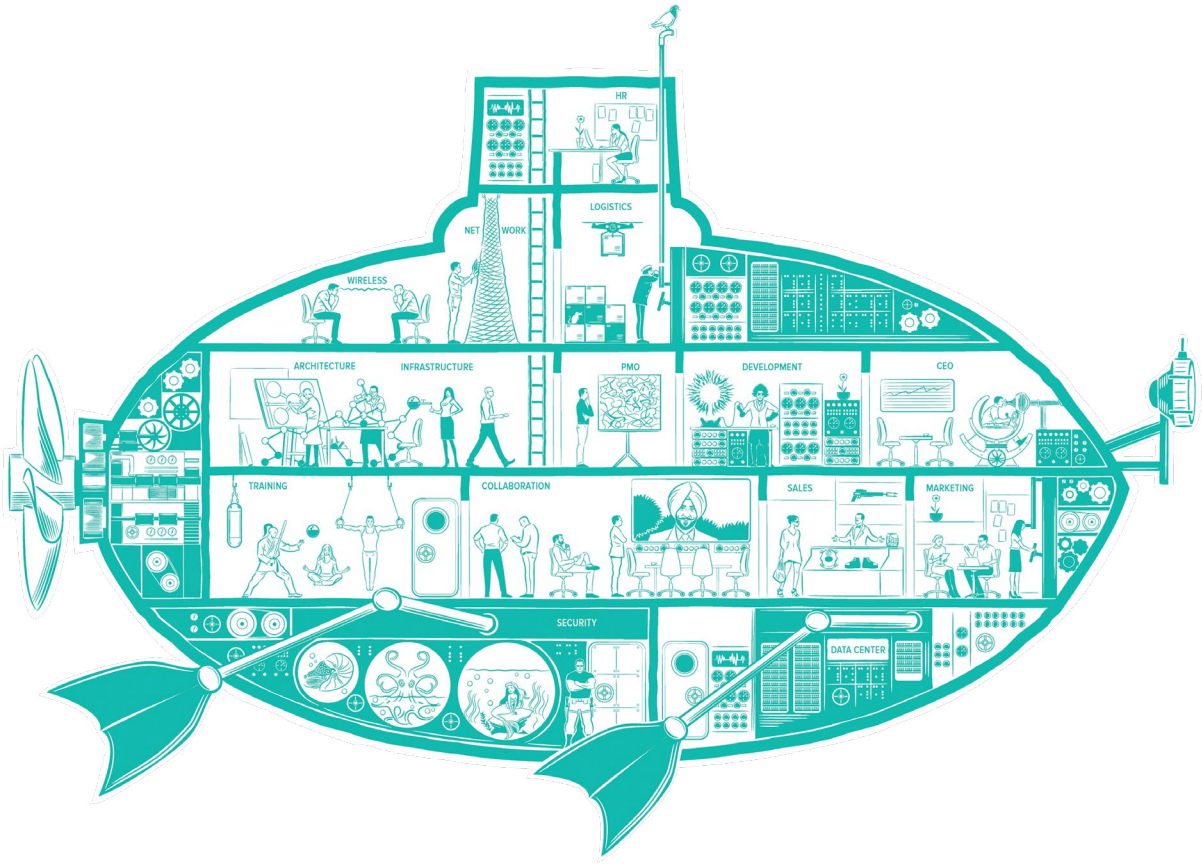
ALEF

Security Report 2019

Trust the Strong
www.alef.com

Obsah



Úvod

Úniky dat, ransomware, phishing. Vzhledem k počtu hrozeb, které na nás každý den cílí, je kybernetická a informační bezpečnost problematikou, kterou si nemůže dovolit opomíjet žádná moderní organizace. Hrozby se však neustále mění a je tak třeba sledovat trendy v této oblasti a držet s jejich vývojem krok.

Předložený report, vytvořený členy bezpečnostního týmu ALEF CSIRT a dalšími specialisty ALEF Group, obsahuje shrnutí podstatného dění ve vybraných oblastech informační bezpečnosti v roce 2018 – od vývoje zájmu organizací o specifické typy bezpečnostních služeb, přes trendy na poli hrozeb až po vývoj v oblasti bezpečnostního vzdělávání.

Unikátní je přitom tento text tím, že převážná většina uváděných dat a statistik se vztahuje specificky k prostředí České republiky. Analýza popsaných trendů tak může být mj. dobrým podkladem pro rozhodování o implementaci nových bezpečnostních opatření pro organizace, které v ČR působí. Z dostupných dat je například patrné, že v celosvětovém měřítku došlo v průběhu roku 2018 k poklesu výskytu různých typů škodlivého kódu. V datech týkajících se České republiky je ale naopak patrný citelný nárůst detekcí malwaru ke konci roku. Pro domácí organizace tak může být vhodné uvažovat na základě tohoto trendu například o implementaci pokročilých anti-malwarových nástrojů.

Zdrojem inspirace v rámci rozhodování o nových bezpečnostních opatřeních může být rovněž v reportu uvedená analýza bezpečnostního vzdělávání v českých organizacích, nebo shrnutí zájmu lokálních organizací o vybrané bezpečnostní služby v roce 2018.

Zájem o různé typy služeb a produktů bude bezpochyby zajímavé sledovat i nadále, neb již nyní jsou patrné určité rozdíly oproti loňskému roku. Vedle „stálic“, jakými jsou bezpečnostní audity a analýzy nebo penetrační testy, jsou například stále častěji poptávány vícefaktorové autentizační mechanismy, zvýšený zájem je však také o bezpečnostní služby a produkty spojené se zabezpečením průmyslových sítí a systémů, nebo o služby spojené s bezpečnostním logováním, monitoringem a analýzou.

V souvislosti s problematikou bezpečnostního logování a monitoringu 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 v České republice, ale také na celosvětové úrovni.

Vývoj zájmu o bezpečnostní služby v roce 2018

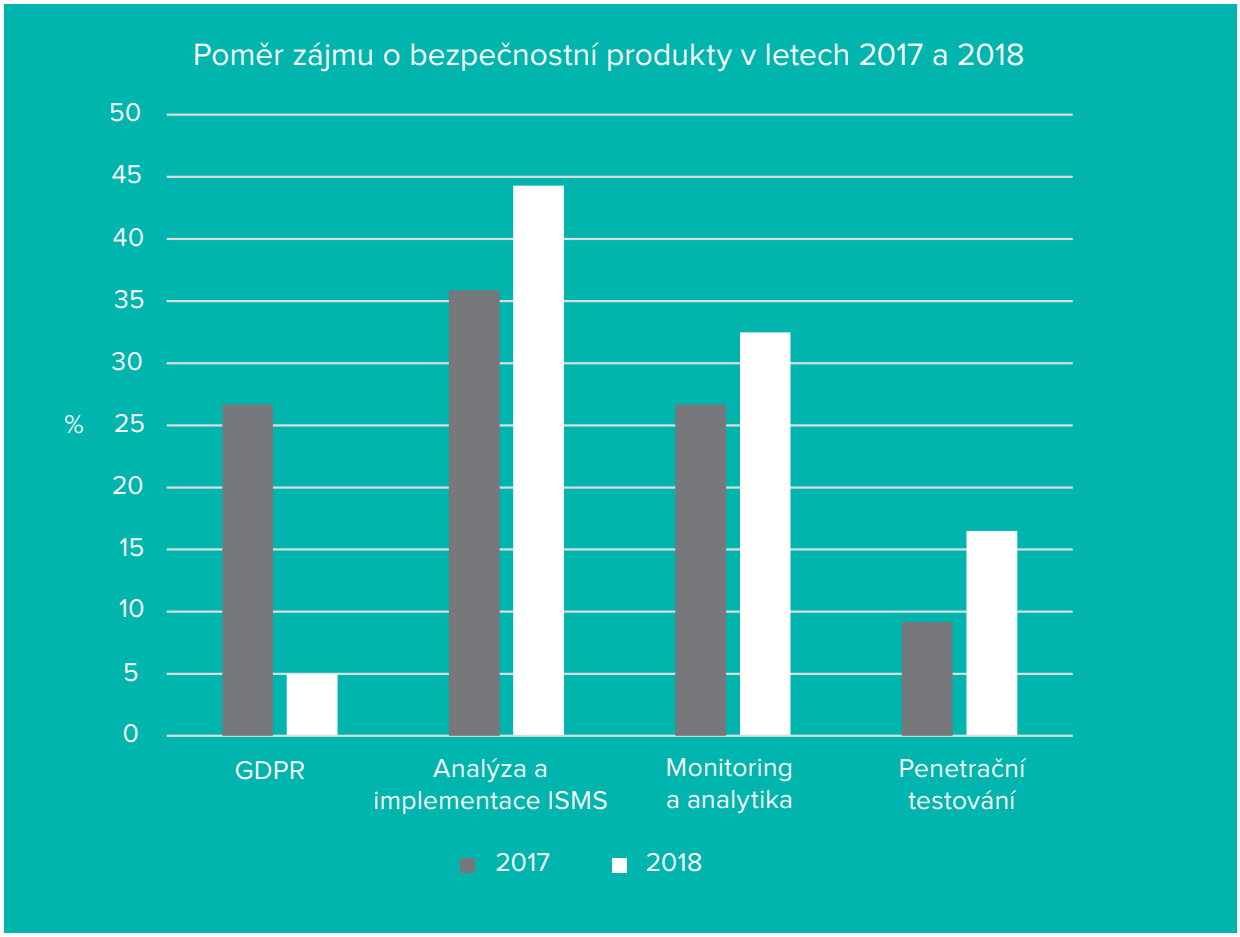
Jana Little

Oddělení ALEF Security se každoročně zabývá širokým spektrem bezpečnostních projektů. Se zvyšujícím se tlakem na organizační i technickou bezpečnost vnímáme nárůst poptávky po jednotlivých IT security službách. Na základě analýzy našich dat o požadavcích zákazníků byl v roce 2018 ze strany organizací zájem především o zajištění souladu jejich prostředí s normou ISO 27 001 a zákonem o kybernetické bezpečnosti. Zde je patrná souvislost s novelizací prováděcí vyhlášky. Není to ale jediný trend, který jsme pozorovali. V této části reportu se tak budeme zabývat vývojem poptávky po čtyřech nejčastěji objednávaných bezpečnostních službách a produktech v letech 2017 a 2018.

Z analýzy bezpečnostního oddělení ALEF NULA vyplývá, že v období 2017 – 2018 byl v oblasti služeb nejčastěji zájem o čtyři hlavní produkty s vazbou na bezpečnost. Jedná se především o:

- analýzy a další produkty spojené s GDPR
- analýzy a implementace ISMS
- návrhy a implementace bezpečnostních monitorovacích a analytických platforem
- penetrační testování

Obecně lze říci, že v roce 2018 oproti předchozímu roku citelně vzrostl zájem o tři z výše uvedených typů služeb, přičemž došlo k poklesu zájmu o služby spojené s GDPR. Zajímavější než absolutní hodnoty přitom může být poměr zájmu o nejčastěji objednané bezpečnostní produkty v letech 2017 – 2018, který shrnuje následující graf.



GDPR
Vzhledem ke vstupu obecného nařízení o ochraně osobních údajů ze dne 25. května 2018 v účinnost zaznamenalo Security oddělení v roce 2017 zvýšenou poptávku po konzultacích v rámci implementace GDPR. V roce 2018 pak zájem o tyto služby razantně klesl.

Analýza a implementace ISMS
Pod pojem Analýza a implementace ISMS zahrnujeme objednávky rozdílových analýz a implementací ISMS dle různých standardů.

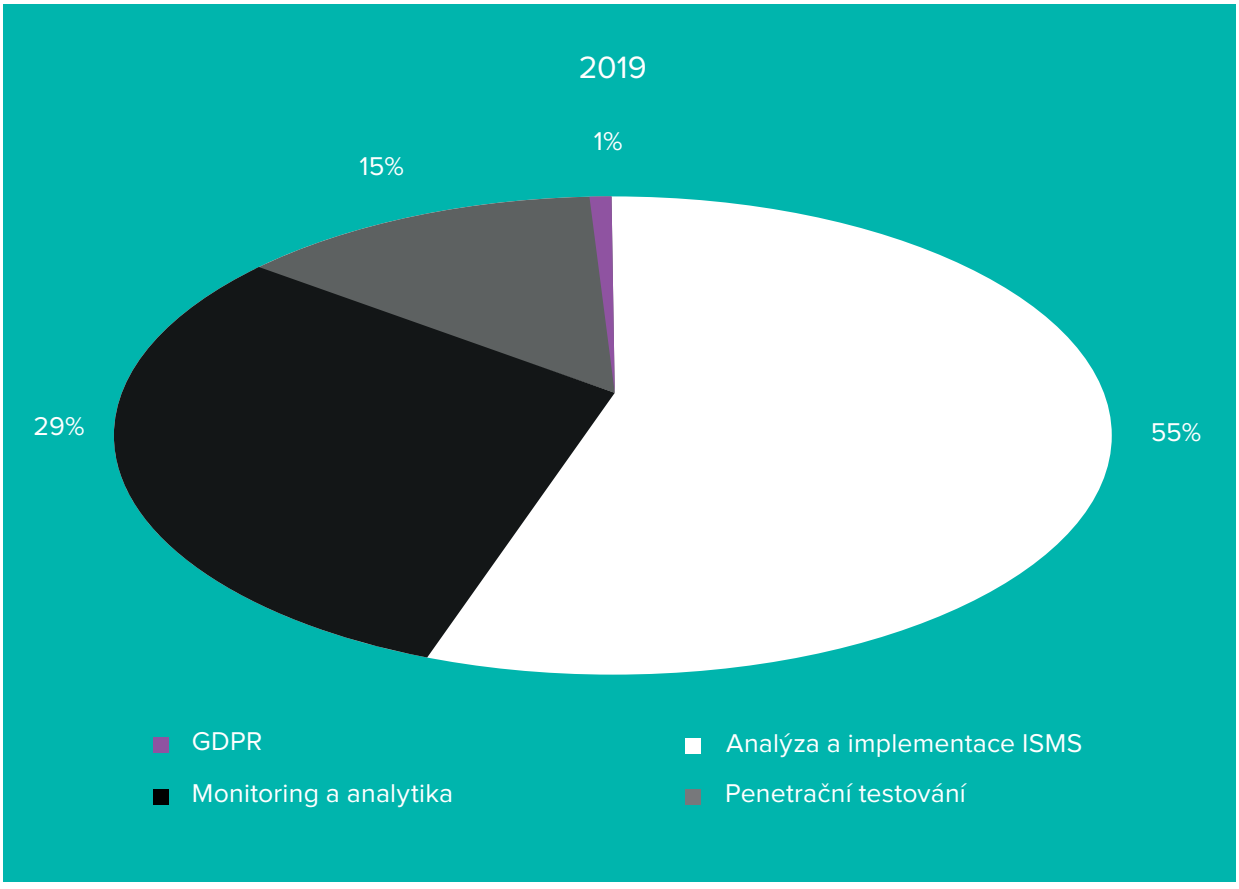
Zvýšený zájem zaznamenáváme zejména v oblasti ZKB, a to jak v rámci konzultací, tak i v jeho implementaci. V oblasti rozdílových analýz sledujeme poměrně konstantní vývoj v poptávce po posouzení stavu stávajícího prostředí proti požadavkům ZKB a také implementaci nápravných opatření vycházející z těchto analýz.

Zákazníci mají zájem především o:
- definování metodiky identifikace a hodnocení aktiv
- definování metodiky analýzy rizik
- identifikaci a hodnocení aktiv
- analýzu rizik
- vytvoření plánu zvládání rizik
- vytvoření plánu rozvoje bezpečnostního povědomí
- vytvoření strategie řízení kontinuity
- úpravu stávající dokumentace dle ZKB

Pro úplnost je vhodné zmínit, že narůstá také zájem o implementace rámců TOGAF a ITIL. Poměrně značná část objednaných bezpečnostních služeb spadá do oblasti bezpečnostního monitoringu a analýzy. Zde se jedná o konzultace, implementace i dodávání relevantních nástrojů.

Nejprudší růst zaznamenaly služby penetračního testování. V poslední době převládá zájem o prověření reálné odolnosti bezpečnosti informačních a komunikačních systémů. Výsledky penetračních testů také většinou ukazují, že je co zlepšovat.

Níže uvedený graf shrnuje aktuální (1Q 2019) rozložení zájmu o čtyři nejoblíbenější bezpečnostní produkty let 2017 a 2018.



Útoky, incidenty a další dění v roce 2018

Jan Kopřiva

Rok 2018 byl na počty útoků, incidentů i nových hrozeb bezpochyby velmi bohatý. Výskyt z pohledu bezpečnosti negativních i pozitivních jevů přitom nebyl v průběhu roku rovnoměrně rozložený a na globální úrovni i v rámci České republiky je tak možné pozorovat mnoho zajímavých trendů. Detailnější pohled na vybrané typy útoků a událostí z posledního kvartálu roku 2018 poskytují dvě následující kapitoly, v této části se ale ještě před tím zaměříme na vybrané dění z průběhu celého roku 2018.

Data využitá v této části reportu pocházejí 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.

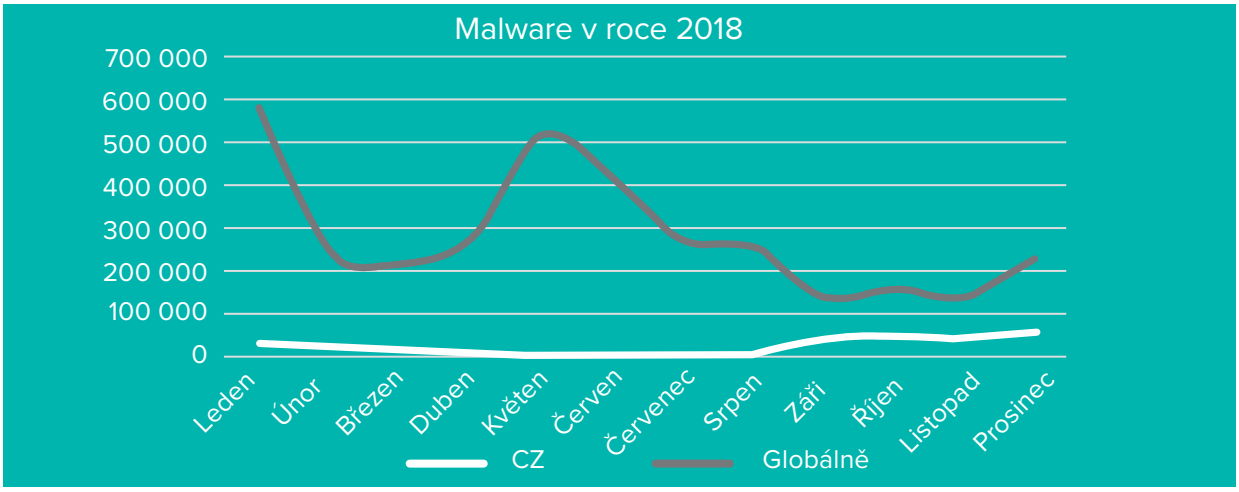
Škodlivý kód

Malware je právem považován za jednu z největších kybernetických hrozeb současnosti. Přestože v roce 2018 bylo možné pozorovat citelný odklon útočníků od užívání ransomwaru (převážně ve prospěch šíření škodlivého kódu sloužícího ke cryptominingu/cryptojackingu), neznamená to, že by tato hrozba již nebyla aktuální. Nové typy krypto ransomwaru i mnoha jiných typů škodlivého kódu nás provázely celým rokem 2018, přičemž jediný infikovaný stroj mohl pro organizaci znamenat nedostupnost kritických služeb, ztrátu všech dat na síťových discích, nebo únik citlivých informací.

Dle dostupných dat byl v roce 2018 na malware celosvětově nejbohatší leden s téměř 578 000 evidovanými detekcemi spojenými s šířením škodlivého kódu. V několika následujících měsících pak nastal v celosvětových detekcích citelný propad, přičemž tento trend kopírovala i situace v prostředí České republiky.

V květnu, který byl globálně hned po lednu na škodlivý kód nejbohatší, bylo v rámci ČR evidováno nejméně detekcí z celého roku. Celosvětově byl následně až do září patrný postupný úbytek detekcí, přičemž na domácí scéně byl naopak patrný jejich postupný růst. Přestože nelze vyloučit, že popsané rozdíly v datech týkajících se globálních trendů a situace v ČR jsou způsobeny pouze omezeným množstvím sledovaných systémů, je jejich přítomnost přinejmenším zajímavá.

Od září do konce roku kopírovala domácí situace globální trend, v rámci něhož byly počty detekcí škodlivého kódu až do konce listopadu vyrovnané, přičemž v prosinci bylo možné pozorovat jejich drobný nárůst. Zmínku zaslouží, že dle dostupných dat byl v rámci ČR na šíření a výskyt škodlivého kódu nejbohatší právě prosinec s více než 52 000 detekcemi.

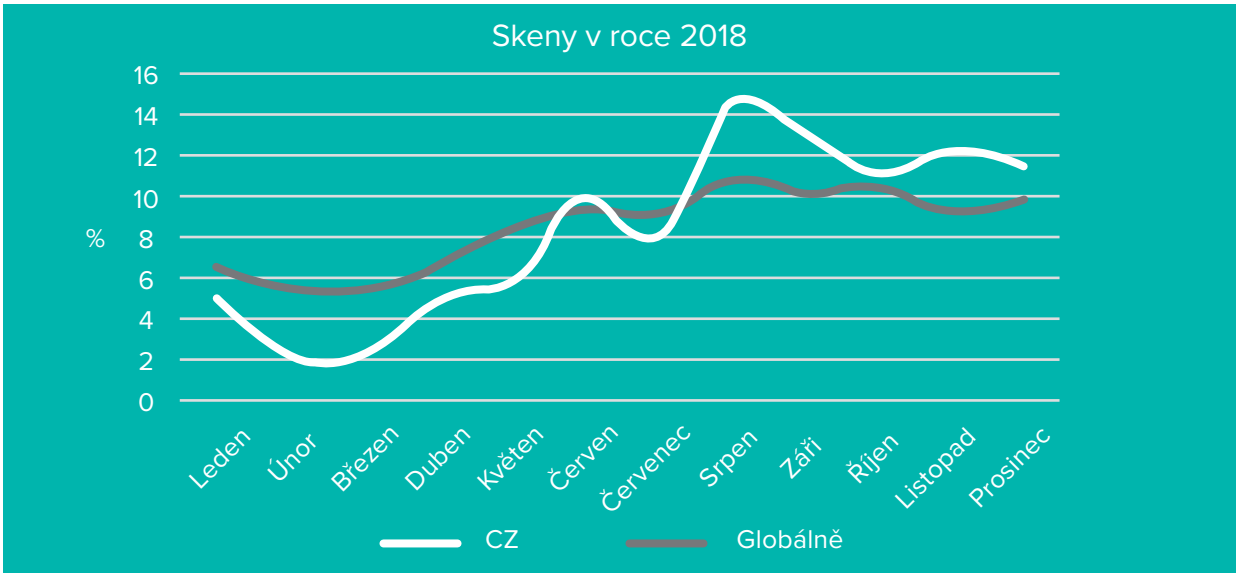


Skeny
Snad každý systém dostupný z Internetu je několikrát denně „skenován“ různými automatizovanými nástroji. Mnohé z nich jsou zcela legitimní, nebo alespoň nejsou užívány se škodlivými záměry. Většina z nich je však využívána útočníky za účelem nalezení zranitelných nebo špatně chráněných systémů. Skeny prováděné těmito nástroji mohou mít různou podobu – od detekce otevřených portů a na nich běžících služeb až po identifikaci zranitelností ve webových aplikacích.

Vzhledem k rozdílu mnoha řádů mezi počty evidovaných skenů pro globální a české prostředí v analyzovaných datech není vhodné porovnávat tyto hodnoty přímo. Podstatně větší vypovídací hodnotu může mít porovnání procentuálních rozdělení detekovaných skenů do jednotlivých měsíců.

Z dat z celosvětového sledování skenů je v takovém případě patrný drobný propad v jejich detekcích v prvním kvartálu, následovaný pomalým růstem jejich počtu až do srpna, kdy dosáhl vrcholu. Až do listopadu, kdy došlo k drobnému propadu detekovaných skenů (následovanému jejich opětovným růstem v průběhu prosince), zůstaly jejich počty velmi vysoké.

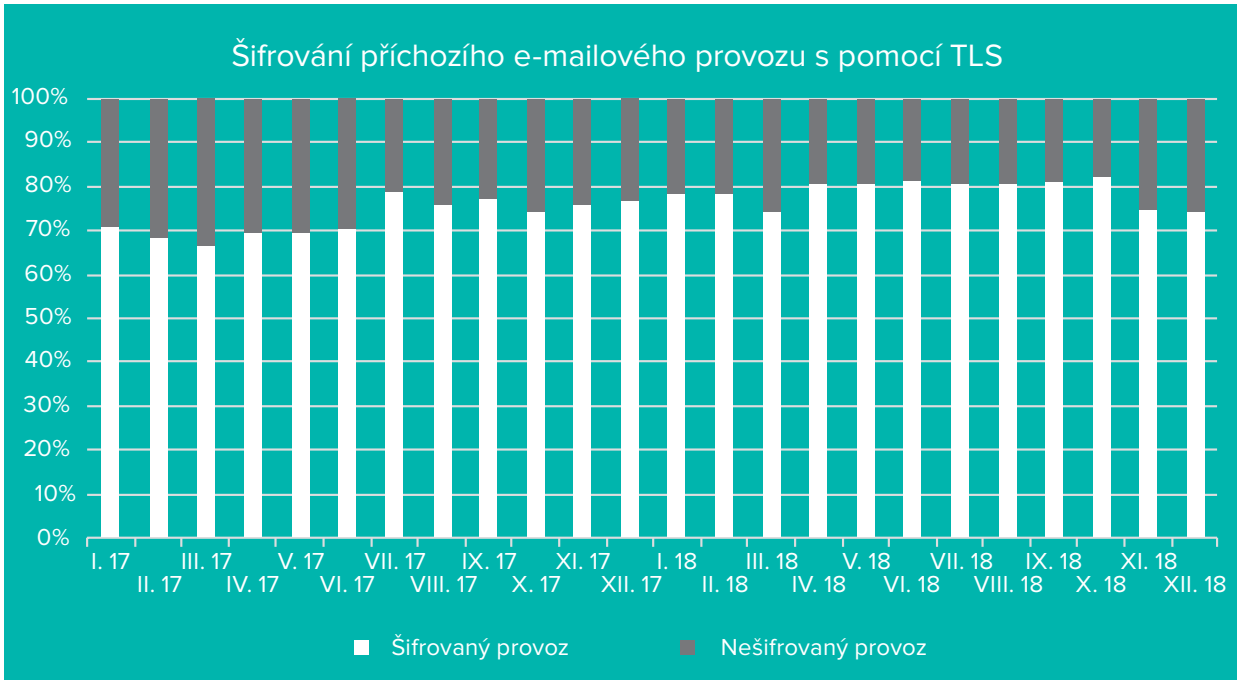
Data z českého prostředí z prvních 9 měsíců roku 2018 plně odpovídají výše popsaným trendům, přičemž jak úvodní propad, tak následný růst, jsou ale podstatně citelnější. Zajímavou skutečností je, že v posledním kvartálu situace v rámci ČR vykazovala přesně obrácené tendence proti trendům globálním, tedy drobný propad počtu detekcí skenů v říjnu, jejich nárůst v listopadu a opětovný drobný propad v prosinci.

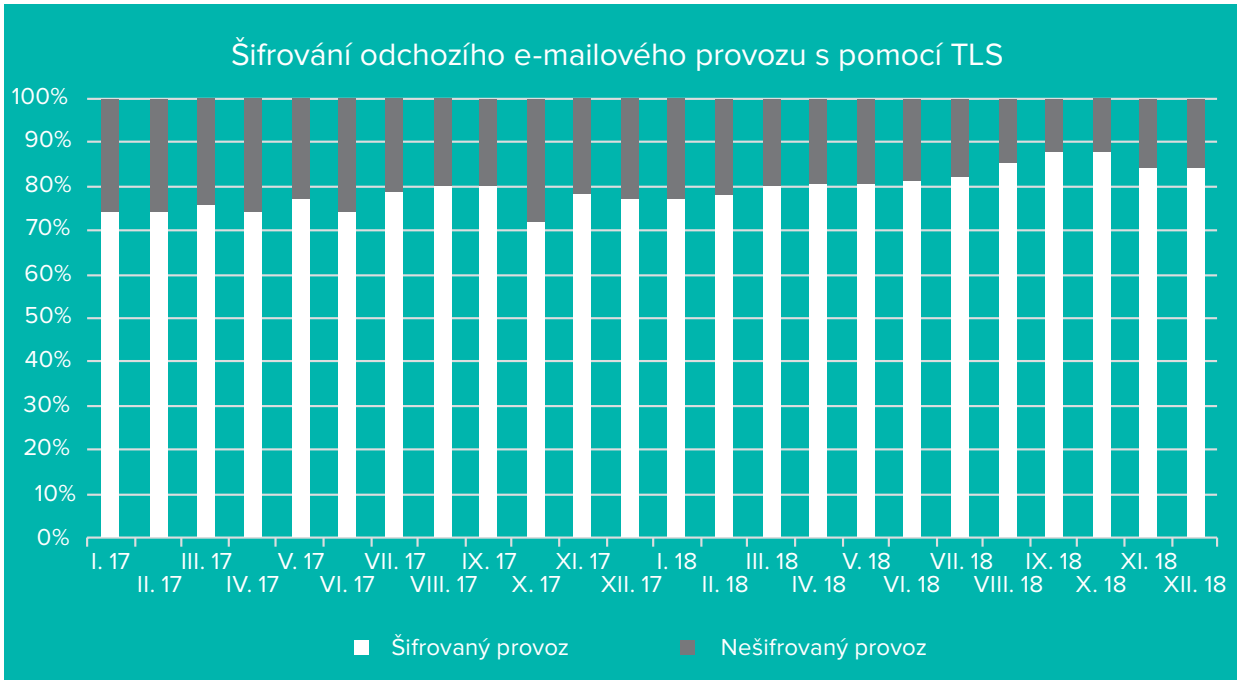


E-mail
Problematice spamu, phishingu a dalším hrozbám spojeným s e-mailem je věnována následující kapitola. V rámci diskuze dlouhodobých trendů je však vhodné zmínit na tomto místě alespoň jednu zajímavost týkající se vývoje v zabezpečení e-mailové komunikace, konkrétně v používání TLS k šifrování jejího přenosu mezi servery.

Pro ochranu důvěrnosti obsahu e-mailových zpráv je vedle jejich end-to-end šifrování (S/MIME nebo PGP) často užívané i zabezpečení komunikace mezi odesílajícím a přijímajícím e-mailovým serverem s pomocí mechanismu STARTTLS, resp. protokolu TLS. Pouhé šifrování kanálu, kterým komunikují servery, sice nenabízí stejnou úroveň ochrany přenášených dat, jako uživatelem zašifrovaný e-mail (chráněna jsou jen data přenášená mezi servery a nikoli e-mail uložený ve schránce nebo data přenášená mezi serverem a uživatelem), má ale jednu nespornou výhodu. Z pohledu uživatelů je zcela transparentní. Navíc se šifrování aplikuje oportunisticky, kdykoli je to možné – pokud tedy šifrování podporuje jak server odesílatele, tak

server příjemce, bude jejich komunikace (včetně přenášeného e-mailu) zabezpečena.
Ne všechny e-mailové servery oportunistické šifrování podporují, počty těch, které tuto možnost nabízí, však každoročně rostou. Zvyšuje se tak i podíl e-mailů, které jsou při přenosu mezi servery automaticky šifrovány. Tento trend je, jak ukazují následující grafy, patrný i z dostupných dat týkajících se podmínek v České republice v posledních dvou letech. Pro jejich doplnění je vhodné uvést, že na základě analyzovaných dat bylo v roce 2017 šifrováno v průměru 72,8 % příchozích a 76,7 % odchozích e-mailů, zatímco v roce 2018 bylo šifrováno již 78,9 % příchozích a 82,6 % odchozích zpráv.





CSIRT.CZ

cesnet certs

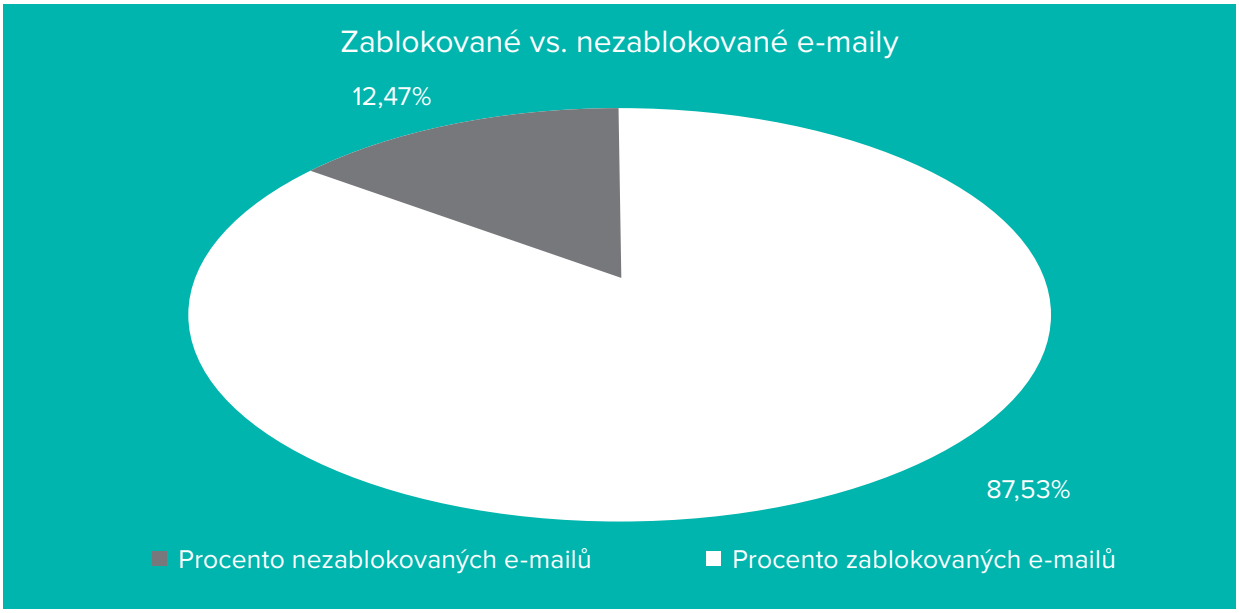
Analýza dat z e-mailových bran

Milan Habrcetl

Tato část reportu diskutuje výsledky analýzy dat, získaných z e-mailových bran ALEF NULA a dalších subjektů, z posledních tří měsíců roku 2018. Celkový počet zpracovaných e-mailových zpráv v těchto nástrojích byl větší než 31 milionů.

V posledním kvartálu roku 2018 byla většina e-mailů, které byly zpracovávány ve sledovaných e-mailových branách, zablokována. Z téměř 31 milionů e-mailových zpráv bylo zablokováno více než 87 procent.

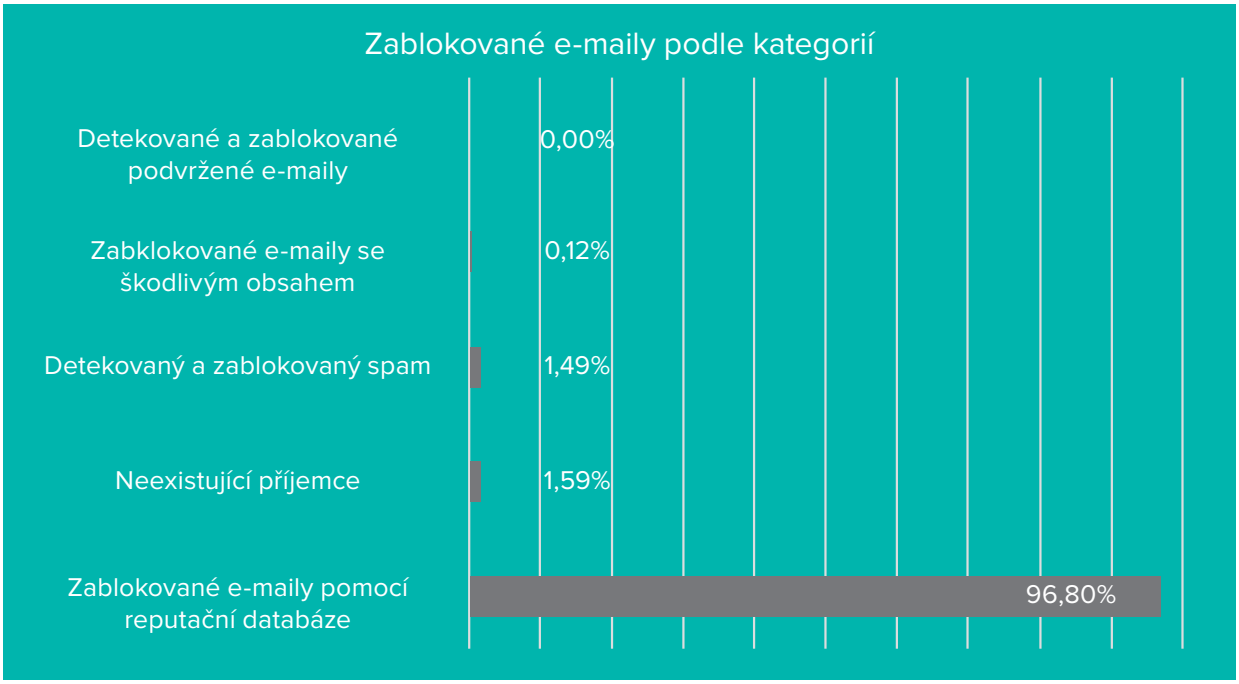
Analýza důvodu blokace e-mailových zpráv
Při analýze důvodů blokace e-mailových zpráv na sledovaných e-mailových branách jsme zjistili, že téměř všechny odmítnuté e-mailové zprávy byly zablokovány na základě informací z reputační databáze o serverech, ze kterých e-mailové



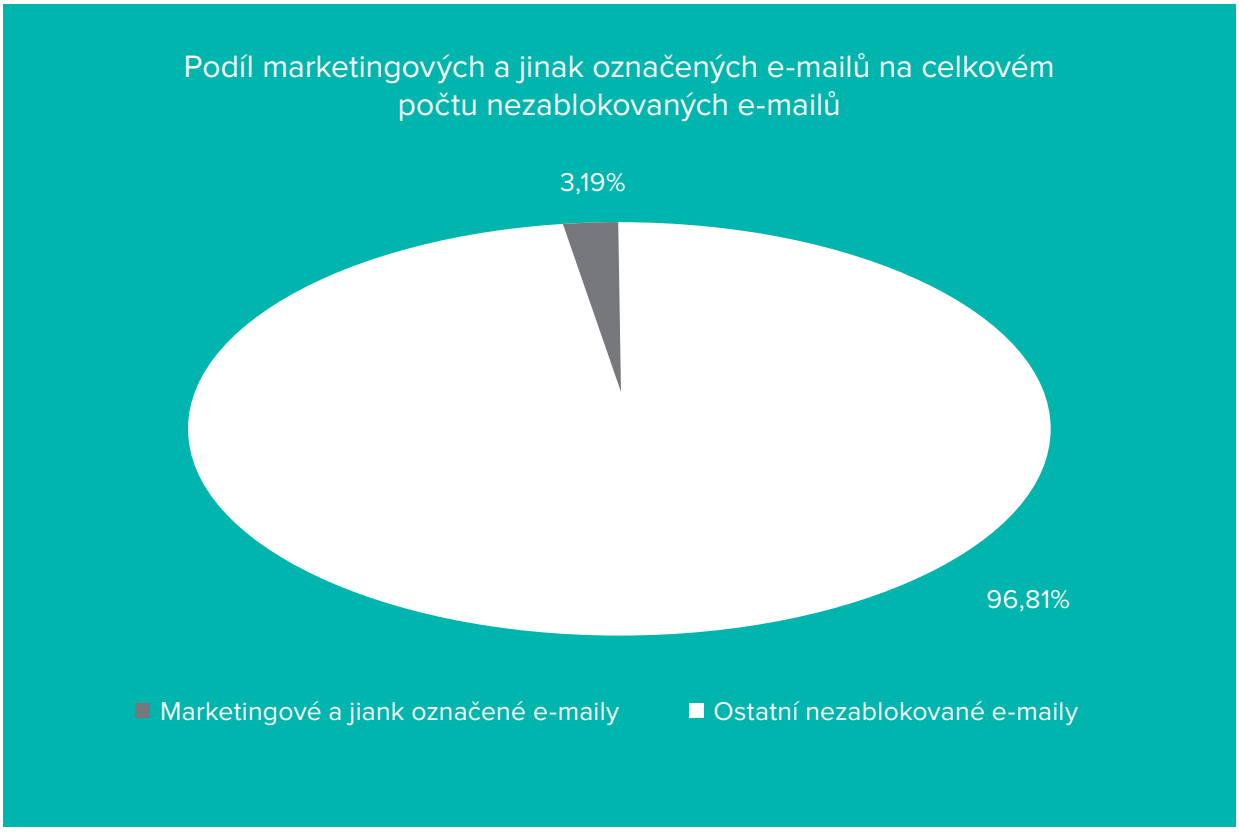
zprávy přišly. V reputační databázi je serverům přiděleno skóre, a pokud je toto skóre nízké nebo negativní, je komunikace z odpovídajícího serveru zablokována.

Některé e-mailové zprávy byly zablokované 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 jejich seznamech s e-mailovými adresami.
Další e-mailové zprávy byly zablokovány kvůli tomu, že byly klasifikovány jako spam, nebo byl jejich součástí škodlivý obsah. Většina zablokovaných e-mailových zpráv se škodlivým obsahem v sobě nesla URL adresu, která odkazovala na škodlivé webové stránky. Zbytek zablokovaných zpráv se škodlivým obsahem pak obsahoval přílohu, která v sobě nesla škodlivý kód.

I když se adopce DMARC (Domain-based Message Authentication, Reporting and Conformance), autentizačního mechanismu odchozích e-mailových zpráv, stále zvyšuje, nebyla na základě tohoto mechanismu ve sledovaném období zablokována žádná podvržená e-mailová zpráva.

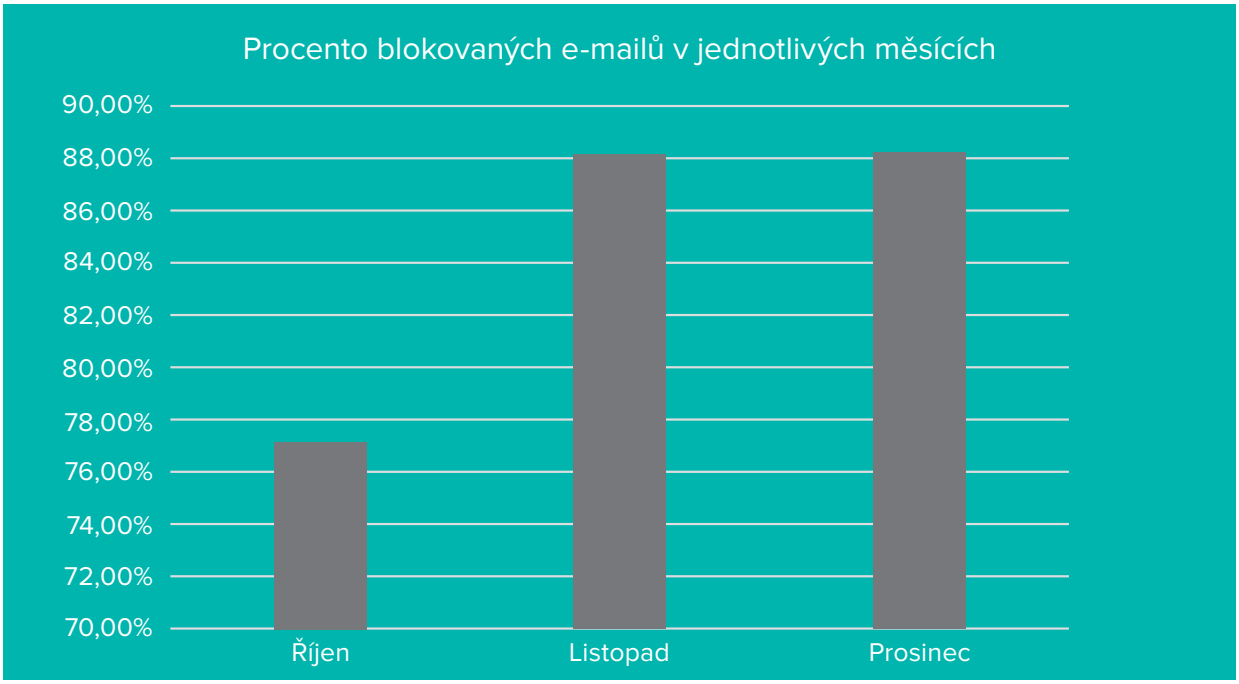


E-mailové brány jsou obvykle nakonfigurovány tak, aby určitým způsobem označovaly e-mailové zprávy s marketingovým obsahem či zprávy ze sociálních sítí. Často jsou tyto typy e-mailových zpráv hromadně nazývány „Graymail“, protože někteří uživatelé je považují za nevyžádanou poštu, ale pro jiné jsou zcela legitimní. Protože se nedá jednoznačně určit, jestli se skutečně jedná o nežádoucí e-maily, tyto zprávy se zpravidla 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 zpráv z e-mailových bran více než 3 procenta z celkového počtu nezablokovaných e-mailů.

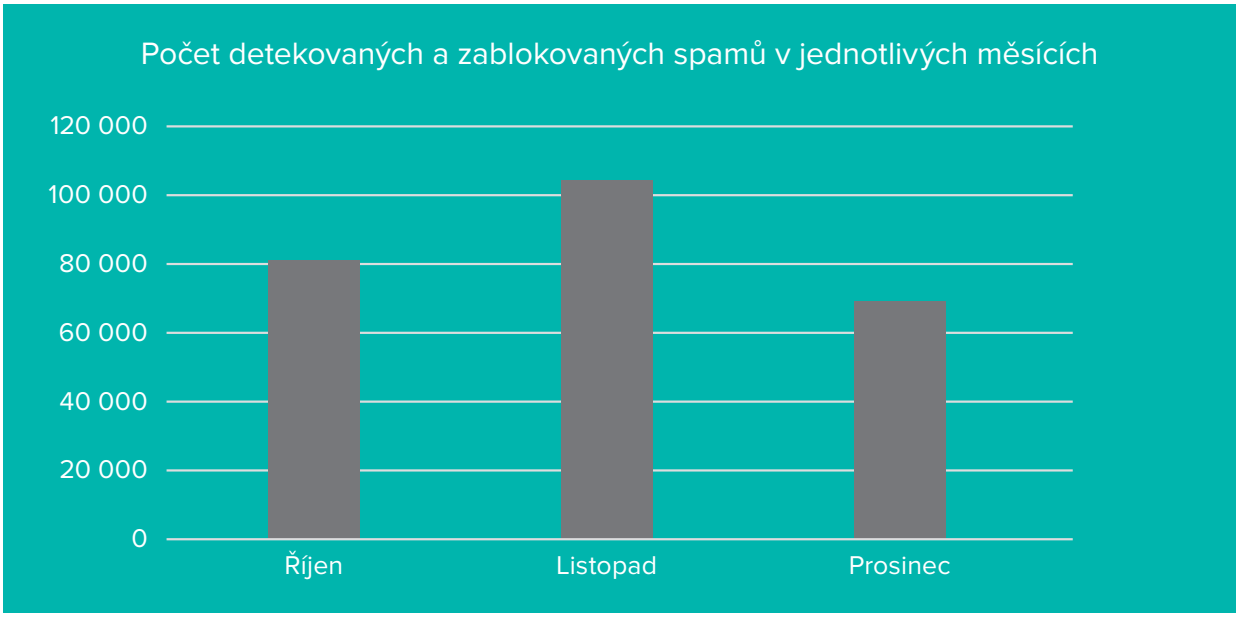


Nárůst útoků v období svátků

Jelikož v posledních měsících roku začínají přípravy na oslavy vánočních svátků, využívají útočníci toto období ke zvýšení svých šancí na získání citlivých informací nebo peněz od uživatelů s pomocí e-mailových zpráv nabízející levné zboží a odkazujících na podvodné stránky. Útočníci v tomto období také stupňují phishingové útoky na organizace a snaží se využít zvýšené nepozornosti uživatelů v období svátků. Na níže uvedeném grafu je tak možné pozorovat velký nárůst zablokovaných e-mailových zpráv, který začíná v listopadu, kdy jsou přípravy na svátky a nakupování dárků v plném proudu, a pokračuje až do konce roku. Největší počet škodlivých e-mailových zpráv je přitom opět zablokován na základě informací získaných z reputačních databází.



U nevyžádané pošty, neboli spamu, lze také pozorovat výrazný nárůst v listopadu. V prosinci je pak možné detekovat její výrazný pokles. To může být následek přidání nově objevených serverů, které odesílají spam, do reputačních databází a následné blokování e-mailových zpráv z těchto serverů na základě skóre z reputačních databází a ne na základě spamových blacklistů.

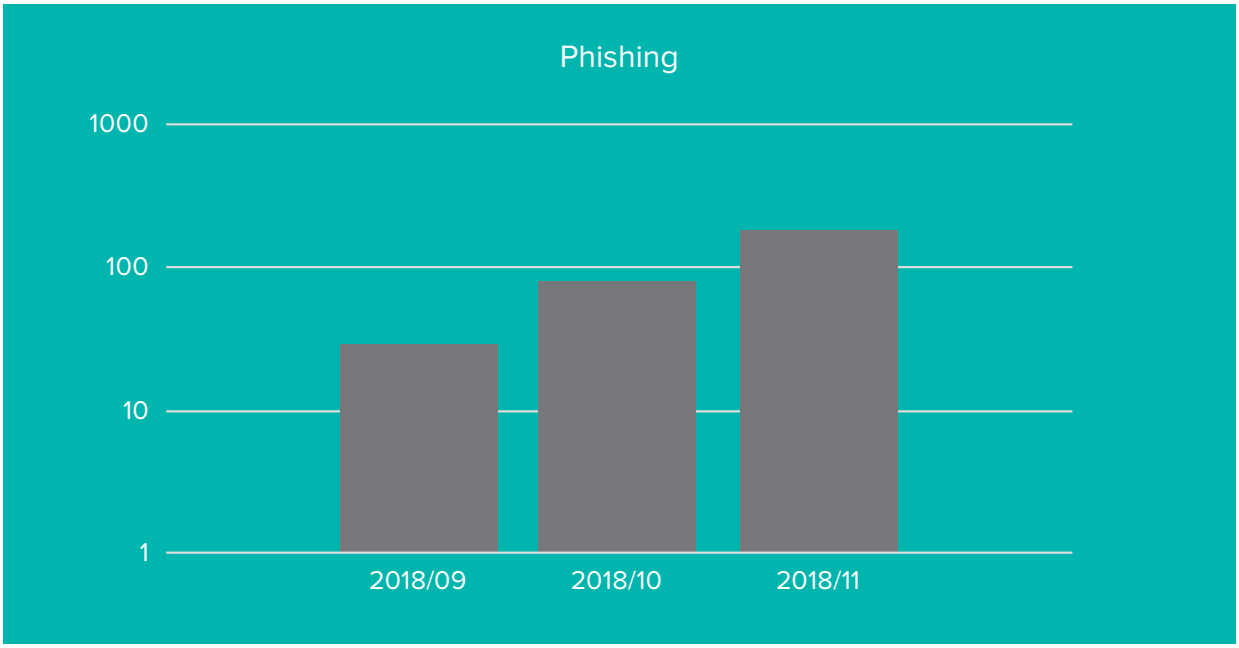


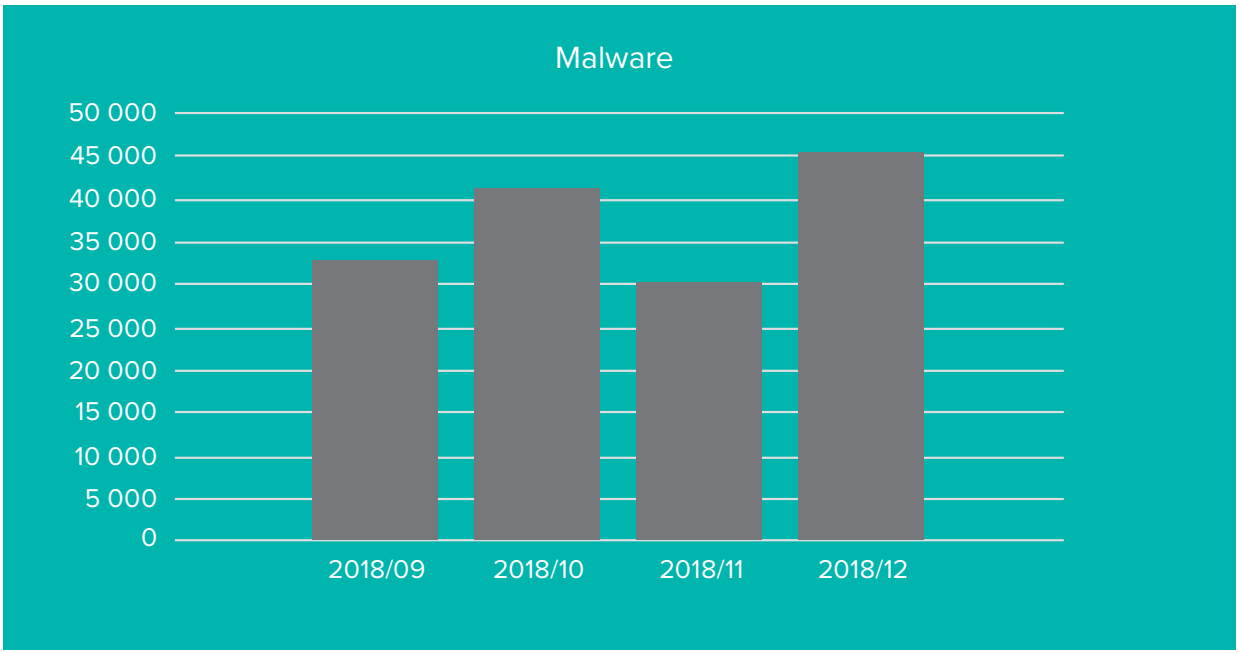
Analýza dat z IPS

Stanislav Techlovský

Tato část reportu se zabývá analýzou dat z IPS systémů a dohledových sond rozmístěných v rámci vlastních i spravovaných infrastruktur. V analýze se zaměříme na data z období posledních čtyř měsíců roku 2018.

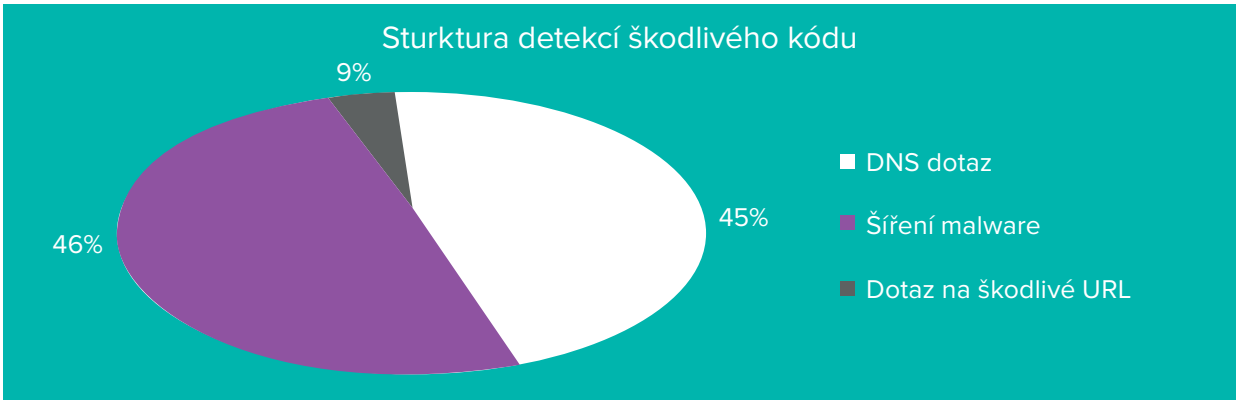
V první části analýzy se nejprve blíže podíváme na phishing, který měl od měsíce září směrem ke konci roku vzrůstající tendenci. Intrusion prevention systémy detekují události spojené s phishingem vždy, když se uživatel pokusí navštívit blokované phishingové stránky, data se tak týkají výkyvů v uživatelské ostražitosti ke konci roku, spíše než počtů šířených podvodných zpráv.





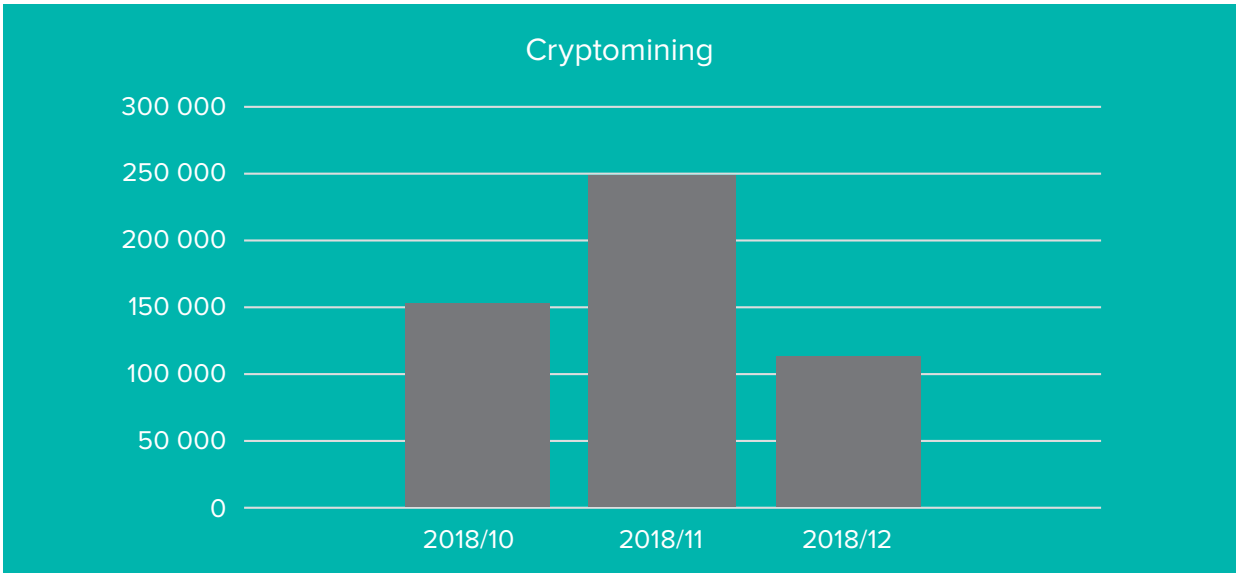
Ve čtvrtém kvartálu roku 2018 bylo detekováno nejvíce malwaru v prosinci, kdy celkové množství událostí přesáhlo 45 tisíc, jednalo se o nárůst o 47 % oproti předchozímu měsíci.

IPS sondy a nástroje, s pomocí nichž byla data shromážděna, dělí detekce škodlivého kódu do tří základních kategorií. V kategorii šíření malware se nacházejí události, při kterých byla detekována shoda s reputační databází IPS. Ta obsahuje IP adresy, na nichž se vyskytuje nebo vyskytoval malware, přičemž se porovnává zdrojová a cílová IP adresa komunikace. Kategorie Dotaz na škodlivé URL obsahuje pokusy o přístup k URL, na nichž byl zaznamenán výskyt malwaru. Samotnou detekci provádí sondy na základě kontroly webového provozu pomocí HTTP, případně HTTPS. Poslední kategorií je DNS dotaz, reputační databáze v tomto případě obsahuje seznam domén, které jsou užívány k šíření škodlivého kódu. Detekovány jsou tak DNS dotazy na překlad domén, na nichž se vyskytuje nebo vyskytoval malware. Struktura detekcí škodlivého kódu v průběhu čtvrtého kvartálu roku 2018 je shrnuta v následujícím grafu.



Jedním z podstatných trendů roku 2018 byl stále citelnější zájem útočníků o těžení kryptoměn s pomocí strojů jejich obětí. Není proto nijak překvapivé, že počty detekcí spojených s nežádoucí těžbou kryptoměn byly i v posledním kvartálu roku 2018 velmi vysoké.

Jednotlivé události spadající do kategorie „Cryptomining“ byly na IPS sondách detekovány pomocí reputační databáze IP adres, u nichž byly a jsou vedeny pokusy o těžbu kryptoměn. Detekce se dále zaměřuje na stahování a analyzování binárních dat, webových klientů, těžebních protokolů a kontrolu blacklistu domén a SSL/TLS certifikátů. V listopadu 2018 byl zachycen nejvyšší počet pokusů o těžbu kryptoměn o celkovém množství přes 245 tisíc pokusů. Oproti předchozímu měsíci se jednalo o 63 % nárůst. V prosinci pak došlo k poklesu pokusů o těžbu kryptoměn o 54 % oproti předchozímu měsíci.



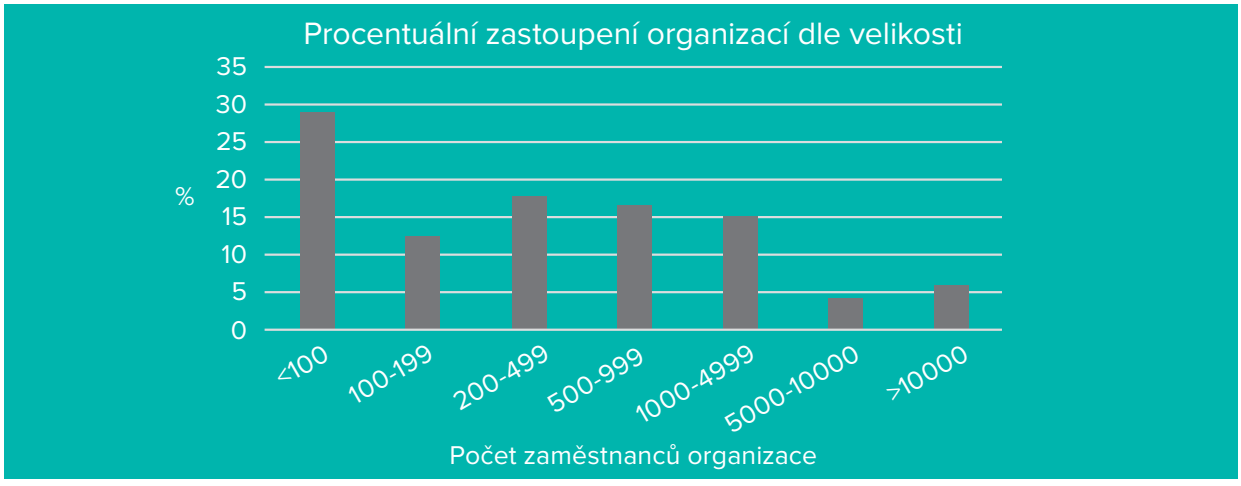
Trendy v oblasti bezpečnostního vzdělávání

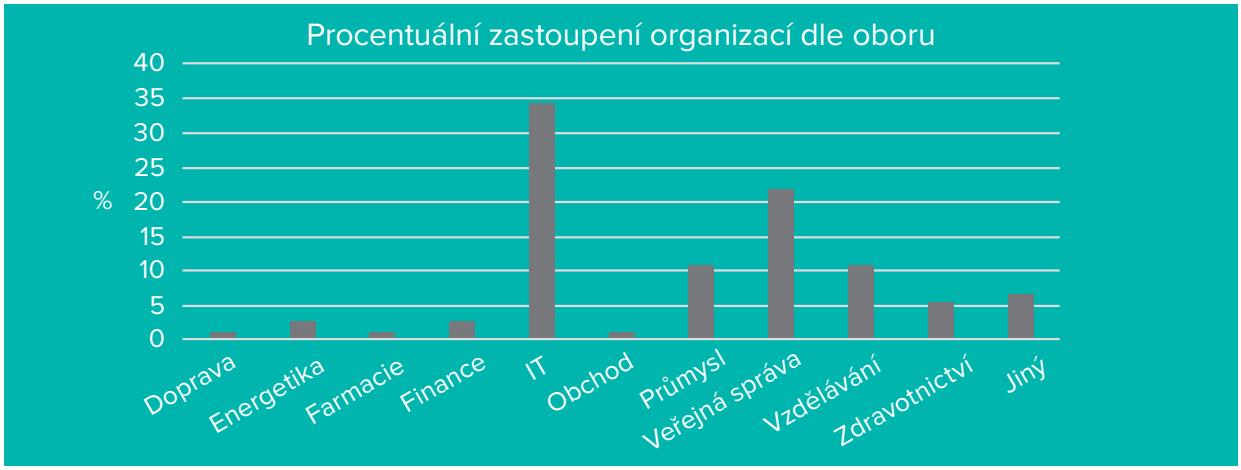
Jan Kopřiva

Je všeobecně známou skutečností, že ve většině případů je právě člověk oním příslovečným nejslabším článkem bezpečnostního řetězce. Technickým i bezpečnostním specialistům často chybí hlubší znalost aktuálních hrozeb, v důsledku čehož před nimi nedokážou své organizace efektivně chránit, a běžní uživatelé často bez rozmyslu klikají na v podstatě jakýkoli odkaz, který se vyskytne v jim adresovaných e-mailových zprávách.

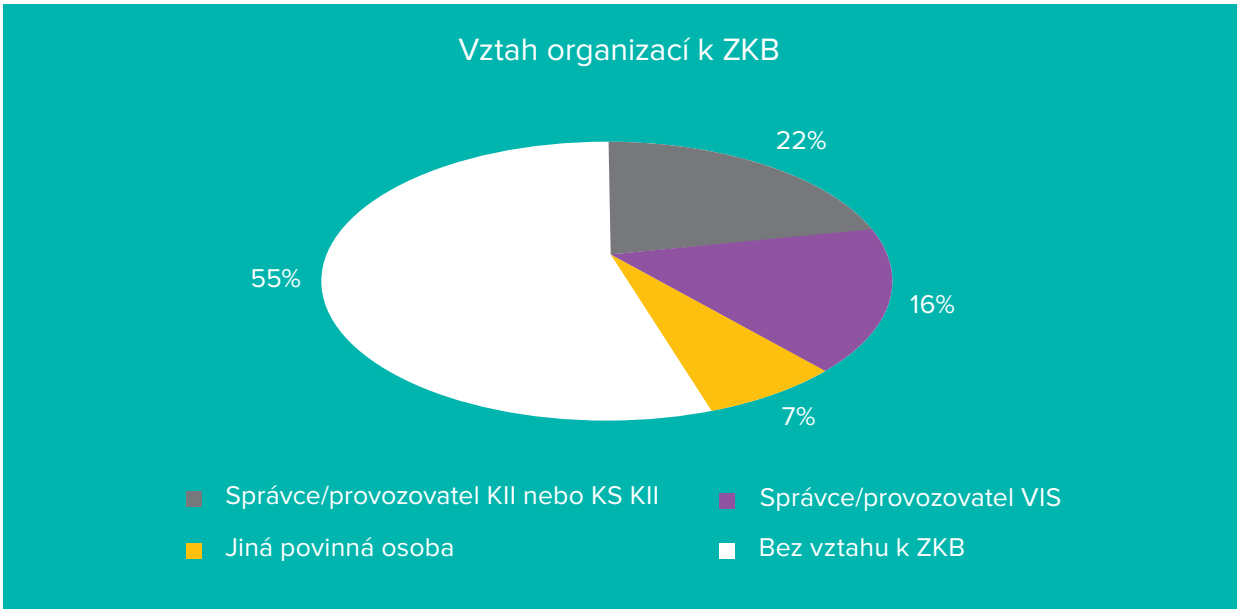
Druhým všeobecně přijímaným faktem však je, že člověk má potenciál být tím nejefektivnějším bezpečnostním mechanismem. Uživatelé, kteří jsou seznámeni s technikami tradičně užívanými při tvorbě phishingových e-mailů, jsou zpravidla schopní podvodné zprávy rychle identifikovat, a dobře vyškolení techničtí specialisté dokážou v případě výskytu bezpečnostních incidentů efektivně analyzovat jejich okolnosti a implementovat vhodná nápravná opatření.

Zvyšování bezpečnostního povědomí a relevantních odborných kompetencí u zaměstnanců je tak pro mnoho organizací prioritou. Zaměření vzdělávacích programů, stejně jako jejich zacílení, se však v různých organizacích často citelně rozchází. Abychom byli schopní se o trendech v této oblasti v rámci České republiky vyjadřovat přesněji než jen ve velmi obecných termínech, realizoval ALEF CSIRT spolu se vzdělávacím centrem ALEF TRAINING v průběhu ledna 2019 mezi organizacemi působícími v rámci ČR průzkum zaměřený na jimi realizované nebo plánované vzdělávací programy a aktivity. Průzkumu se zúčastnili zástupci 73 organizací různých velikostí působících v různých oborech, jak demonstrují následující grafy.





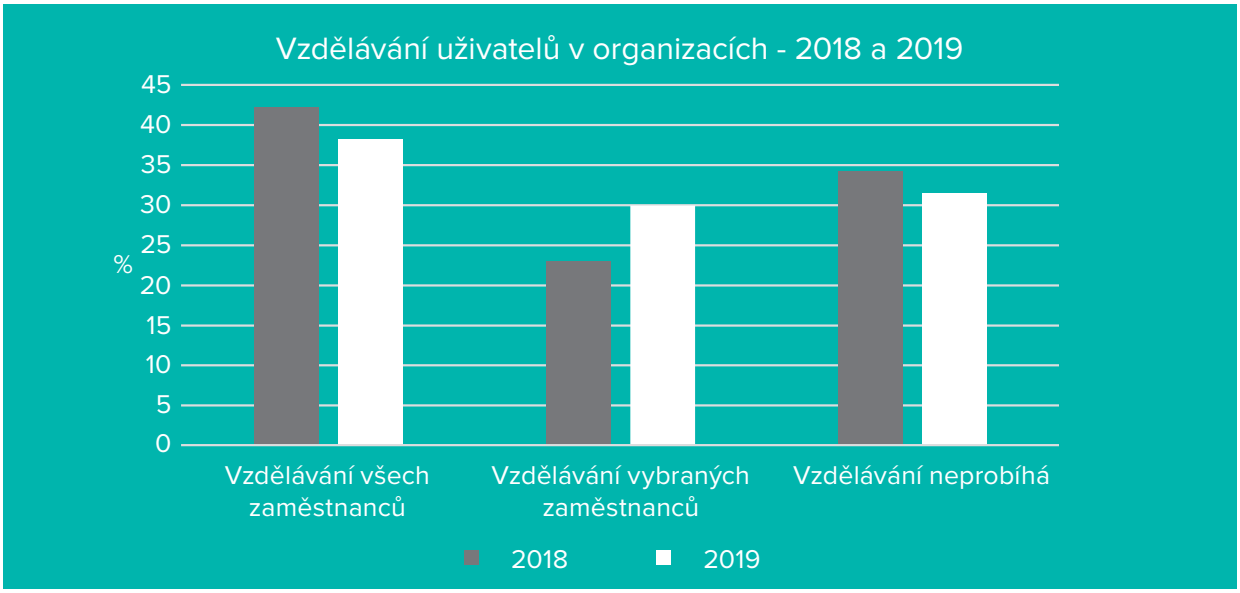
Pro úplnost je vhodné uvést, že na 45 % organizací, jejichž zaměstnanci na průzkumu participovali, se určitým způsobem vztahují požadavky zákona o kybernetické bezpečnosti.



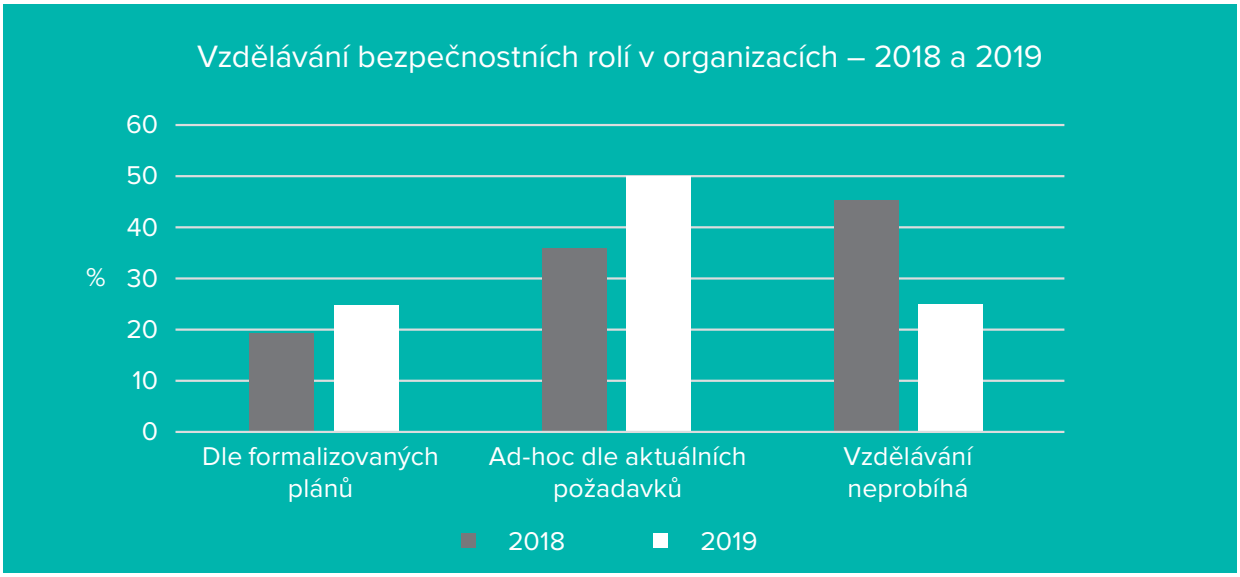
Plánované změny

V rámci průzkumu se respondenti vyjadřovali k realizovaným vzdělávacím programům ve svých organizacích v roce 2018 a k plánovaným vzdělávacím aktivitám pro rok 2019. Na základě získaných odpovědí lze i přes omezenou velikost vzorku usuzovat, že trendy v České republice sledují v obecné úrovni trendy globální a že stále větší počet organizací zavádí určité formy bezpečnostního vzdělávání v případě řadových zaměstnanců i odborných bezpečnostních rolí. Jak ukazuje následující graf, nějakou formu bezpečnostního vzdělávání zaměstnanců zajišťovalo v roce 2018 necelých 66 % organizací zapojených do průzkumu, zatímco pro rok 2019 plánovalo zaměstnance aktivně vzdělávat již téměř 68,5 % z nich.

Krátkou zmínku zaslouží vedle uvedeného obecného pozitivního trendu rovněž z grafu patrný plánovaný drobný odklon od plošného vzdělávání všech zaměstnanců ve prospěch vzdělávání pouze vybraných pracovníků v roce 2019. Přestože vzhledem ke zmíněné omezené velikosti zkoumaného vzorku nelze tento trend považovat za reprezentativní pro situaci v celé ČR, je jeho přítomnost v získaných datech přinejmenším zajímavá.

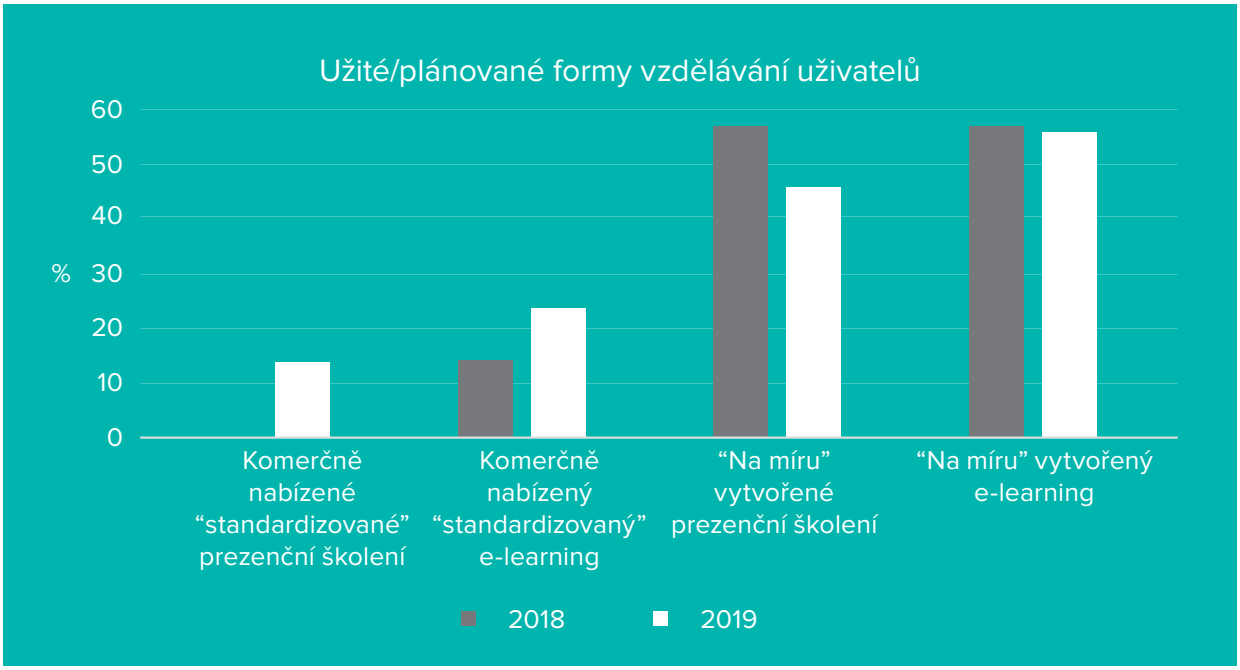


Ještě citelnější pozitivní trend, než v případě vzdělávání běžných uživatelů, je patrný z dat týkajících se vzdělávání bezpečnostních rolí – manažerů a architektů kybernetické bezpečnosti a dalších bezpečnostních specialistů. Zatímco v roce 2018 probíhalo dle vyjádření respondentů vzdělávání bezpečnostních rolí v necelých 55 % organizací, pro rok 2019 plánovalo své bezpečnostní specialisty vzdělávat již 75 % z nich.

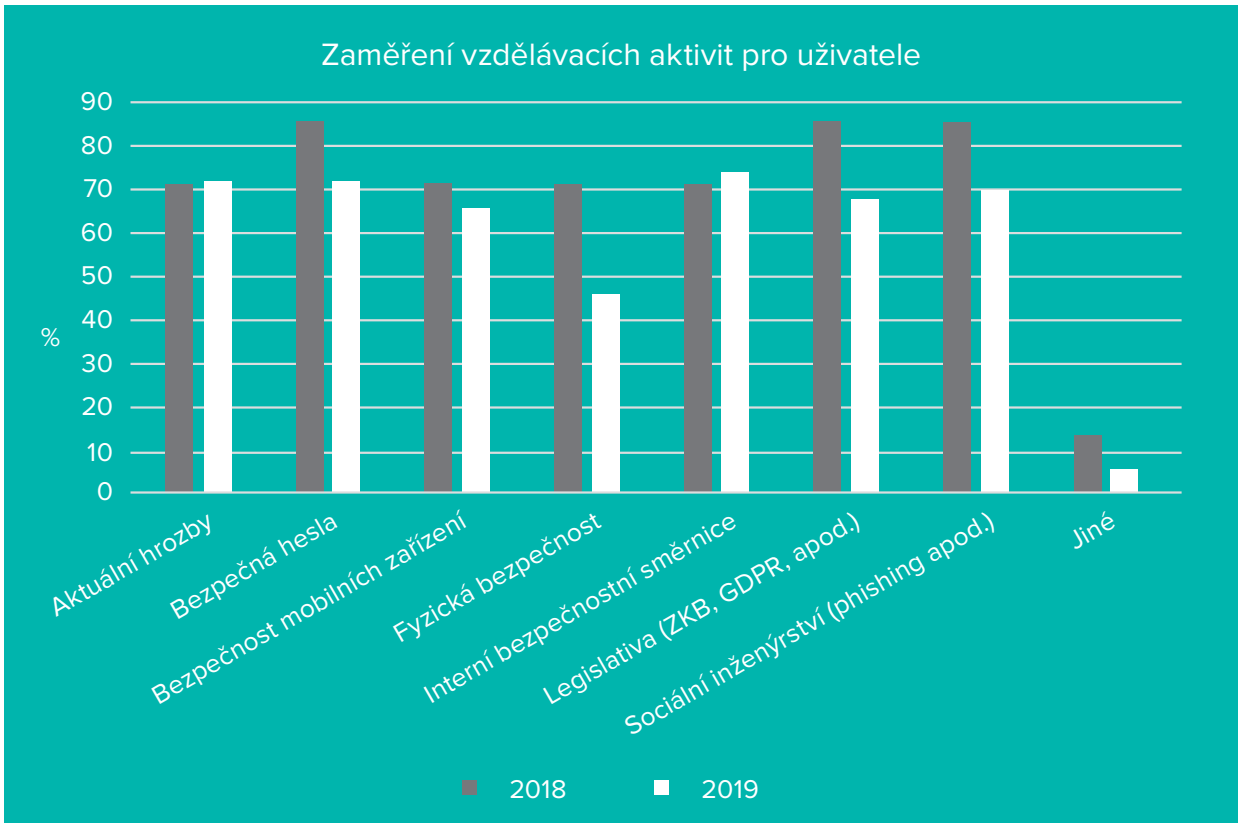


Vzdělávání uživatelů

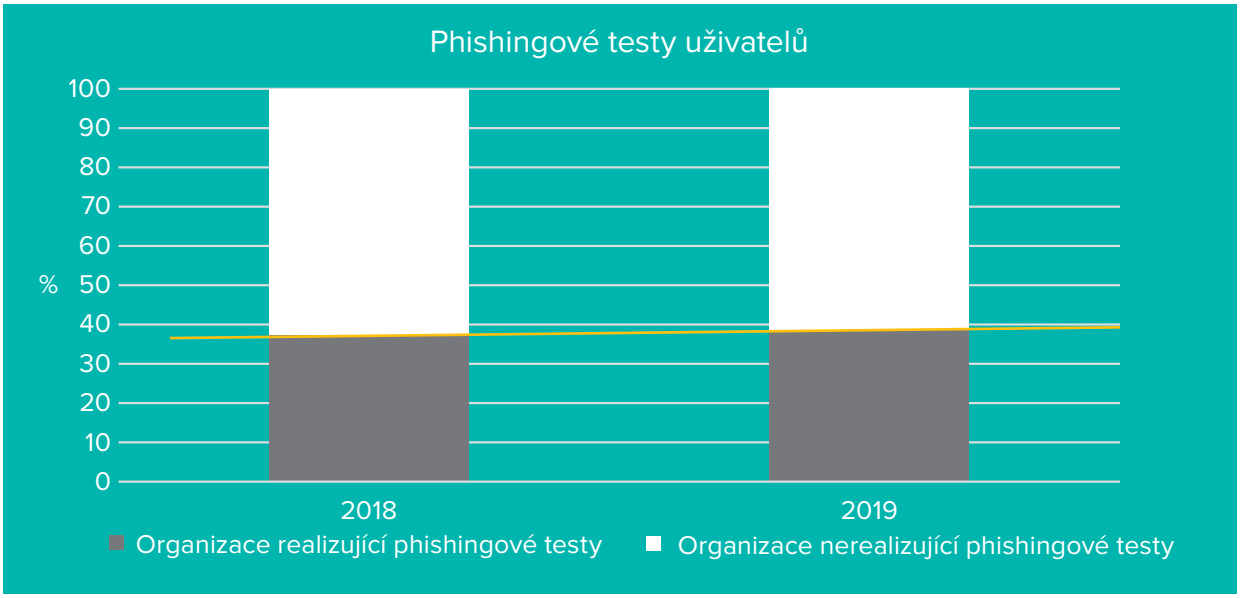
Zřejmě největší změnou, plánovanou organizacemi pro rok 2019 v oblasti vzdělávání uživatelů, se zdá být zvýšený zájem o využívání standardizovaných komerčních školení, a to jak ve formě prezenčních kurzů, tak e-learningových školení. Širší využívání standardizovaných kurzů bylo ve většině případů plánováno na úkor „na míru“ vytvořených školení, a to zejména těch realizovaných prezenčně. I přes tento posun směrem ke standardizovaným bezpečnostním kurzům zůstanou v roce 2019 dle vyjádření respondentů dominantní formou vzdělávání uživatelů kurzy a školení vytvořené dle specifických potřeb konkrétních organizací. V prezenční formě s nimi pro rok 2019 počítalo 46 % a v podobě e-learningu pak 56 % organizací, které plánují nějaký uživatelský vzdělávací program provozovat.



Druhým zajímavým trendem pro rok 2019, týkajícím se vzdělávání uživatelů, se zdá být zájem o přesnější cílení vzdělávacích programů tak, aby pokrývaly pouze oblasti kritické pro danou organizaci, a související omezování šíře záběru těchto programů. Zmíněný trend je nejpatrnější v oblasti fyzické bezpečnosti. Uvedené problematice se v roce 2018 věnovalo 71 % vzdělávacích programů, zatímco v roce 2019 se jí mělo věnovat pouze 46 % z nich.



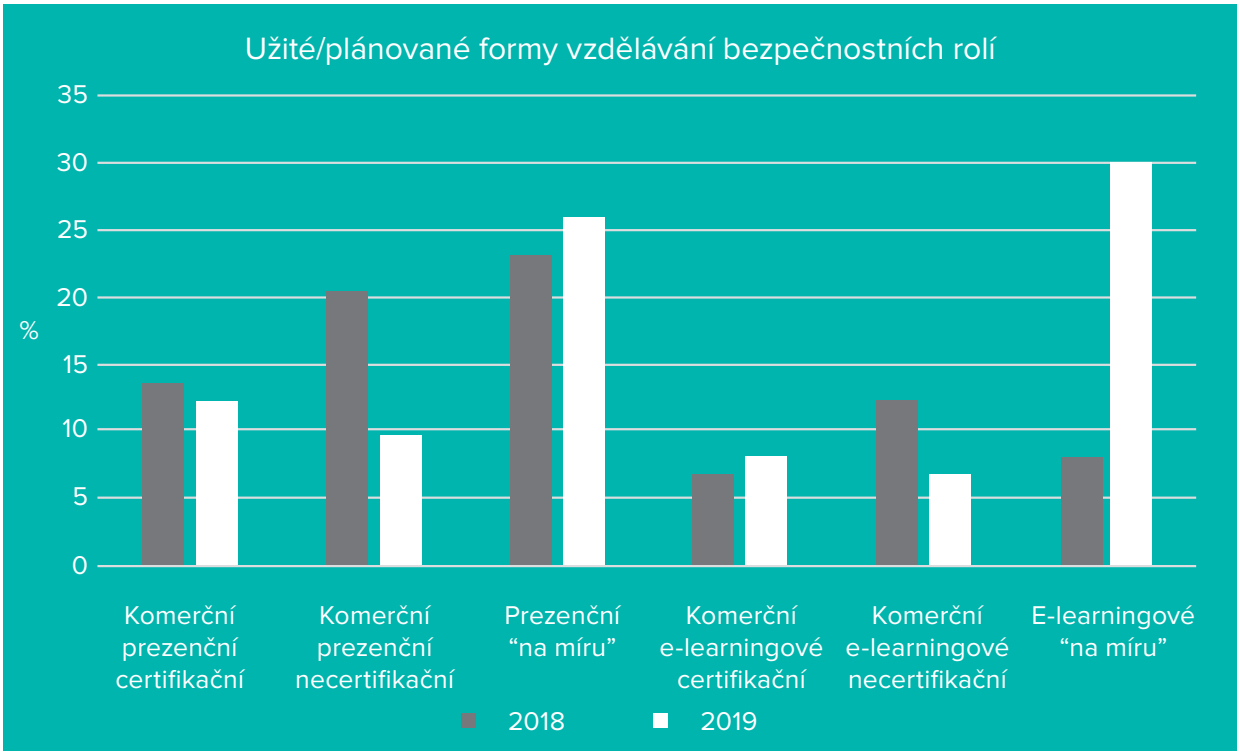
Pro úplnost je vhodné zmínit, že počty organizací, které užívají phishingové testy, jako nástroje pro verifikaci účinnosti programů zvyšování bezpečnostního povědomí, se v roce 2019 oproti předchozímu roku zřejmě nebudou citelněji zvyšovat, nicméně svou oblibu si udrží. V roce 2018 tyto testy dle reakcí respondentů realizovalo 37,5 % organizací a do roku 2019 s nimi počítalo necelých 39 % organizací.



Vzdělávání odborných rolí
Jak je uvedeno výše, dle odpovědí respondentů se v roce 2019 chystaly tři ze čtyř organizací zapojených do průzkumu vzdělávat své bezpečnostní specialisty, což je citelný nárůst oproti 55 % v předchozím roce.

Formami vzdělávání bezpečnostních specialistů, kterých mělo v plánu využít v roce 2019 nejvíce organizací, byly kurzy „na míru“, a to jak ve variantě e-learningu (30 % organizací), tak prezenčních školení (26 % organizací).

Pomineme-li extrémně velký nárůst zájmu o e-learningové kurzy „na míru“, nejcitelnější rozdíly mezi lety 2018 a 2019 lze pozorovat ve sníženém zájmu o necertifikační odborná školení, a to jak v oblasti prezenčních, tak e-learningových kurzů.

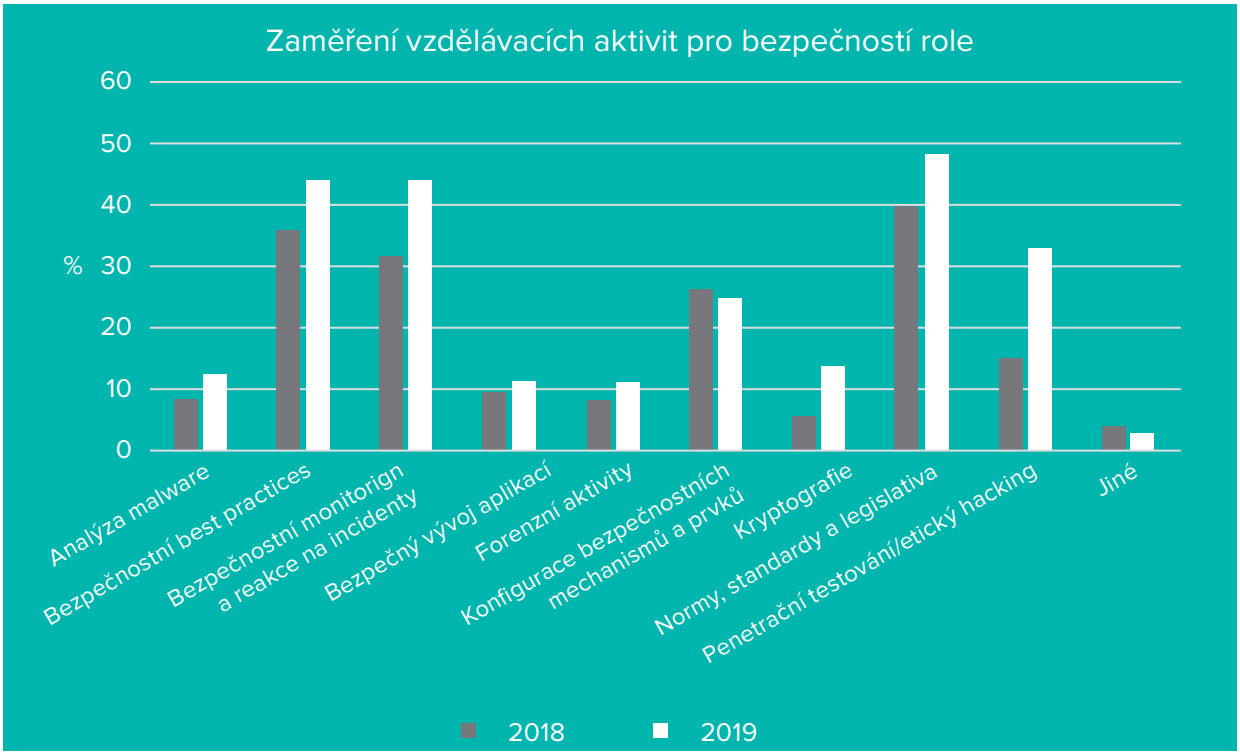


Na rozdíl od vzdělávání uživatelů, u něhož je v plánech pro rok 2019 patrný zájem omezovat oblasti, kterých se mají vzdělávací programy týkat, je v rámci odborného vzdělávání bezpečnostních rolí z odpovědí respondentů znatelný zájem většiny organizací vzdělávat své specialisty ve stále větší šíři oblastí.

Největší zájem v rámci odborného vzdělávání pro rok 2019 byl indikován v oblasti bezpečnostních norem, standardů a legislativy. Vzdělávat své specialisty v této problematice mělo v roce 2019 dle vyjádření respondentů v plánu téměř 48 % organizací.

Největší meziroční nárůsty patrné z výsledků průzkumu se týkají oblasti penetračního testování a etického hackingu (své specialisty v této problematice vzdělávalo v roce 2018 15 % organizací, v roce 2019 tak plánovalo činit téměř 33 % organizací) a oblasti bezpečnostního monitoringu a reakce na incidenty (v této problematice byli v roce 2018 školeni bezpečnostní specialisté v 31,5 % organizací, zatímco v roce 2019 plánovalo vzdělávat v ní své odborníky 44 % organizací).

Zvýšený zájem o vzdělávání interních bezpečnostních specialistů v problematice penetračního testování a problematice incident response je ze strany organizací zcela pochopitelný. Důvody pro něj lze hledat zejména v situaci na pracovním trhu, kde je již dlouhou dobu pociťován nedostatek kompetentních specialistů v obou těchto oblastech.


Zaměření vzdělávacích aktivit pro bezpečností role
60
50
40
% 30
20
10
0
Analýza malware
Bezpečnostní best practices
Bezpečnostní monitorign a reakce na incidenty
Bezpečný vývoj aplikací
Forenzní aktivity
Konfigurace bezpečnostních mechanismů a prvků
Kryptografie
Normy, standardy a legislativa
Penetrační testování/etický hacking
Jiné
2018
2019

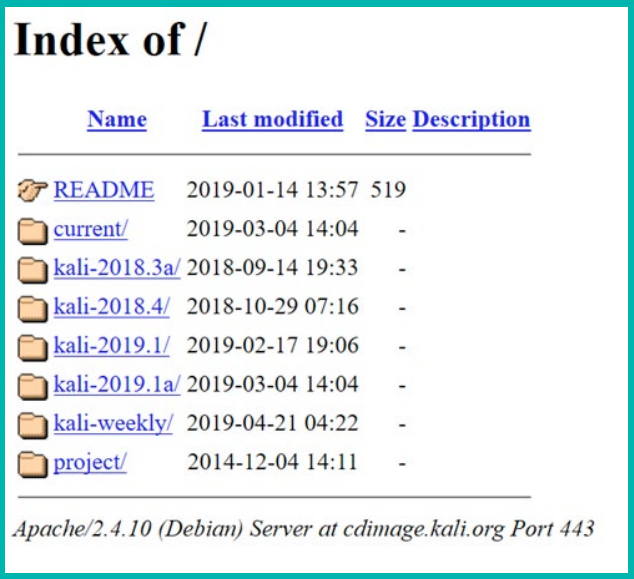
Vybrané výzkumy a analýzy ALEF CSIRT v roce 2018

Jan Kopřiva

V roce 2018 realizoval bezpečnostní tým ALEF CSIRT kromě jiných aktivit i dva výzkumy zaměřené na analýzu různých aspektů bezpečnosti webových serverů provozovaných v rámci národní domény CZ. První z nich byl věnován vyhledávání citlivých dat umístěných v adresářích volně přístupných skrze stránky s automaticky generovaným výpisem jejich obsahu, druhý pak vyhledávání zranitelností webových serverů, které umožňují provést tak zvané otevřené přesměrování.

Citlivá data na českém webu

Automaticky generované stránky zobrazující výpis adresářové struktury, tzv. directory listing, používají administrátoři v případě, kdy chtějí uživatelům do určité míry přes síť zpřístupnit obsah vybraných složek, ale nemají potřebu tvořit pro tento účel odpovídající webové stránky. Nezřídka se však stává, že v důsledku



Index of /

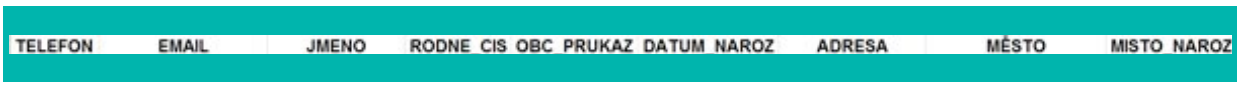
Name	Last modified	Size	Description
README	2019-01-14 13:57	519	
current/	2019-03-04 14:04	-	
kali-2018.3a/	2018-09-14 19:33	-	
kali-2018.4/	2018-10-29 07:16	-	
kali-2019.1/	2019-02-17 19:06	-	
kali-2019.1a/	2019-03-04 14:04	-	
kali-weekly/	2019-04-21 04:22	-	
project/	2014-12-04 14:11	-	

Apache/2.4.10 (Debian) Server at cdimage.kali.org Port 443

administrátorské chyby nebo uživatelské neznalosti jsou s pomocí podobných „otevřených“ adresářů zpřístupněny v podstatě komukoli na internetu i citlivé osobní nebo organizační soubory.

Právě na vyhledávání těchto dat se zaměřili specialisté z týmu ALEF CSIRT v průběhu třetího kvartálu roku 2018 a po analýze obsahu několika tisíc otevřených adresářů identifikovali 159 serverů v doméně CZ, na nichž byly volně přístupné citlivé soubory.

Nejpočetnějším (zřejmě) nezáměrně sdíleným typem nalezených dat byly soubory s hudebním obsahem. Ty se podařilo najít na 22,6 % ze zájmových webových serverů. Podstatně problematičtější byl druhý nejčastěji nalezený typ dat – na celkem 25 serverech bylo možné nalézt osobní údaje. V mnoha případech šlo pouze o seznamy relativně neškodných identifikátorů, např. e-mailů a jmen, na několika serverech se však nacházely i soubory obsahující podstatně širší množství informací (viz záhlaví jedné z nalezených excelových tabulek v následujícím obrázku).



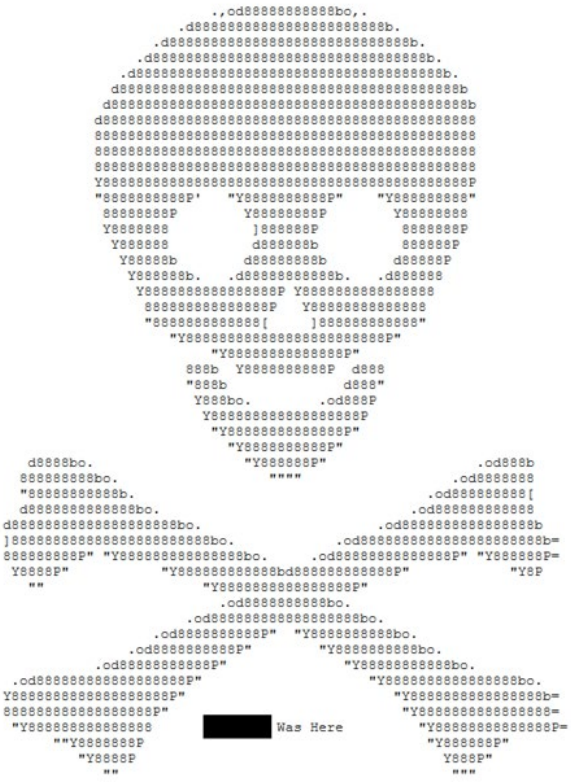
TELEFON	EMAIL	JMENO	RODNE CIS OBC PRUKAZ	DATUM NAROZ	ADRESA	MĚSTO	MISTO NAROZ

Na dalších serverech se pak podařilo identifikovat potenciálně ne plně legální software (v 18,2 % případů), filmy, seriály a další audiovizuální obsah (na téměř 14 % serverů), e-booky a audio knihy (v necelých 7 % případů), osobní fotografie různě citlivé nebo intimní povahy (necelých 17 % serverů) nebo explicitní pornografický obsah (5 % serverů).

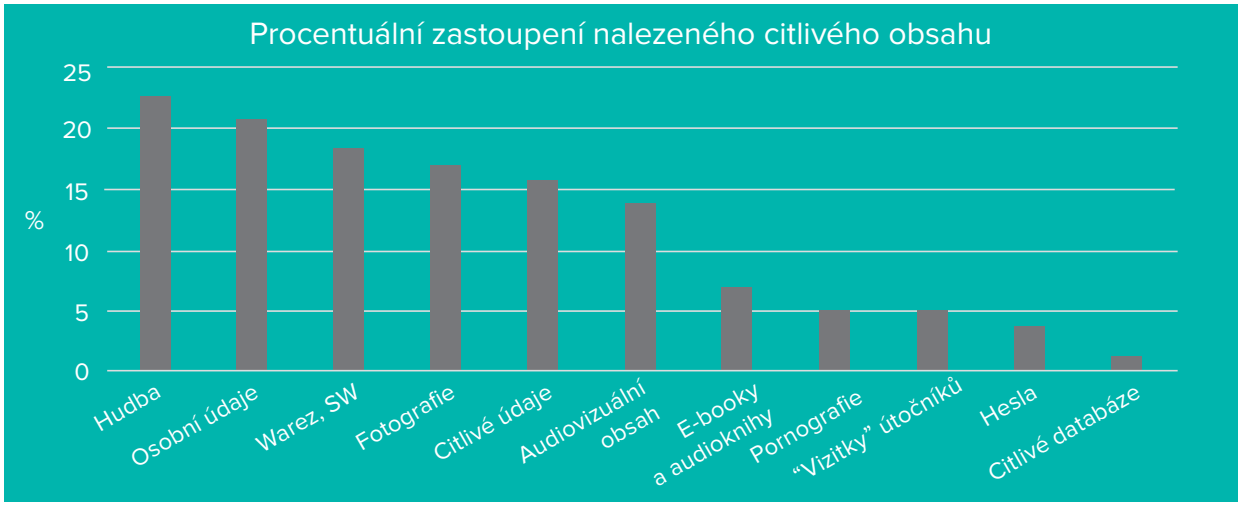
Přestože výše uvedená data nebyla ve většině případů sdílena záměrně, nelze je považovat za tak problematická, jako již zmíněné osobní údaje, nebo další „citlivé“ informace, které byly v rámci analýzy objeveny na téměř 16 % zájmových serverů. Za „citlivé“ v tomto smyslu byly při výzkumu považovány například soubory obsahující finanční data organizací a jednotlivců (např. účetní záznamy a daňová přiznání), zálohy e-mailové komunikace nebo naskenované osobní doklady – obecně téměř libovolná data, která nemají povahu osobních údajů, ale jejichž zveřejnění je možné jednoznačně považovat za nežádoucí z pohledu jejich vlastníka.

Do kategorie citlivých informací nebyla vedle osobních údajů zahrnuta ani hesla k různým službám a systémům (nalezená na téměř 4 % serverů) a soubory databází s citlivým obsahem (přístupná na 1,3 % zájmových systémů).

Na nezanedbatelných 5 % zájmových serverů byly rovněž objeveny indikátory určité formy škodlivého průniku do těchto systémů. Jednalo se o textové nebo obrazové „vizitky“ různých skupin či jednotlivců, převážně s obsahem hlásajícím slávu svému autorovi, nebo informujícím administrátora serveru o úspěšném „hacknutí“ jím spravovaného systému (viz následující ukázky).



Procentuální rozdělení citlivých dat nalezených v rámci zmíněného výzkumu shrnuje následující graf. Detailnější popis analýzy zahrnující i data nalezená na serverech mimo doménu CZ byl publikován na serveru Root.cz.



Otevřené přesměrování na českém webu

Po skončení výše popsané analýzy citlivých dat realizoval bezpečnostní tým ALEF CSIRT v posledním kvartálu roku 2018 další projekt zaměřený na identifikaci potenciálních slabých míst českého webu. V této analýze se specialisté ALEF zaměřili na vyhledávání stránek, umožňujících provést tak zvané otevřené (případně „nevalidované“) přesměrování v rámci národní domény CZ.

Termínem otevřené přesměrování se označuje slabina/zranitelnost, která umožňuje vytvořit odkaz na určitou webovou aplikaci, po jehož otevření bude uživatel bez jakékoli další interakce přesměrován na libovolné v odkazu specifikované URL (i mimo tuto aplikaci). Příklad, který vhodně demonstruje princip otevřeného přesměrování je uveden níže.

https://www.trustednetwork.tld/redirect?to=www.untrustednetwork.tld =>
https://www.untrustednetwork.tld

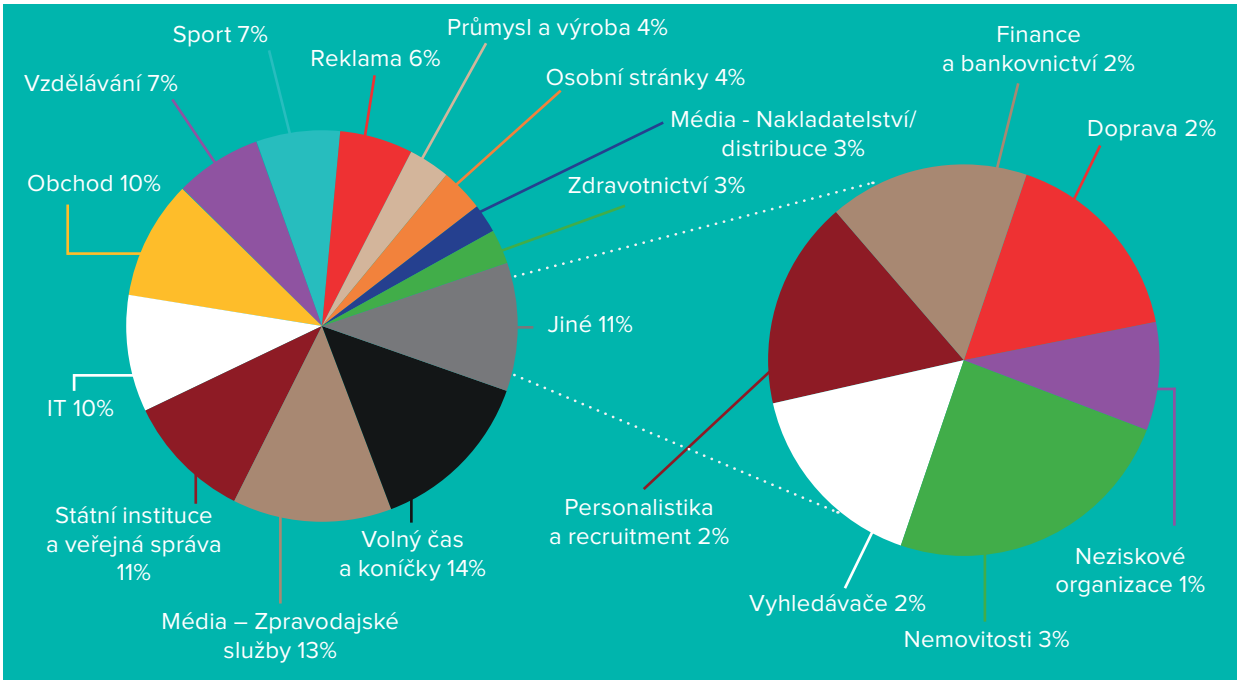
Techniku přesměrovávání uživatelů na nové URL s pomocí interního přesměrovávacího skriptu, případně jiného mechanismu, používají autoři webových aplikací zejména pro marketingové účely, neboť s jejich pomocí je možné snadno zjistit, na které odkazy návštěvníci stránek klikají. Pokud však není žádným způsobem omezena možnost specifikace cíle přesměrování, může škodlivý aktér vytvořit odkaz na legitimní web, po jehož otevření bude oběť automaticky přesměrována na podvodnou nebo škodlivou stránku, a tento odkaz distribuovat například s pomocí phishingových kampaní.

hxxps://www.trustednetwork.tld/redirect?to=www.newsite.tld => hxxps://www.newsite.tld
hxxps://www.trustednetwork.tld/redirect?to=www.newsite2.tld => hxxps://www.newsite2.tld

Vzhledem k výše popsanému principu otevřeného přesměrování je zjevné, že tato zranitelnost nepředstavuje pro většinu webů přehnaně velký problém, pro vysoce citlivé a důvěryhodné stránky (např. stránky bank a jiných finančních institucí), resp. jejich uživatele, však může představovat velmi citelné nebezpečí.

V rámci národní domény CZ bylo v průběhu analýzy zkoumáno cca 700 webových stránek užívajících nějaký přesměrovávací skript nebo jiný mechanismus. U 114 z nich se přitom podařilo identifikovat výše popsanou zranitelnost spočívající v možnosti provést z nich přesměrování na libovolný jiný web.

Následující graf shrnuje zaměření webů, na nichž byly zranitelnosti objeveny. Pro jeho doplnění je vhodné uvést, že zranitelnosti umožňující provést otevřené přesměrování se podařilo identifikovat mj. na stránkách dvou bank, jednéTV stanice s celostátním pokrytím, ministerstva a několika dalších subjektů, které jsou povinnými osobami z pohledu zákona o kybernetické bezpečnosti.



Zmínku rovněž zaslouží, že v rámci výše popsaného projektu se specialistům z týmu ALEF CSIRT podařilo odhalit open redirect zranitelnost také v SW modulu Babel, poskytujícím podporu pro vícejazyčný obsah webům vytvořeným s pomocí redakčního systému CMS Made Simple (CMSMS). Celosvětově se počet webů, užívajících tento modul, potenciálně pohyboval v době odhalení zranitelnosti až v řádu tisíců.

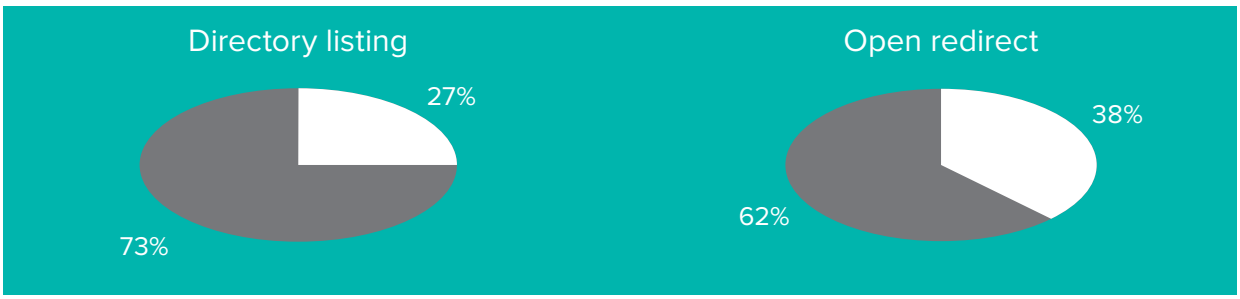
Detailnější popis analýzy zahrnující i zranitelnosti nalezené na serverech mimo doménu CZ byl i v případě tohoto výzkumu publikován na serveru Root.cz.

Kontakt provozovatelů

Provozovatele výše zmíněných zranitelných webů i serverů, na nichž byla přístupná citlivá data, jsme po ukončení každé z analýz kontaktovali a informovali o našich zjištěních, buď sami (případně s využitím platformy Open Bug Bounty), nebo s pomocí organizace CZ.NIC, které bychom tímto chtěli ještě jednou vyjádřit velké díky za poskytnutou součinnost.

Ke konci dubna roku 2019 byla provedena kontrola dat získaných v průběhu obou analýz. V návaznosti na výše zmíněné informování provozovatelů relevantních serverů byl v mezidobí zablokován přístup k „otevřeným“ adresářům na 27 % systémů, na nichž byla nalezena citlivá data. Toto číslo nemusí být nutně konečné, neb bez hlubší kontroly obsahu přístupného na zbylých webech nelze vyloučit možnost, že provozovatelé odstranili citlivý obsah při zachování nastavení umožňujícího přistupovat ke zbylým souborům skrze directory listing.

V případě webů, které obsahovaly zranitelnosti umožňující provést otevřené přesměrování, byla reakce ze strany jejich provozovatelů ještě citelnější – ke konci dubna 2019 byly již zranitelnosti záplatovány na téměř 38 % původně identifikovaných zranitelných serverů.



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