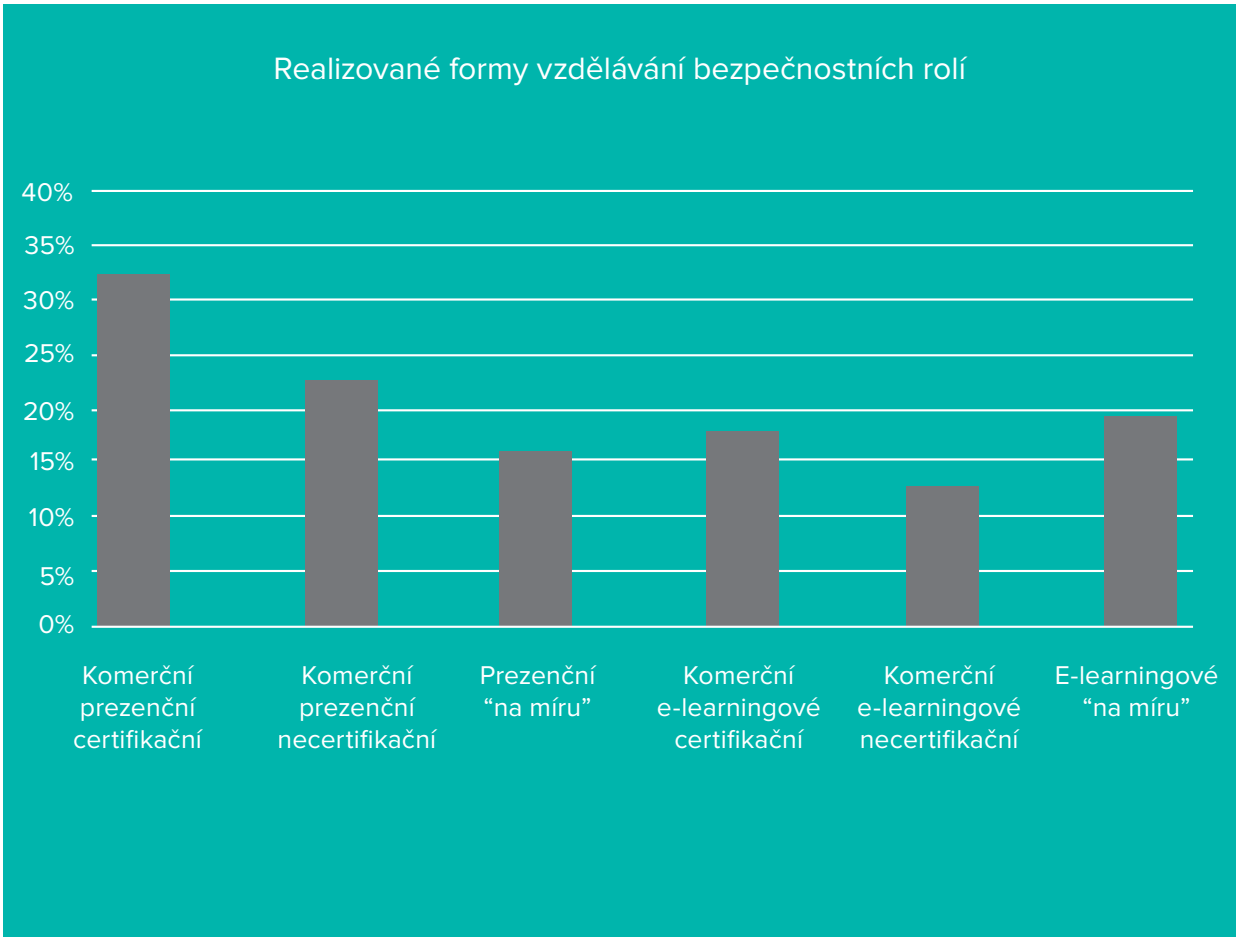


Vzdělávání odborných rolí

Zaměstnanci zastávající bezpečnostní role jsou klíčoví pro realizaci a udržitelnost bezpečnostních pravidel v organizaci. Jejich znalosti a dovednosti mohou mít významný dopad na efektivitu zvládání bezpečnostních incidentů.

Z výstupů šetření (viz graf níže) je zřejmé, že více než třetina organizací, které se účastnily průzkumu, preferovalo komerční školení zakončená certifikacemi. V rámci ostatních odborných prezenčních vzdělávacích aktivit naopak bylo nejméně využíváno možnosti školení vytvořeného na míru organizaci.

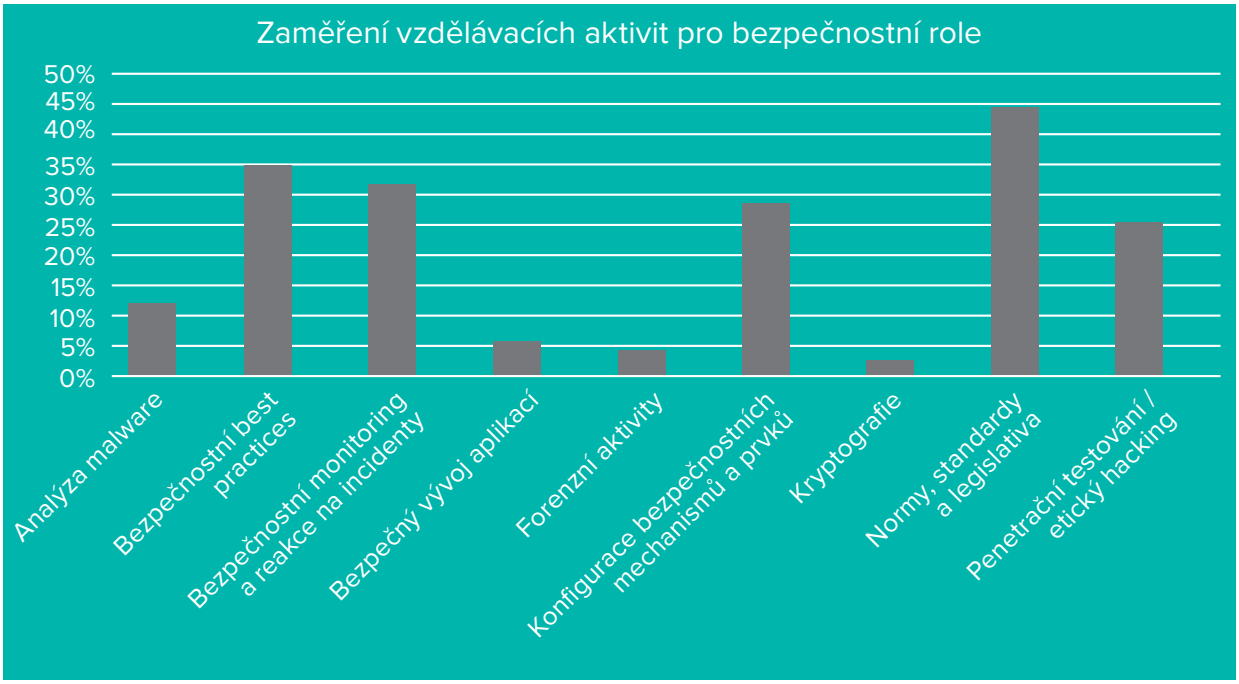
Naopak v oblasti e-learningových nástrojů bylo preferovanou volbou využití na míru šitého vzdělávacího programu. Vzhledem k poměrně omezené velikosti zkoumaného vzorku v kombinaci s velmi malým množstvím speciálně zaměřených pracovníků nemusí výstup tohoto výzkumu plně korespondovat s realitou v podobě komplexní reprezentace organizací v ČR.



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 best practices, konfigurace bezpečnostních mechanismů, bezpečnostní monitoring a reakce na incidenty a také penetrační testování a etický hacking. Každé z výše vyjmenovaných zaměření vzdělávání bylo využito v roce 2019 přibližně třetinou respondentů.

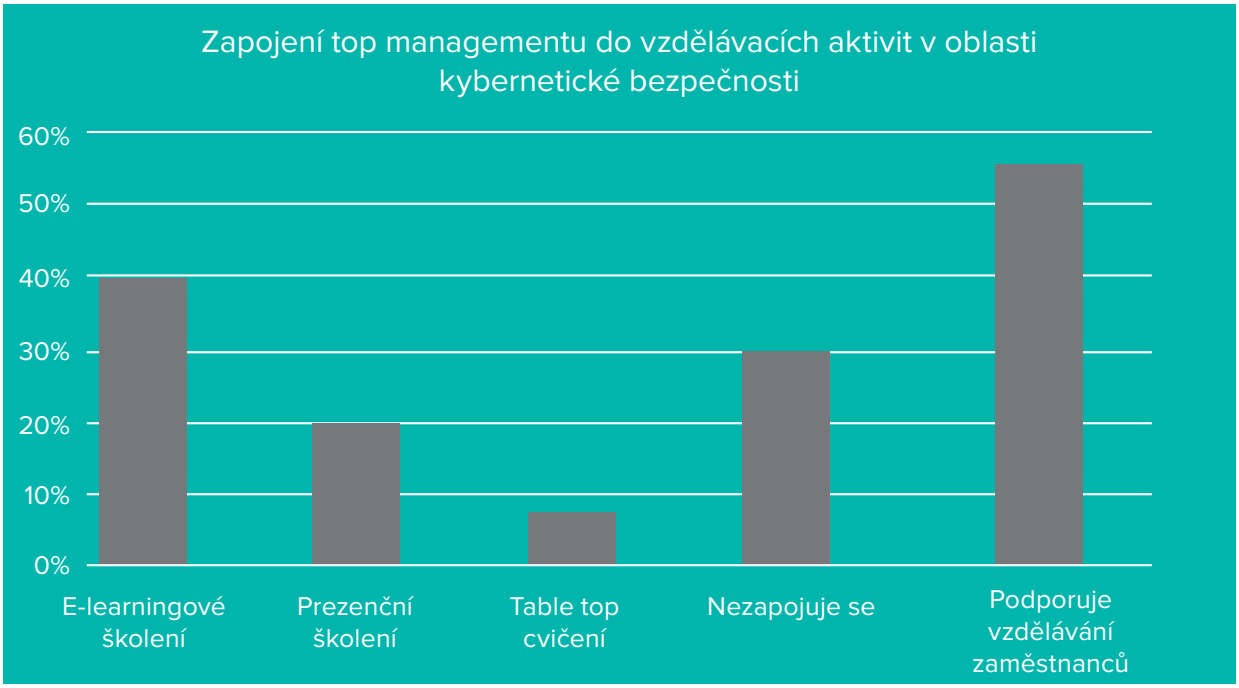
Mezi aktuálně „slabá“ témata z hlediska vzdělávání bezpečnostních rolí je možné zařadit oblasti kryptografie, forenzních aktivit a bezpečného vývoje aplikací, které nedosáhly z hlediska využití nad testovacím vzorkem hranice deseti procent, jak je patrné z grafu níže.



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 téměř 60 % zástupců vrcholového vedení organizací, jež se zúčastnily průzkumu, podporuje vzdělávání zaměstnanců v kybernetické bezpečnosti. Více než 40 % respondentů uvedlo, že se top management účastní e-learningových školení a 10 % dokonce „table top" cvičení. Smutným konstatováním pro dotčené subjekty může být naprostá absence vzdělávacích aktivit u 32 % respondentů.



Průmyslové systémy na českém a globálním internetu

Jan Kopřiva

Z médií se čas od času dozvídáme děsivé informace o útocích na průmyslové systémy (ICS – Industrial Control Systems). Většinou jde o útoky cílící na kritickou infrastrukturu určitého státu a za jejich zdroj bývají tradičně označovány jiné státy.

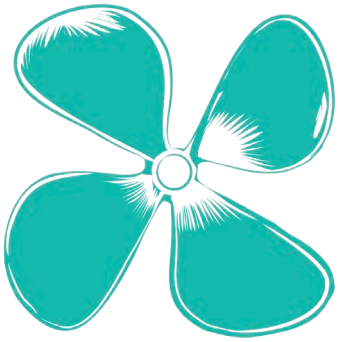
Vzhledem k tomu, že kritická infrastruktura zpravidla nebývá přímo připojená k internetu – bývá naopak oddělena od jakýchkoli jiných sítí v rámci nasazení v tzv. air-gapped režimu – musí být útoky vedené vůči ní většinou relativně sofistikované. I přes zmíněnou (obvyklou) absenci vysoce kritických průmyslových systémů na internetu by však bylo naivní domnívat se, že jiné, potenciálně méně kritické průmyslové systémy k internetu připojeny nejsou a nevystavují do něj citlivé služby… a že tyto služby nejsou cílem útoků.

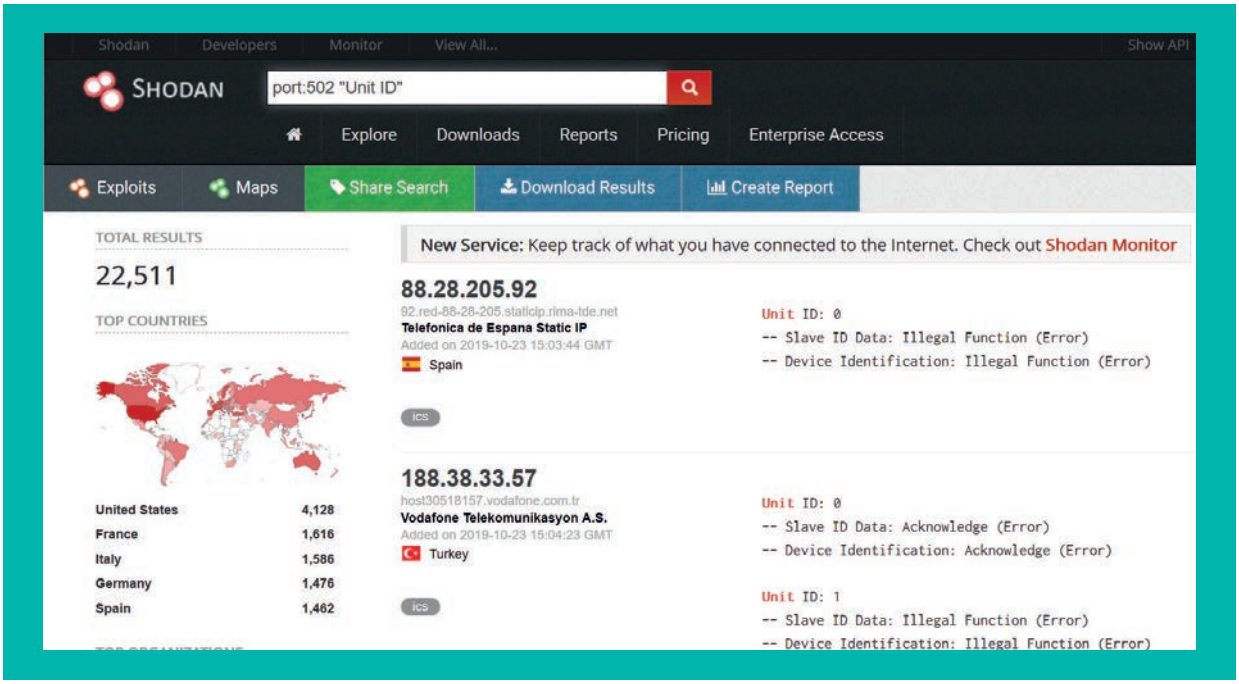
Vzhledem k tomu, že při návrhu většiny dnes používaných průmyslových protokolů nebyla příliš zohledňována bezpečnost (je to dáno tím, že jde o historické protokoly a v této oblasti tedy může být na místě analogie např. s HTTP v1.0 nebo SNMP v1) a mnoho z nich neposkytuje mj. ani žádné autentizační mechanismy, jejich přímé připojení k nezabezpečené síti – v extrémním případě k internetu – lze označit za více než nevhodné.

Vzhledem k výše uvedenému jsme se s kolegy z bezpečnostního týmu ALEF CSIRT v říjnu 2019 rozhodli analyzovat IP rozsahy českých ISP a zkusit, zda se nám podaří nějaké průmyslové systémy identifikovat. Výsledky této analýzy jsme publikovali na konferenci SCADA Security 4. listopadu 2019 a některé její výsledky si představíme i zde.

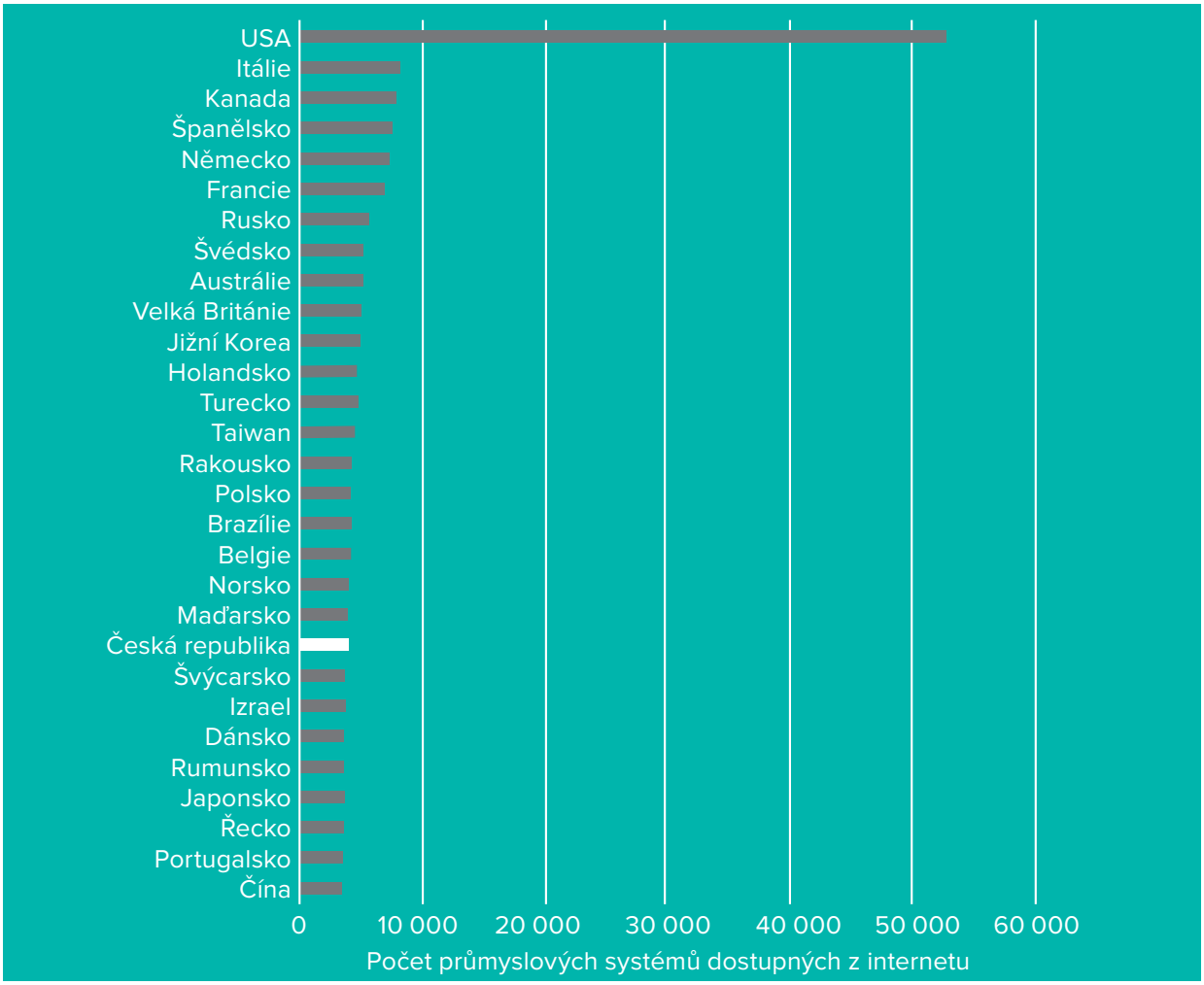
Vzhledem k tomu, že jsme chtěli být co možná nejméně invazivní vůči analyzovaným systémům, rozhodli jsme se sami neprovádět aktivní skeny ani s identifikovanými systémy, s drobnou výjimkou (viz níže), nijak neinteragovat.

Pro identifikaci průmyslových systémů (resp. systémů komunikujících s pomocí standardních průmyslových protokolů) připojených k internetu jsme se rozhodli využít informace ze služby Shodan. Tato služba kontinuálně prochází celý IP adresní rozsah internetu a zaznamenává otevřené porty a služby dostupné na jednotlivých IP adresách. Vzhledem k tomu, že ze Shodanu získává náš tým data o systémech v mnoha státech světa na denní bázi, měli jsme vedle aktuálních dat k dispozici i relativně zajímavý historický pohled na globální i českou situaci.



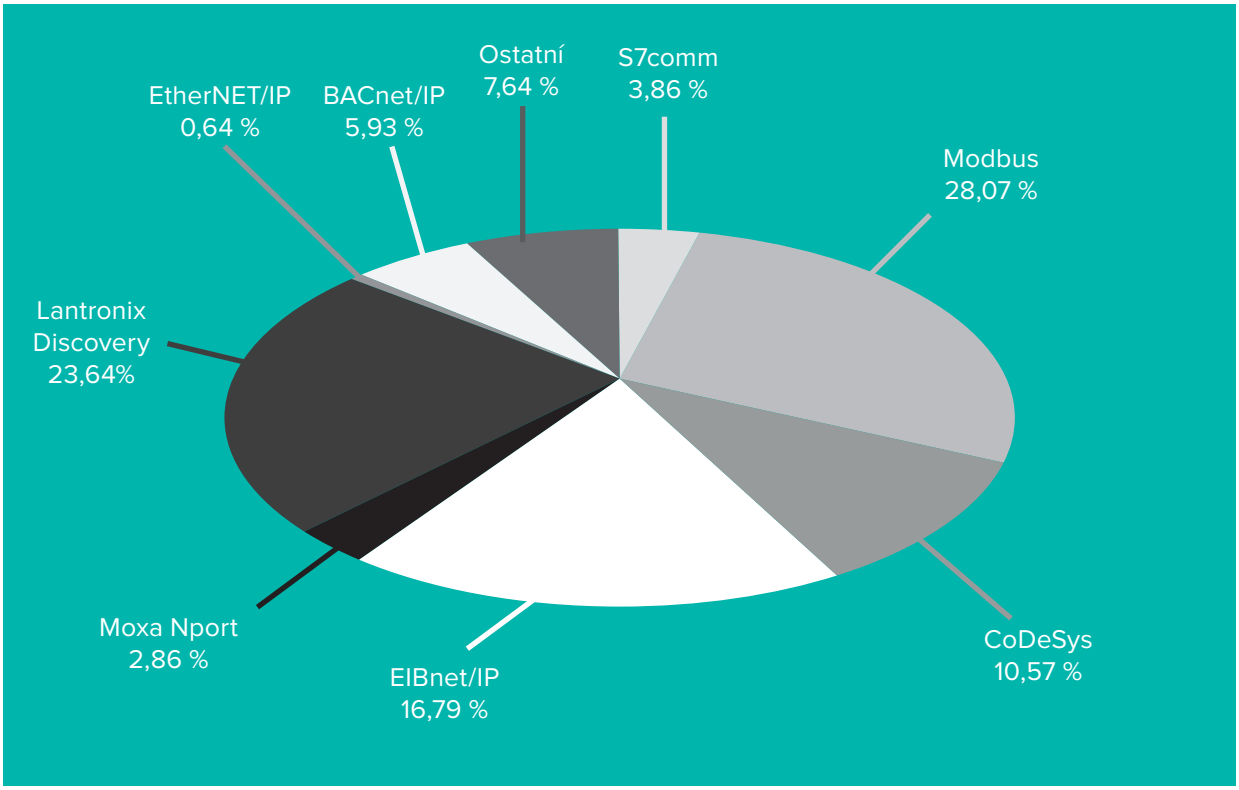


V prostředí českého internetu jsme na konci října s pomocí výše zmíněné služby identifikovali celkem 1400 průmyslových systémů, což, jak demonstruje následující graf, odpovídalo pomyslnému 21. místu mezi jednotlivými státy světa.



Na tomto místě je vhodné poznamenat, že absolutní hodnoty nutně neposkytují úplný obraz situace, vzhledem k tomu, že velikost IP adresních rozsahů náležících k jednotlivým státům, resp. přiřazených v nich působícím organizacím, se významně liší. Tato skutečnost vedla k tomu, že procentuální zastoupení průmyslových systémů v IP prostoru České republiky bylo například vyšší než jejich zastoupení v IP prostoru USA, kde je však z pohledu absolutních hodnot počet ICS připojených k internetu zdaleka nejvyšší.

Mezi průmyslovými protokoly, s pomocí nichž identifikovaná zařízení komunikovala, byly Modbus, Lantronix Discovery Protocol, ElBnet/IP a mnoho dalších (viz následující graf). Za poznámku přitom stojí, že převážná většina detekovaných protokolů buď vůbec neobsahovala podporu autentizačních mechanismů (a tedy bylo možné s pomocí nich průmyslové systémy ovládat bez jakékoli formy přihlášení), nebo autentizaci podporovala, nicméně byly známé zranitelnosti, které ji umožňovaly obejít. Připojení jakéhokoli systému, který s pomocí nich komunikuje, k nezabezpečené síti (jakou internet bezpochyby je) tak lze považovat za extrémně rizikové a nevhodné jednání.

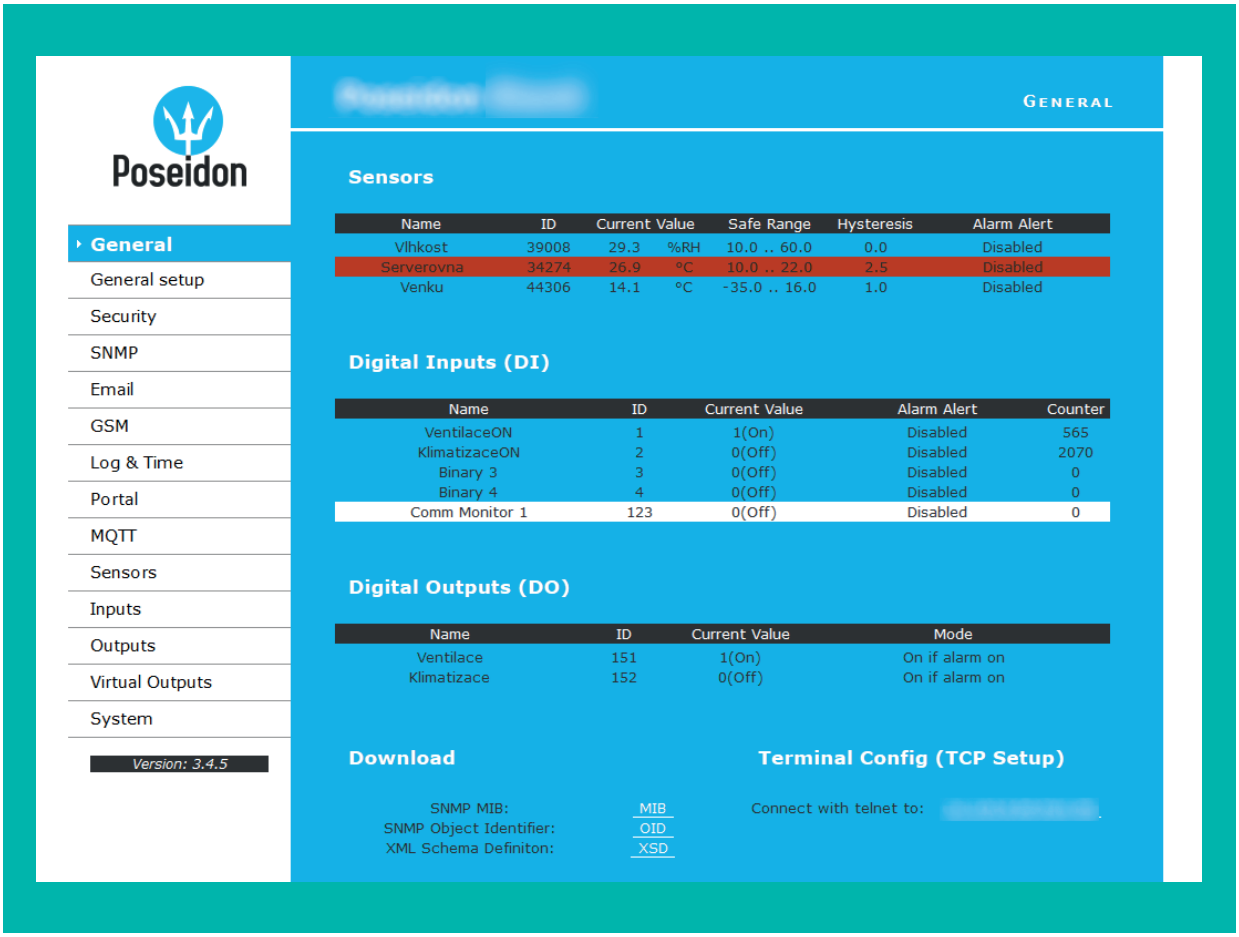


Výše uvedená možnost potenciálně neomezeného ovládání systémů využívajících průmyslové protokoly je o to děsivější, že mezi zařízeními připojenými k internetu, která se v průběhu analýzy podařilo identifikovat, byly kromě ovládacích systémů „chytrých“ budov a domácností, nebo systémů řízení vzduchotechniky a klimatizace, například i systémy pro řízení průmyslových procesů nebo výtahů a mnoho dalších relativně citlivých systémů.

Vzhledem k tomu, že poměrně velké množství průmyslových systémů v současnosti podporuje kromě komunikace s pomocí tradičních industriálních protokolů i webová rozhraní, provedli jsme po identifikaci IP adres, na nichž byla dostupná zařízení komunikující s pomocí průmyslových protokolů nalezena, také aktivní kontrolu otevřeného portu TCP 80 (protokol HTTP) a případné prověření na něm dostupných webových rozhraní.

Značné procento průmyslových systémů, které nějaké webové rozhraní poskytovaly, vyžadovalo přihlášení pro přístup k jakýmkoli řídicím funkcím.

V mnoha případech však bylo s pomocí webových rozhraní možné vzdálené systémy plně ovládat bez potřeby jakékoli autentizace.



Vzhledem k potenciálnímu nebezpečí spojenému s volnou dostupností průmyslových systémů na internetu jsme seznam identifikovaných IP adres předali Národnímu centru kybernetické bezpečnosti (NCKB) a Národnímu bezpečnostnímu týmu CSIRT.CZ s prosbou o informování subjektů, které spadají do jejich gesce a které citlivé systémy na internetu vystavují, o souvisejících rizicích. Oběma jmenovaným institucím bychom tímto chtěli opětovně poděkovat za součinnost. Lze předpokládat, že zejména v důsledku jejich zapojení (a potenciálně i díky publikaci výstupů z obdobné analýzy realizované třetí stranou, k níž došlo po prezentaci našich výstupů na konferenci SCADA Security) vykazoval za poslední dva měsíce roku 2019 počet k internetu připojených průmyslových systémů v České republice klesající trend, jak demonstruje následující graf.

Úroveň kryptografické ochrany internetového bankovnictví a nejnavštěvovanějších stránek v ČR a ve světě

Jan Kopřiva

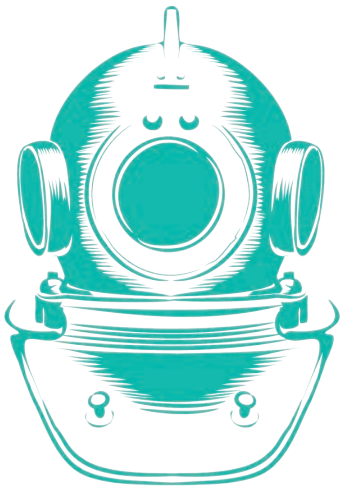
V průběhu roku 2019 realizoval bezpečnostní tým ALEF CSIRT několik analýz nastavení kryptografických protokolů SSL/TLS na různých typech webových portálů. Výsledky dvou z těchto analýz, které poskytují zajímavý pohled na zabezpečení nejpopulárnějších stránek v rámci ČR i světa a domácích a světových portálů internetového bankovnictví, jsou blíže popsány na následujících řádcích.

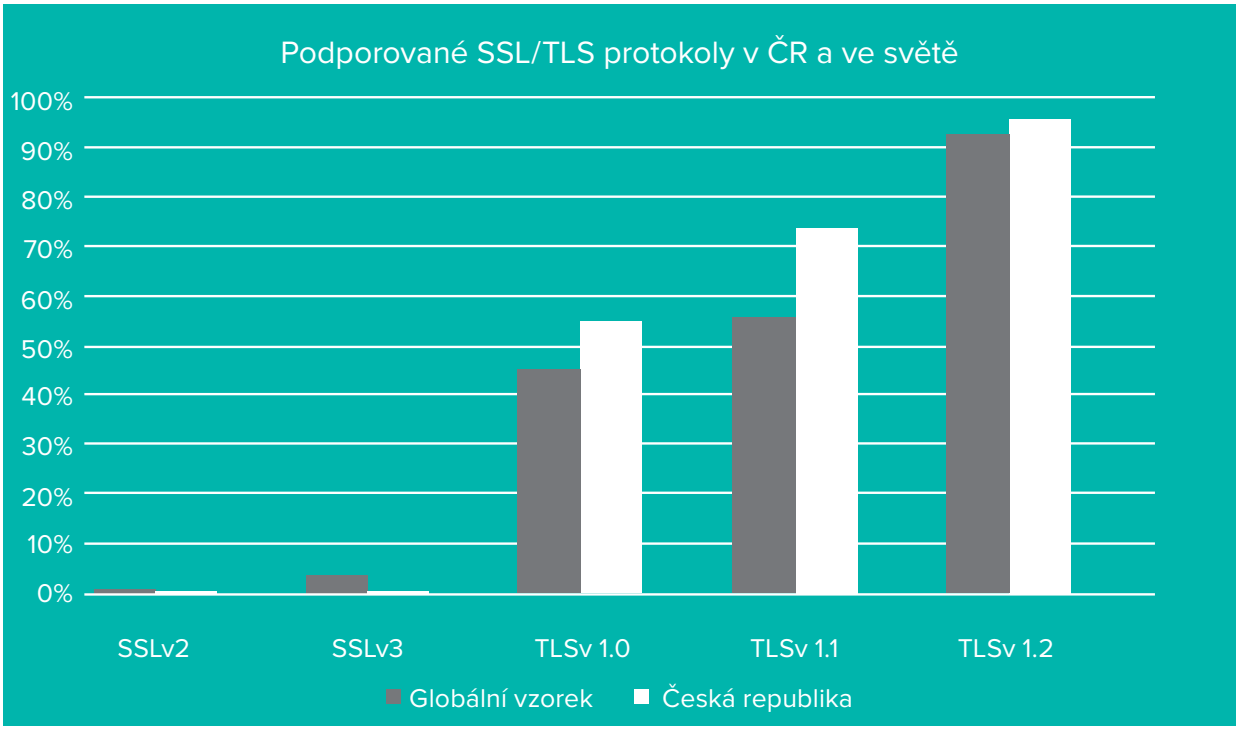
Obě zmíněné analýzy byly realizovány v průběhu prosince 2019. V první z nich jsme se zaměřili na identifikaci nastavení kryptografické ochrany přenosu dat u 1375 serverů internetového bankovnictví z celého světa z celkem 143 domén nejvyšší úrovně.

Cílem analýzy bylo identifkovat podporované kryptografické protokoly, sílu podporovaných šifrovacích sad (ciphersuites) a případné zranitelnosti jednotlivých serverů související s protokoly SSL a TLS. Pro možnost porovnání globální situace s tou domácí jsme následně analyzovali také podporu SSL a TLS na 32 serverech internetového bankovnictví provozovaných finančními institucemi působícími v České republice.

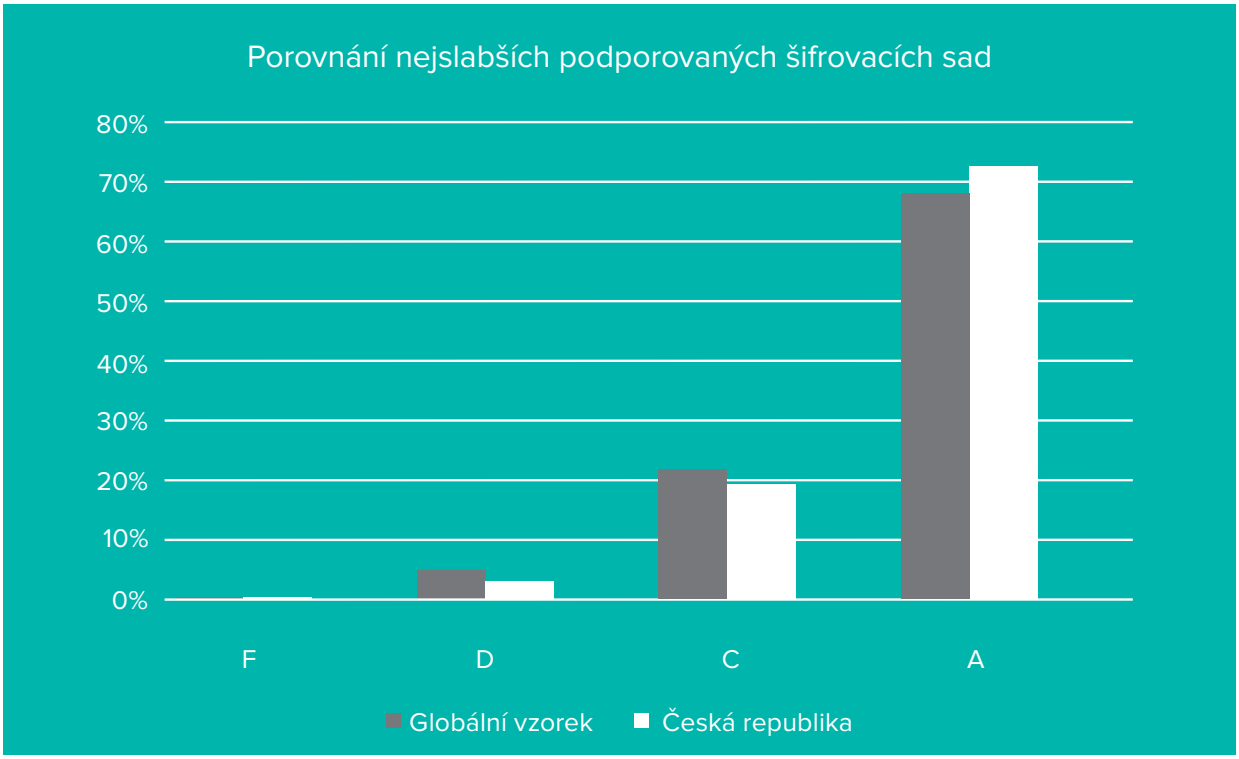
Všechny cílové servery byly oskenovány s pomocí nástroje Nmap za využití skriptů ssl-enum-ciphers a sslv2. Síla šifrovacích sad byla hodnocena na škále A (plně vyhovující) až F (velmi špatná) na základě modifikované verze metodiky SSL Server Rating Guide [1, 2] a v rámci hodnocení byla pro každý server určena nejslabší podporovaná šifrovací sada.

Výsledky analýzy byly u globálního vzorku až překvapivě špatné – více než tři procenta zkoumaných serverů stále podporovala protokol SSLv3.0 a téměř jedno procento dokonce protokol SSLv2.0. V obou zmiňovaných protokolech existují vysoce závažné zranitelnosti a jejich použití pro ochranu jakýchkoli služeb vyžadujících přenos důvěrných údajů přes síť je tak již mnoho let považováno za více než nevhodné [3, 4]. České servery byly, pokud jde o podporu protokolů, nastaveny podstatně lépe – ani jeden z nich nepodporoval protokol SSLv2.0 ani SSLv3.0 a všechny tak byly nastavené v souladu se soudobou dobrou bezpečnostní praxí. Za zmínku rovněž stojí, že v českém prostředí byla v případě všech serverů detekována podpora nejsilnějšího zkoumaného kryptografického protokolu TLSv1.2.





V oblasti nejslabších podporovaných šifrovacích sad byla situace u českých serverů rovněž lepší než u zkoumaného globálního vzorku, ani u všech domácích serverů internetového bankovnictví však nebyla situace zcela ideální. Pouze tři čtvrtiny serverů provozovaných finančními institucemi působícími v České republice podporovaly výhradně velmi silné šifrovací sady (hodnocené stupněm A). Necelých 22 % serverů pak podporovalo také šifrovací sady hodnocené stupněm C a v případě přibližně 3% serverů byla identifikována i podpora šifrovací sady hodnocené stupněm D. V případě globálního vzorku byla situace obecně horší. Zvláštní zmínku přitom zaslouží skutečnost, že téměř 0,3 % serverů podporovalo i používání šifrovacích sad hodnocených s pomocí nejslabšího stupně F.

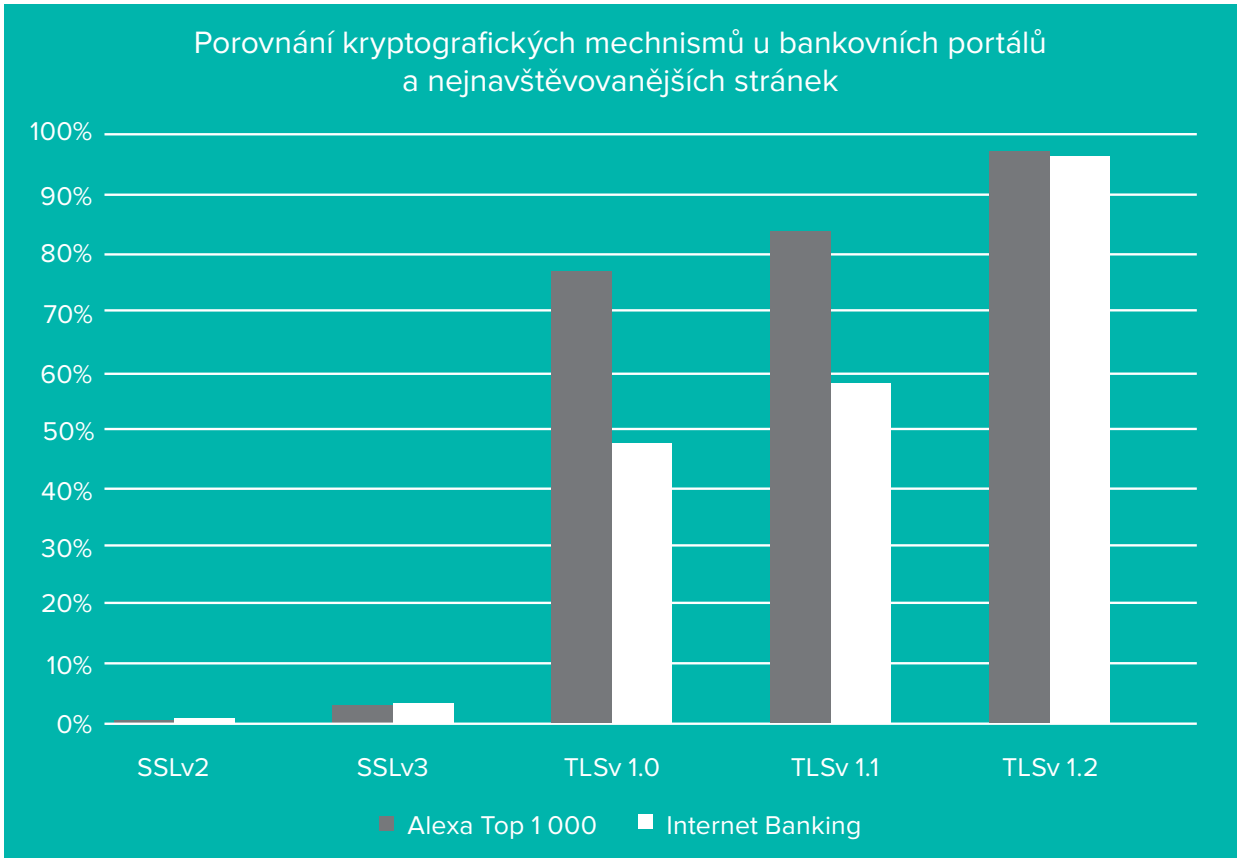


Pro zajímavost je možné uvést, že u jednoho z domácích serverů byla detekována i podpora slabé šifry RC4, jejíž použití je již mnoho let považováno za vysoce nevhodné [5]. Podpora stejné šifry pak byla detekována u 7 serverů z globálního vzorku.

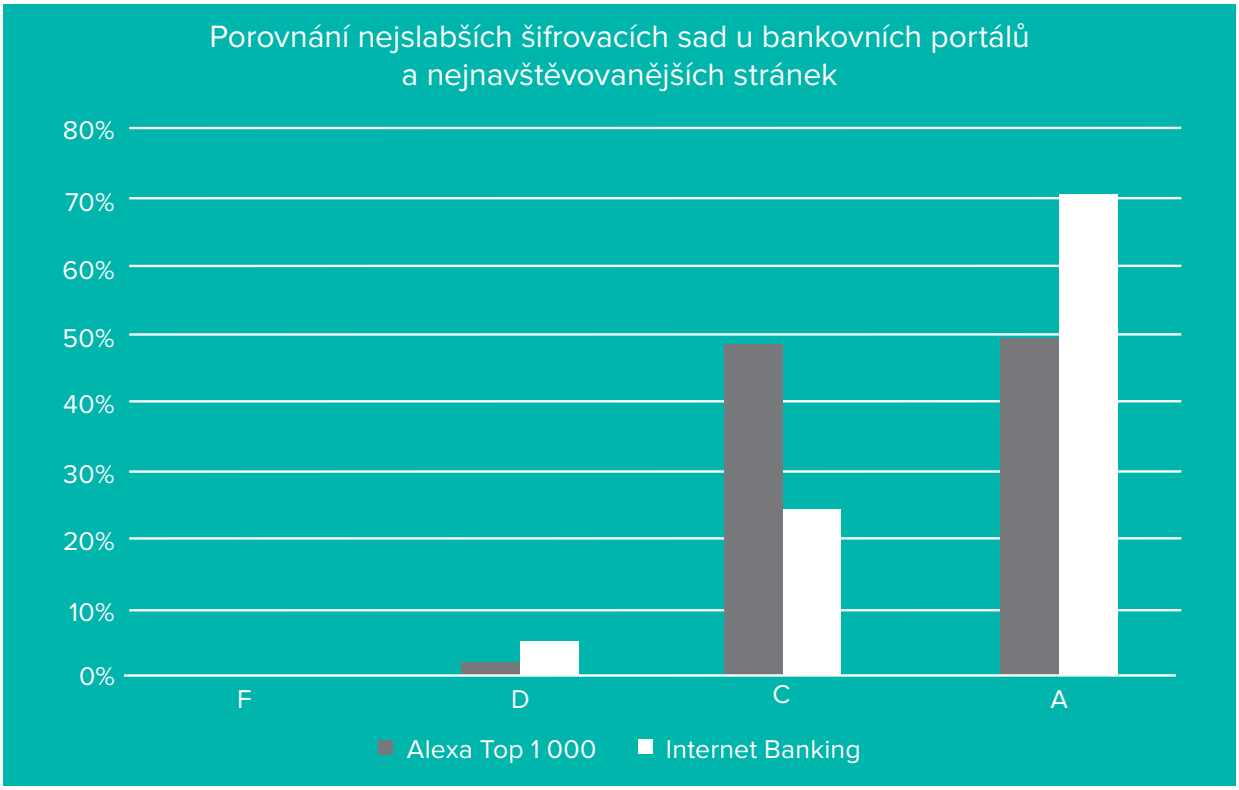
Druhá analýza týkající se používání SSL a TLS, kterou v návaznosti na prozkoumání stavu zabezpečení komunikace u portálů internetového bankovnictví ALEF CSIRT realizoval, se týkala nejpopulárnějších stránek na světě i v České republice dle ratingu Alexa Rank. Pro analýzu bylo zvoleno jednak tisíc celosvětově nejpopulárnějších domén (tedy seznam Alexa Top 1000) a po padesáti nejpopulárnějších doménách z každé z kategorií, které Alexa rozeznává.

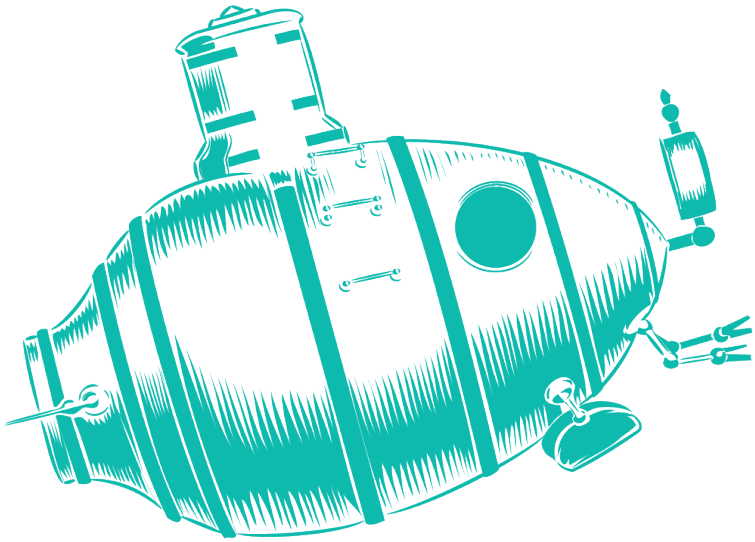
Z tisíce globálně nejpopulárnějších domén mělo přímé DNS záznamy jen 921. Přestože velikost tohoto vzorku není nikterak závratná, získané výsledky lze považovat za relativně rozumný orientační indikátor stavu nastavení SSL a TLS u populárních stránek obecně.

Jak ilustrují níže uvedené grafy, nastavení protokolů u nejpopulárnějších stránek bylo v některých ohledech vhodnější než u výše zmíněného globálního vzorku serverů internetového bankovnictví. Podpora SSLv2.0 byla detekována pouze u 0,32 % serverů, což je téměř o půl procenta méně než u bankovních serverů a téměř půlprocentní rozdíl byl patrný rovněž v případě podpory SSLv3.0. O téměř tři čtvrtě procenta častější než u serverů internetového bankovnictví pak byla mezi populárními weby podpora TLSv1.2.



V případě nejslabších podporovaných šifrovacích sad byla podstatně citelnější nižší orientace na bezpečnost u populárních stránek oproti bankovním portálům. Pouze 49,4 % nejpopulárnějších webů podporovalo pouze silné šifrovací sady. Dalších 48,43 % pak podporovalo i šifrovací sady hodnocené stupněm C.





Pro úplnost je vhodné zmínit, že podpora slabé šifry RC4 byla identifikována u celkem 12 serverů hostujících weby ze seznamu Alexa Top 1000.

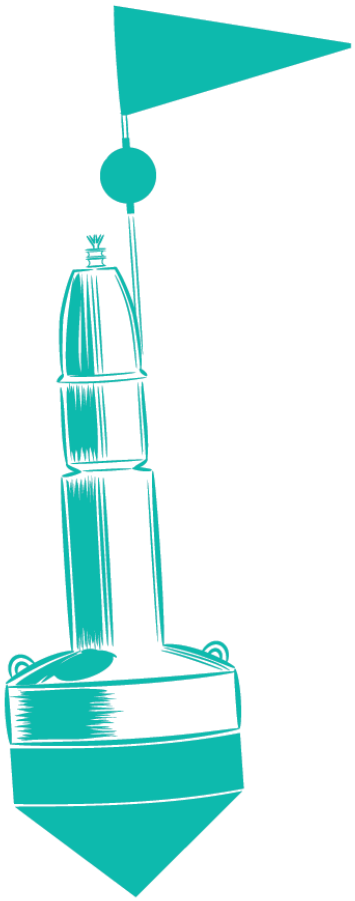
U jednotlivých kategorií, do nichž Alexa populární domény člení, se úroveň zabezpečení citelně rozcházela. Přestože vzhledem ke značně omezené velikosti zkoumaných vzorků nelze považovat níže uvedené hodnoty za reprezentativní, poskytují přinejmenším zajímavý pohled na stav zabezpečení u nejpopulárnějších stránek internetu v závěru roku 2019.

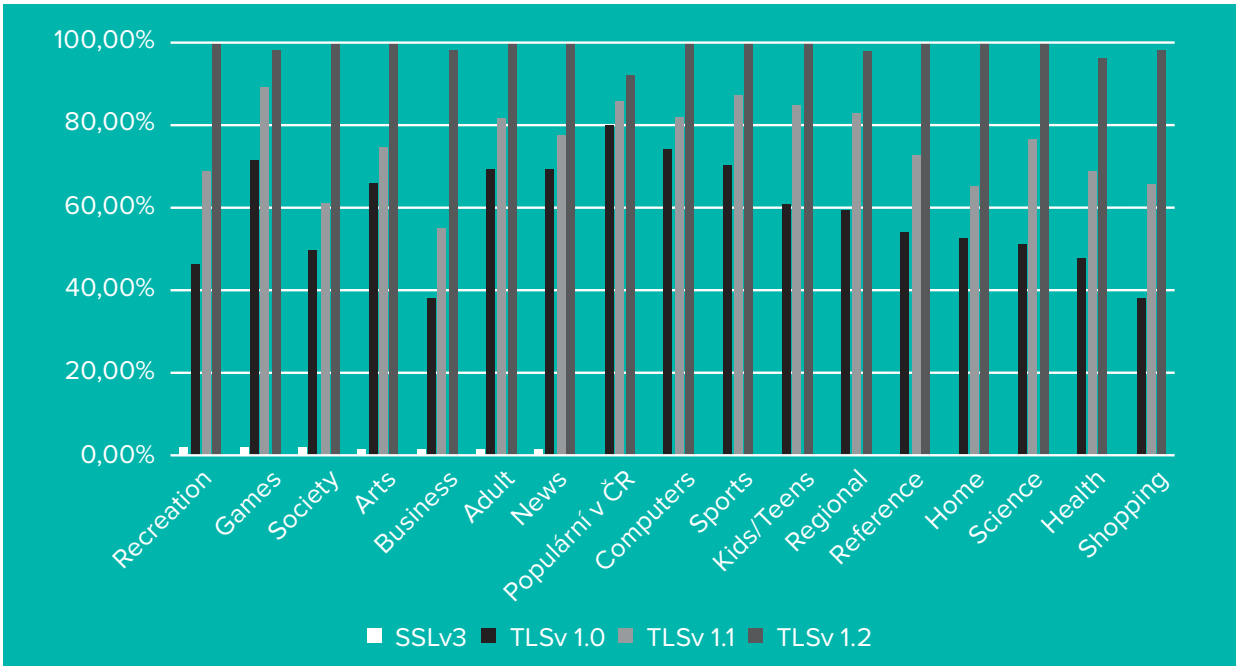
Zkoumán byl stav konfigurace SSL a TLS u následujících kategorií webů, platilo přitom, že pro každou kategorii bylo analyzováno 50 nejpopulárnějších domén. Tak jako u analýzy výše popsaného seznamu Alexa Top 1000, ani v tomto případě nebyly některé z domén směrované na žádnou IP adresu a u některých kategorií tak bylo otestováno méně než 50 serverů.

- Adult
- Arts
- Business
- Computers
- Games
- Health
- Home
- Kids/Teens
- News
- Recreation
- Reference
- Regional
- Science
- Shopping
- Society
- Sports
- Stránky nejpopulárnější v České republice

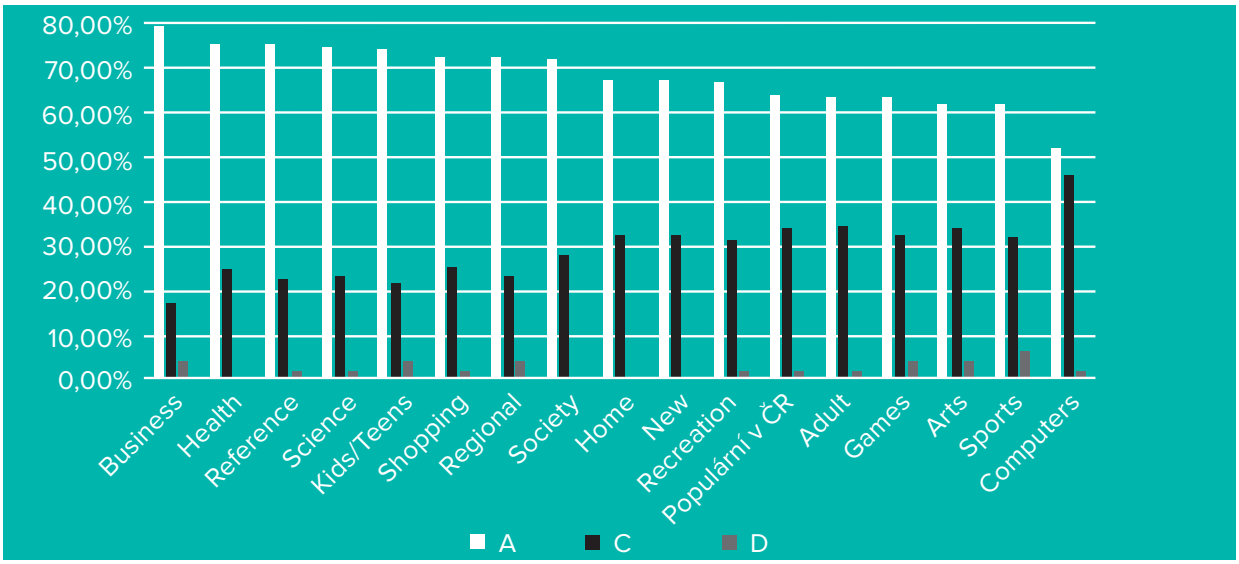
Je vhodné poznamenat, že žádný ze serverů zkoumaných v této fázi analýzy nepodporoval použití protokolu SSLv2.0. Podpora SSLv3.0 byla pak pozorována pouze u serverů v 7 ze 17 zkoumaných kategorií. Největší podíl podpory tohoto protokolu byl zjištěn u kategorie Recreation, tedy u domén věnovaných volnočasovým aktivitám. Šlo o 2,22 % ze zájmových serverů.

Podpora protokolu TLSv1.2 pak byla téměř univerzální – všechny zájmové servery jej nepodporovaly pouze v 6 kategoriích, přičemž jeho nejnižší podpora (pouze 92 % serverů) byla zjištěna u domén, které patří mezi nejpopulárnější v České republice.





Jak ilustruje následující graf, průměrně nejsilnější šifrovací sady podporovaly servery v kategorii Business – téměř 80 % z nich nepodporovalo jiné než velmi silné (hodnocené stupněm A) šifrovací sady. Průměrně nejslabší šifrovací sady pak, poměrně překvapivě, nabízely servery z kategorie Computers. Z nich podporovalo výhradně silné šifrovací sady pouze 52 %. Za zmínku stojí, že servery s podporou slabých šifrovacích sad hodnocených stupněm D byly identifikovány v celkem 13 ze zkoumaných kategorií. Nejvíce (přes 6 %) jich bylo zaznamenáno v kategorii Sports.



Na závěr je pro zajímavost možné uvést, že přestože stránky s „dospělou“, resp. pornografickou tematikou jsou zpravidla považovány za nepříliš dobře chráněné, zabezpečení přenášených dat u 50 nejpopulárnějších z nich bylo koncem roku 2019 silnější než u značného počtu serverů internetového bankovnictví [6].

[1] https://nmap.org/nsedoc/scripts/ssl-enum-ciphers.html
[2] https://github.com/ssllabs/research/wiki/SSL-Server-Rating-Guide
[3] https://tools.ietf.org/html/rfc6176
[4] https://tools.ietf.org/html/rfc7568
[5] https://tools.ietf.org/html/rfc7465
[6] https://untrustednetwork.net/en/2020/01/01/most-visited-adult-sites-actually-beat-some-e-banking-portals-when-it-comes-to-encryption/

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