ALEFNULA

Security Report 2024

Trust the Strong
www.alefnula.com

Obsah

Úvod

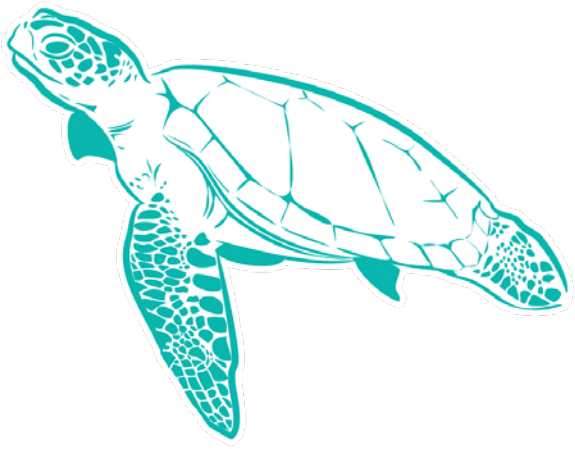
Radek Švadlenka

V posledních letech byl sektor informačních technologií a kybernetické bezpečnosti svědkem nebývalých změn, které byly zapříčiněny řadou významných mezinárodních událostí. Po dopadech pandemie Covid-19 se svět dostal do další krize v podobě válečného konfliktu na Ukrajině. I když Rusko bylo v demokratických státech již dlouho vnímáno jako potenciální bezpečnostní hrozba, jeho invaze v únoru 2022 ještě více rozdělila mezinárodní scénu a zkomplikovala správu bezpečnosti. V roce 2022 bylo také významným krokem přijetí evropské směrnice NIS2, která přináší rozsáhlé změny v oblasti kybernetické bezpečnosti, ovlivňující nejen již regulované organizace, ale i ty, které se dosud těmito povinnostmi nezabývaly. Ani rok 2023 bohužel z pohledu bezpečnosti nepatřil mezi nejklidnější. Konflikt na Ukrajině ještě není zdaleka u konce a už se rozhořela další ohniska bojů na Blízkém východě. V době hybridních válek je třeba být o to více ostražitý a nepodcenit napětí, které je sice geograficky poměrně daleko, nicméně hrozby v kyberptostoru neznají hranice ani vzdálenosti.

Tento report má za úkol poskytnout čtenářům přehled současných trendů v kybernetické bezpečnosti a nabídnout pomoc organizacím a jednotlivcům v této oblasti. Hlavními zdroji bezpečnostních dat pro tuto publikaci byl tým ALEF CSIRT, doplněný o příspěvky dalších odborníků z ALEF Security, kteří se věnovali různým tématům v kybernetické bezpečnosti. Věříme, že obsah tohoto reportu bude pro čtenáře užitečný a poskytne třeba i Vám inspiraci pro řešení kybernetické bezpečnosti ve Vaší organizaci.

V publikaci se mimo jiné dočtete o nejdůležitějších událostech v oblasti kybernetické bezpečnosti, bezpečné e-mailové komunikaci, nejnovějších trendech v bezpečnostním vzdělávání, analýze dat z e-mailových bran a událostech detekovaných IPS sondami, a také o stavu implementace bezpečnostních protokolů SPF, DKIM a DMARC v České republice. Report obsahuje rovněž analýzy týkající se bezpečnostního monitorování a porovnání dat s minulým rokem, což ukazuje, jak se organizace přizpůsobují novým globálním výzvám.

Na závěr bychom rádi poděkovali bezpečnostnímu týmu CSIRT.CZ za poskytnutí dat a statistik, a všem respondentům našich online dotazníků, jejichž spolupráce byla klíčová pro kvalitu obsahu v tomto reportu.



Směrnice NIS2/ nový Zákon o kybernetické bezpečnosti („ZKB“)

Daniel Neumann

Vážení čtenáři,
vstupujeme do éry, kde naše digitální přítomnost nabývá stále rostoucího významu, a s ní přichází nevyhnutelné výzvy a otázky týkající se kybernetické bezpečnosti. Dnešní digitální ekosystém, do něhož jsme pevně zasazeni, vyžaduje pečlivou péči a inovativní přístupy k ochraně našich digitálních aktiv před kybernetickými hrozbami. V tomto kontextu nastupují na scénu směrnice NIS2 a nový zákon o kybernetické bezpečnosti (nZKB), dvě klíčové iniciativy, které mají zásadní vliv na podobu naší kybernetické bezpečnosti. Společně s Vámi se snažíme postavit těmto výzvám čelem.

Věříme, že tyto inovativní legislativní změny přinesou výrazné zlepšení v oblasti kybernetické bezpečnosti a posílí náš společný postoj k ochraně digitální integrity. Vaše názory a zkušenosti, které sdílíte v rámci tohoto dotazníku, jsou významným ukazatelem toho, jak dobře je IT veřejnost informována o nových opatřeních a jak se k nim staví. Děkujeme Vám za Vaši aktivní účast a spolupráci při budování bezpečnější digitální budoucnosti.

Změny, které NIS2 a nový zákon o kybernetické bezpečnosti přinesou, budou obsáhlé. Níže uvádíme stručný přehled několika z nich.

1. **Rozšířená působnost:** Nový zákon o kybernetické bezpečnosti a směrnice NIS2 rozšiřují svůj dosah na širší spektrum subjektů. Z aktuálních cca 400 dotčených subjektů má dle odhadů dojít k navýšení na cca 6000. Tento krok představuje reakci na dynamiku současné digitální scény a zdůrazňuje potřebu ochrany všech aspektů digitální společnosti před kybernetickými hrozbami.

2. **Zvýšená odpovědnost pro subjekty:** Organizace manipulující s citlivými digitálními informacemi jsou nyní povinny nést zvýšenou odpovědnost za implementaci rozsáhlých bezpečnostních opatření. To zahrnuje nejen technická řešení, ale také provádění pravidelných hodnocení rizik a aktivní hlášení kybernetických incidentů.

3. **Povinnost hodnocení rizik:** Směrnice NIS2 a nZKB stanoví povinnost pravidelně provádět důkladná hodnocení rizik. Tyto analýzy mají identifikovat potenciální kybernetické hrozby a umožnit organizacím adekvátně reagovat a předcházet možným kybernetickým incidentům.

4. **Sankce za nedodržení:** V rámci nové legislativy jsou stanoveny výrazné sankce a pokuty pro organizace, které nedodržují stanovené kybernetické bezpečnostní normy a povinnosti. Tímto opatřením má být posílena motivace subjektů k aktivní ochraně svých digitálních aktiv.

5. **Aktivní spolupráce a koordinace:** Zákon a směrnice zdůrazňují důležitost aktivní spolupráce a koordinace mezi členskými státy. Vytvářejí rámec pro efektivní sdílení informací o kybernetických hrozbách a incidentech, což má posílit celkovou kybernetickou odolnost Evropské unie.

6. **Větší důraz na kybernetický výcvik a osvětu:** Nový zákon klade větší důraz na potřebu investovat do kybernetického výcviku a osvěty. Jeho cílem je zvýšení povědomí organizací a jednotlivců o kybernetických hrozbách a optimálních postupech k prevenci.

7. **Zlepšená reakce na kybernetické incidenty:** Pravidla nové legislativy kladou větší důraz na rychlost a efektivitu reakce na kybernetické incidenty. Subjekty jsou povinny vytvářet plány pro řízení krizových situací a úzce spolupracovat s národními bezpečnostními orgány.

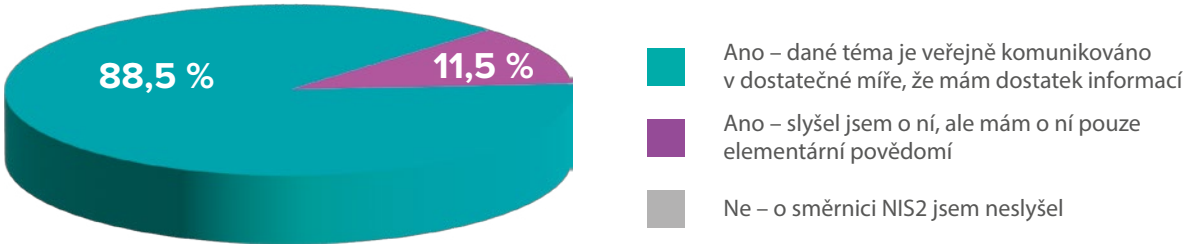
8. **Harmonizace na úrovni EU:** NIS2 a nový zákon o kybernetické bezpečnosti přinášejí větší harmonizaci na úrovni EU. Cílem je dosáhnout sjed-

nocení postupů a standardů v oblasti kybernetické bezpečnosti napříč členskými státy, což by mělo zvýšit celkovou efektivitu a interoperabilitu kybernetických bezpečnostních opatření.

V rámci našeho průzkumu jsme oslovili respondenty s celkem devíti otázkami, které se hlouběji zabývají problematikou směrnice NIS2 a nZKB. Naším cílem bylo získat pestrý a informovaný pohled s názory a postoji respondentů vůči těmto klíčovým aspektům digitální bezpečnosti.

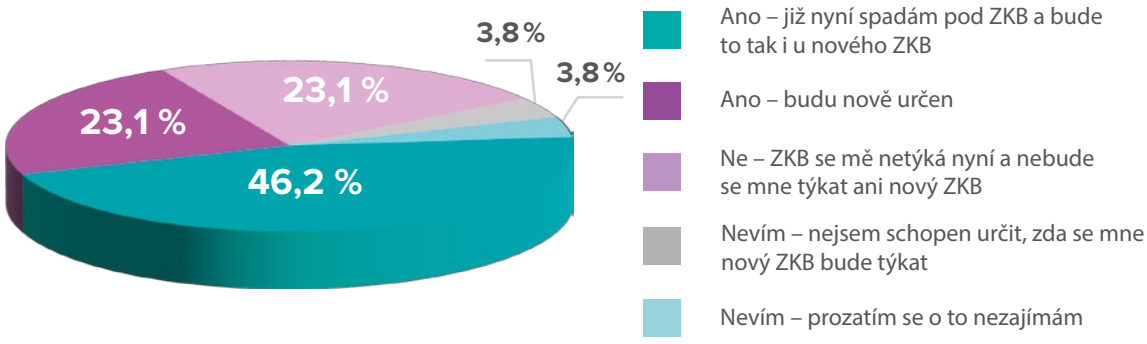
Níže uvádíme přehled získaných odpovědí, odhalující různorodost názorů a postoje respondentů k novým opatřením v oblasti kybernetické bezpečnosti.

Slyšeli jste již o směrnici NIS2?



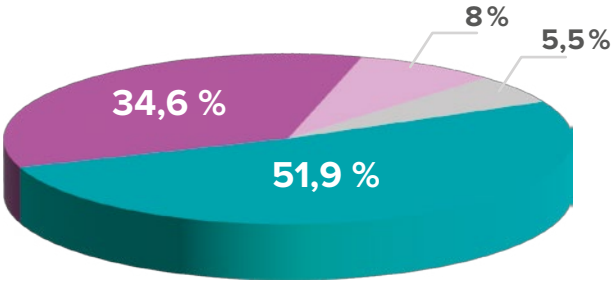
Z výsledků otázky týkající se povědomí o směrnici NIS2 vyplývá, že naprostá většina respondentů (88,5 %) má dostatečné informace o této směrnici, což naznačuje, že téma je veřejně komunikováno v dostatečné míře. Zbytek respondentů odpověděl, že mají pouze elementární povědomí o NIS2 (11,5 %). To může naznačovat, že informace o kybernetické bezpečnosti jsou prezentovány široké veřejnosti, i když někteří mohou mít jen omezené povědomí o konkrétních detailech směrnice. Překvapivě nula procent respondentů nezná směrnici NIS2, což svědčí o vysoké informovanosti vzorku respondentů, neboť nikdo neoznačil, že o této směrnici neslyšel. Celkově lze tedy konstatovat, že úsilí o informování veřejnosti o směrnici NIS2 dosahuje významného úspěchu.

Patříte mezi subjekty, kterých se bude týkat nový ZKB?



U otázky týkající se zahrnutí subjektů pod nový ZKB vyplynulo zajímavé rozložení odpovědí. Z celkového počtu respondentů vyplývá, že 46,2 % již nyní spadá pod působnost stávajícího ZKB a očekává, že toto zařazení zůstane zachováno i u nového ZKB. Naopak, 23,1 % respondentů očekává nové určení pod ZKB, zatímco stejný podíl respondentů (23,1 %) nepatří pod stávající ZKB a předpokládá, že nový ZKB je pro ně rovněž irelevantní. Malý podíl respondentů (3,8 %) vyjádřil nejistotu ohledně toho, zda se jich nový ZKB týkat bude, a stejný podíl uvedl, že se prozatím o tuto problematiku nezajímá. Celkově ukazují výsledky na rozmanitost postojů a očekávání respondentů vůči novému ZKB.

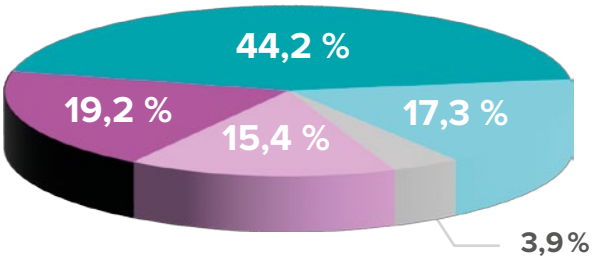
Je pro Vás způsob samourčení dostatečně srozumitelný?



- Ano – NÚKIB připravil naprosto srozumitelný návod, na základě něhož vím s jistotou, zda se mne bude nový zákon týkat či nikoli
- Ano – principiálně chápu způsob, jak vyhodnotit, zda pod nový ZKB spadnu či nikoli, ovšem na základě různých faktorů stojím na pomyslné hranici určení a nejsem proto schopen jednoznačně určit, zda se mne nový ZKB bude týkat
- Ne – ač se snažím vycházet z vodítek a podkladů poskytnutých ze strany NÚKIB, nejsem schopen se „najít" ve vyhlášce o regulovaných službách, a tudíž se budu muset obrátit na NÚKIB, aby rozhodl, zda se mne nový ZKB bude týkat
- Ne – způsob sebeurčení mi přijde složitý, nesrozumitelně popsaný a nechápu jej

Na základě výsledků otázky ohledně srozumitelnosti způsobu samourčení podle nového zákona o kybernetické bezpečnosti (ZKB) vyplývá, že většina respondentů, a to konkrétně 51,9 %, považuje Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB) připravený návod za naprosto srozumitelný. Tito respondenti prohlašují, že jsou schopni jednoznačně určit, zda se na ně nový ZKB vztahuje. Zároveň 34,6 % účastníků zaznamenává, že ačkoliv principy způsobu samourčení chápou, jejich konkrétní situace a různé faktory je staví na hranici určení, zda se nový ZKB na ně vztahuje. Nižší procentuální zastoupení pak zahrnuje skupiny respondentů, kteří buď hodnotí způsob sebeurčení jako složitý a nesrozumitelný (5,5 %), nebo jsou nuceni obrátit se na NÚKIB pro definitivní rozhodnutí o tom, zda se na ně nový ZKB vztahuje (8 %). Tyto výsledky poukazují na vysokou míru srozumitelnosti a dostupnosti informací o samourčení pod novým zákonem o kybernetické bezpečnosti ze strany dotazovaných.

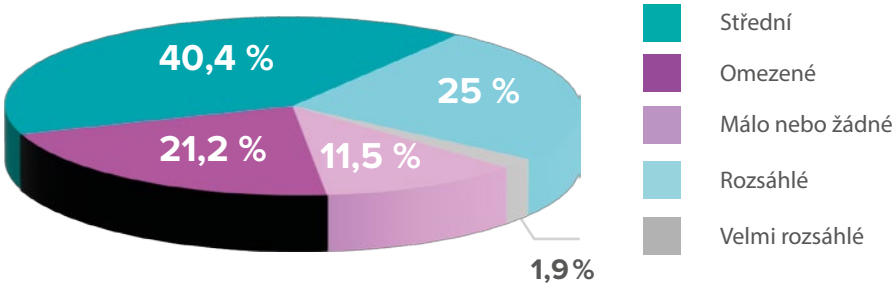
Jak jste informováni o požadavcích směrnice NIS2 a jejich aplikaci ve Vašem odvětví?



- Dobře
- Středně
- Zčásti
- Velmi dobře
- Nedostatečně

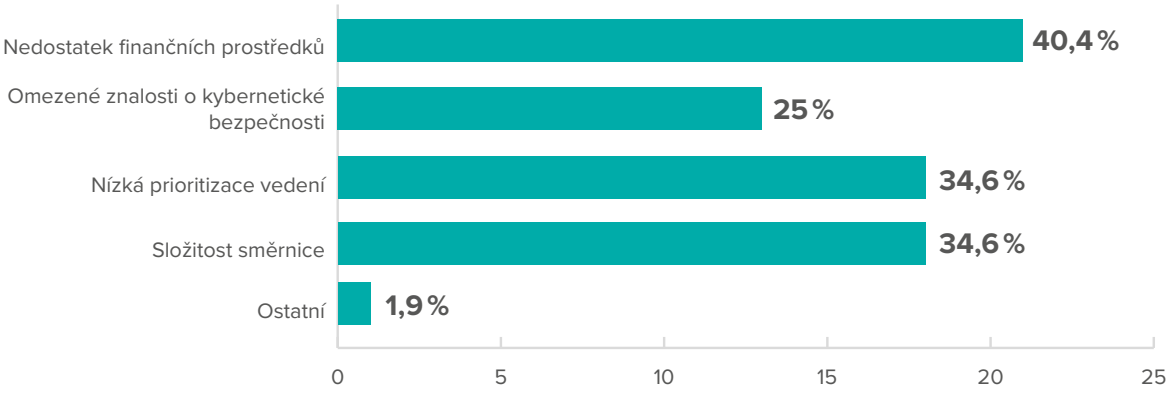
Z odpovědí na otázku týkající se informovanosti o požadavcích směrnice NIS2 a jejich aplikaci ve sledovaném odvětví vyplynulo, že většina respondentů má již dobré a velmi dobré povědomí o této směrnici. Celkem 61,5 % odpovědělo, že jsou informováni dobře až velmi dobře. Naopak, menší část respondentů (3,9 %) uvádí, že jsou informováni nedostatečně. Získaná data naznačují, že většina subjektů v průzkumu má alespoň střední úroveň informovanosti o požadavcích směrnice NIS2, což může signalizovat pozitivní trend směrem k širšímu povědomí a dodržování kybernetických bezpečnostních standardů ve sledovaném odvětví.

Kolik prostředků věnuje Vaše firma implementaci bezpečnostních opatření v souladu se směrnicí NIS2?



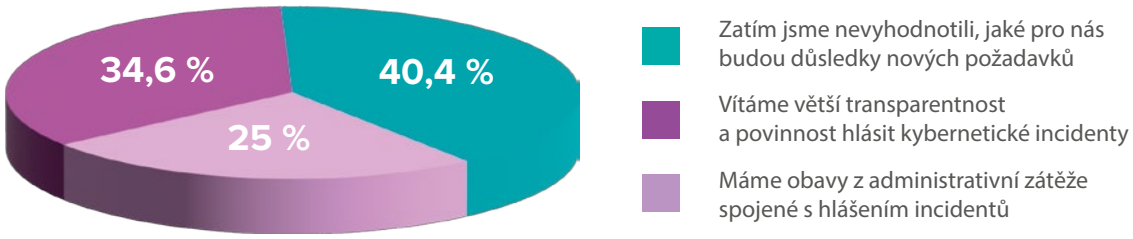
Na základě odpovědí u otázky týkající se financování implementace bezpečnostních opatření v souladu se směrnicí NIS2 vyplývá, že firmy přistupují k této problematice s různými přístupy a alokují finanční zdroje na kybernetickou bezpečnost v odlišné míře. Nejčastější odpovědí bylo "Střední", což naznačuje, že většina firem zvolila umírněný přístup k finančním investicím do bezpečnostních opatření. Významná část respondentů však vyjádřila ochotu věnovat "Rozsáhlé" finanční prostředky na zajištění kybernetické bezpečnosti, což zdůrazňuje význam této oblasti pro některé organizace. Méně častým jevem bylo vyčlenění " Velmi rozsáhlých" finančních prostředků, což svědčí o relativním omezení firemních zdrojů v této kategorii. Celkově se tedy zdá, že firmy volí variabilní přístup k financování bezpečnostních opatření, přičemž dávají přednost vyváženému postoji mezi náklady a efektivitou.

Které konkrétní výzvy považujete za nejtěžší při implementaci směrnice NIS2 ve Vaší organizaci? (možnost více odpovědí)



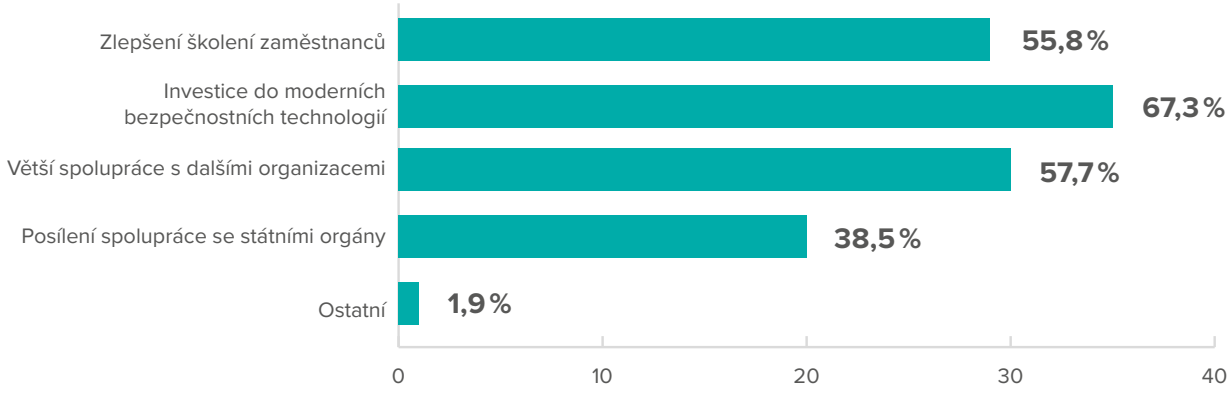
Z výsledků dotazníkového průzkumu vyplývá, že organizace čelí řadě výzev při implementaci směrnice NIS2. Značná část respondentů (40,4 %) identifikovala nedostatek finančních prostředků jako nejvýznamnější překážku. To naznačuje, že ekonomické omezení může být klíčovým faktorem brzdícím efektivní provedení bezpečnostních opatření. Dalším významným problémem je vnímán nedostatek odborníků a nízká znalost kybernetické bezpečnosti (25 %), což ukazuje na nutnost dalšího rozvoje odborných znalostí a dovedností v této oblasti. Zajímavým zjištěním je i téměř shodné procentuální zastoupení (34,6 %) dvou dalších faktorů: nízké prioritizace ze strany vedení a složitost samotné směrnice. Tato data poukazují na nutnost vyváženého přístupu, který zohledňuje jak technické a finanční aspekty, tak i potřebu zapojení vedení a snadné pochopení směrnice pro efektivní implementaci bezpečnostních opatření. Jako další výzvy respondenti uvedli nedostatek odborníků na kybernetickou bezpečnost, řízení dodavatelských řetězců či organizační neschopnost uživatelů.

Jaký je Váš postoj k novým požadavkům na hlášení kybernetických incidentů dle směrnice NIS2?



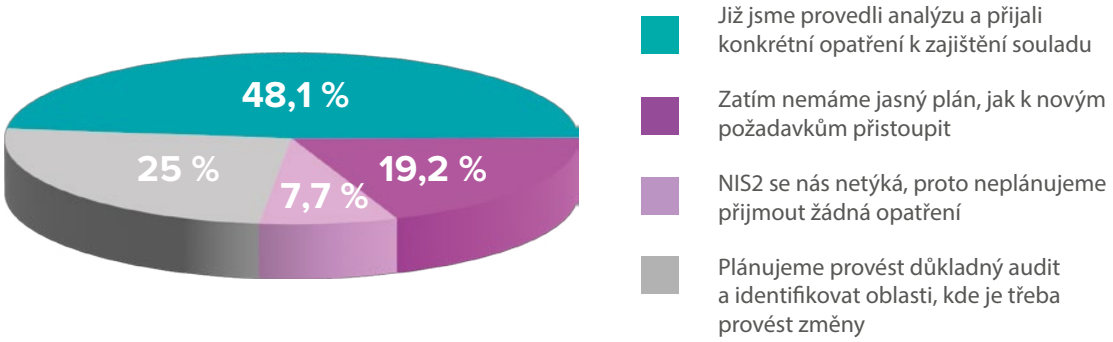
Odpovědi týkající se postojů k novým požadavkům na hlášení kybernetických incidentů dle směrnice NIS2 předkládají zajímavý obraz názorů respondentů. Zhruba 25 % z nich vyjádřilo obavy z administrativní zátěže spojené s hlášením incidentů, zatímco 34,6 % vítá větší transparentnost a povinnost hlásit kybernetické incidenty. Naopak, 40,4 % respondentů uvedlo, že zatím nevyhodnotili, jaké pro ně budou důsledky nových požadavků. Tato heterogenita názorů odráží rozmanitost postojů a potřeb organizací vůči novým opatřením v oblasti kybernetické bezpečnosti. Zároveň naznačuje, že i přes určité obavy existuje také podpora pro větší transparentnost a systematické hlášení kybernetických incidentů jako prostředku k posílení celkové kybernetické odolnosti.

Jaké změny ve strategii kybernetické bezpečnosti byste rádi viděli jako reakci na nové požadavky směrnice NIS2? (možnost více odpovědí)



Z výsledků analýzy otázky týkající se strategie kybernetické bezpečnosti a reakce na nové požadavky směrnice NIS2 vyplývají klíčové priority respondentů – viz graf výše (pozn. autora: u této otázky bylo možné uvést více odpovědí). Nejvíce se zdá, že organizace kladou důraz na investice do moderních bezpečnostních technologií, což podtrhuje 67,3 % odpovědí. Tato preference reflektuje rostoucí důležitost inovativních řešení při odolávání stále složitějším kybernetickým hrozbám. Dále v pořadí následuje zlepšení školení zaměstnanců, což bylo vybráno 55,8 % respondentů. Tato tendence ukazuje na význam osvěty a zvyšování kybernetické gramotnosti uživatelů. Větší spolupráce s dalšími organizacemi byla zvážena 57,7 % respondentů, což signalizuje uznání potřeby koordinovaného úsilí v boji proti kybernetickým hrozbám. Naopak, posílení spolupráce se státními orgány, i když stále relevantní, bylo označeno 38,5 % respondentů. Někteří z respondentů by si dále představovali lepší uvědomění důležitosti kybernetické bezpečnosti na úrovni vyššího managementu, automatizaci a centralizaci řízení rizik či lepší informování širší veřejnosti o kybernetické bezpečnosti (uvedeno pod odpovědí „Ostatní“).

Jaká opatření plánujete přijmout k zajištění souladu s požadavky směrnice NIS?



Ze získaných dat z dotazníku vyplývá, že většina respondentů (48,1 %) již provedla důkladnou analýzu a aktivně přijala konkrétní opatření k zajištění souladu s požadavky směrnice NIS2. Tato skupina projevuje vysokou úroveň připravenosti a odpovědnosti v reakci na nové kybernetické bezpečnostní normy. Zároveň 25 % respondentů plánuje provést důkladný audit a identifikovat oblasti, kde budou nutné změny, což naznačuje záměr vylepšit své kybernetické bezpečnostní postupy. Naopak 19,2 % respondentů zatím nemá jasný plán, jak k novým požadavkům přistoupit, což může odrážet potřebu dalšího informačního porozumění či zdrojů pro implementaci. Pouze malá část respondentů (7,7 %) tvrdí, že se jich směrnice NIS2 netýká, a proto neplánují přijmout žádná opatření.

Trendy v oblasti bezpečnostního vzdělávání

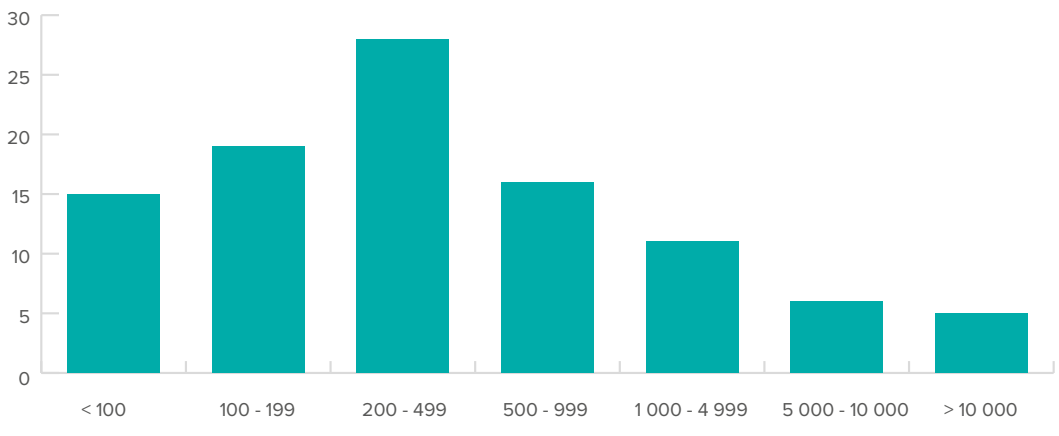
Radek Švadlenka

Vzdělávání zaměstnanců v oblasti kybernetické bezpečnosti se stalo neodmyslitelnou součástí bezpečnostní strategie všech organizací, které si uvědomují rizika spojená s hrozbami kyberprostoru, souvisejícími s nízkou či nulovou ostražitostí lidí. 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.

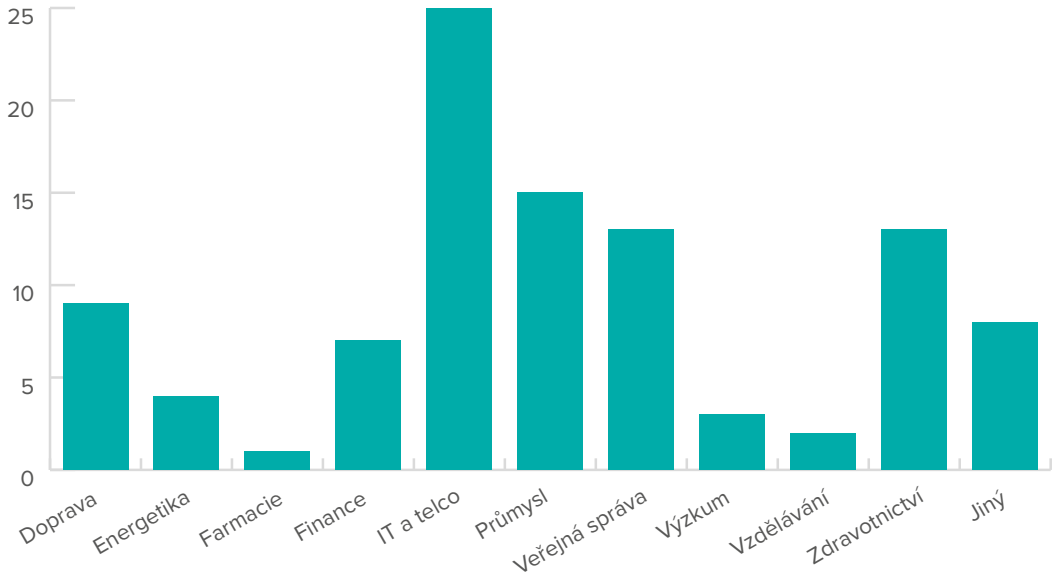
Není tedy žádným překvapením, že zákon o kybernetické bezpečnosti vyžaduje od povinných subjektů realizovat bezpečnostní opatření v podobě stanovení plánu rozvoje bezpečnostního povědomí, jehož cílem je zajistit odpovídající vzdělávání a zlepšování bezpečnostního povědomí uživatelů, administrátorů a osob zastávajících bezpečnostní role. Nový zákon o kybernetické bezpečnosti, který bude transponován do české legislativy z evropské směrnice NIS2 bude explicitně vyžadovat přímé zapojení top managementu do těchto vzdělávacích aktivit.

Každoročně uveřejňujeme výsledky průzkumu zaměřeného na realizované a plánované vzdělávací programy a aktivity organizací a ani tento rok není výjimkou. Abychom byli schopni sledovat trendy ve vývoji těchto aktivit, připravili jsme pro Vás nový průzkum za rok 2023 s ohledem na plánovaná opatření pro rok 2024. Ani v průběhu loňského roku nebylo na globální úrovni o aktivity související s bezpečností rozhodně nouze. O to zajímavější by mělo být meziroční srovnání plánovaných a realizovaných aktivit v oblasti vzdělávání v kybernetické bezpečnosti. Našeho průzkumu se zúčastnilo bezmála sto organizací různých zaměření a velikostí, jak je vidět z grafů níže. Výzkumný vzorek je velmi podobný tomu z loňského roku, a to jak s ohledem na počet respondentů, tak i v poměru zastoupení organizací dle oboru a velikosti.

Procentuální zastoupení organizací dle velikosti

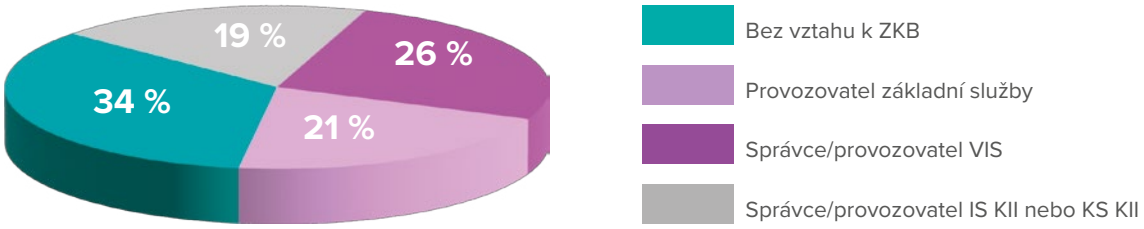


Procentuální zastoupení oragnizací dle oboru



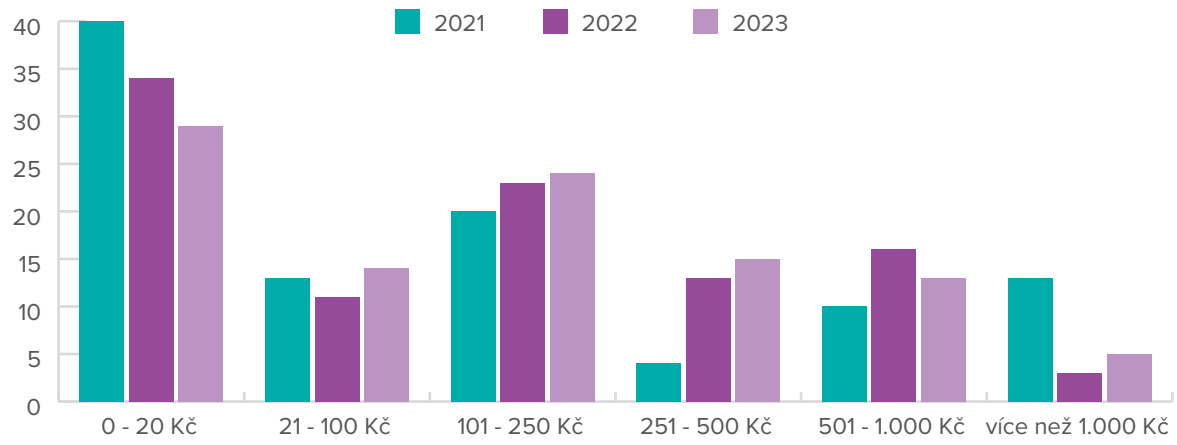
Aby interpretace jednotlivých výstupů nebyla zkreslena, je třeba upřesnit, že téměř dvě třetiny respondentů průzkumu se řadí mezi povinné subjekty podle zákona o kybernetické bezpečnosti, jak ilustruje následující graf.

Vztah organizací k ZKB



Realizaci vzdělávacích aktivit v oblasti kybernetické bezpečnosti je možné zajistit za pomoci jak interních, tak i externích zdrojů v podobě prezenčních školení či e-learningových nástrojů. Trendem posledních let, zejména v souvislosti s pandemií, byla školení realizovaná prostřednictvím virtuálních a online platforem. Pojďme se podívat, jak se situace v oblasti vzdělávání vyvíjela v posledních třech letech. V grafu níže je možné sledovat porovnání investovaných prostředků do vzdělávání v letech 2021, 2022 a 2023. Jako pozitivní trend je možné označit postupný pokles počtu organizací, které investují do vzdělávacích aktivit méně než 20 Kč měsíčně na uživatele. Celkem logicky pak meziročně rostl počet firem investujících do vzdělávání mezi 101 Kč až 500 Kč na zaměstnance. Bohužel, množství organizací s ochotou investovat do vzdělávání zaměstnanců 500 Kč a více se meziročně drží stále na poměrně nízké úrovni.

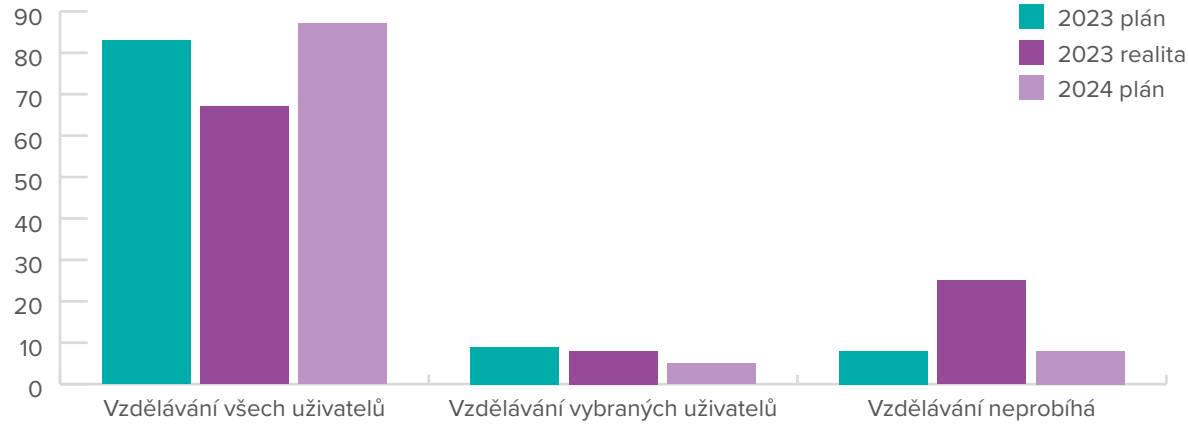
Zastoupení organizací dle výdajů na vzdělávání v kybernetické bezpečnosti



Vzdělávání uživatelů – realita versus plán

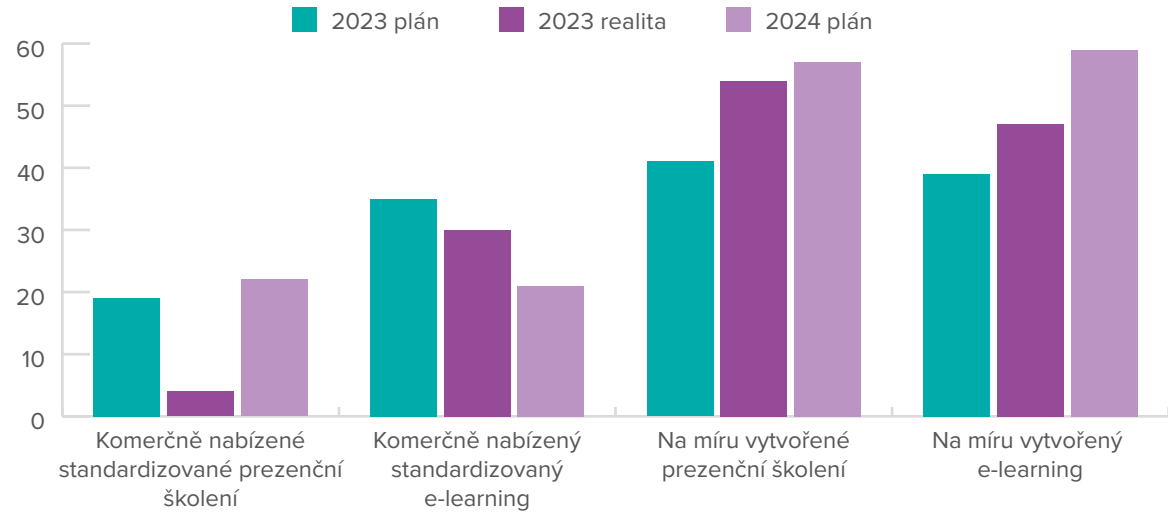
V této části průzkumu se zástupci organizací vyjadřovali k realizovaným a plánovaným aktivitám v oblasti vzdělávání uživatelů s výjimkou bezpečnostních rolí. Bohužel z grafu níže je patrné, že plány z roku 2022 pro vzdělávání všech uživatelů nebyly v roce 2023 zdaleka naplněny. Naopak počet organizací, kde vzdělávání vůbec neprobíhá je trojnásobný oproti plánu z předchozího roku. Pozitivní trend není vidět ani u vzdělávání vybraných uživatelů, kde realita lehce zaostala za plánem z roku 2022. Co se týče plánu vzdělávacích aktivit pro rok 2024, v podstatě se hodnotově příliš neliší od plánu pro rok 2023 s mírně rostoucím trendem v oblasti vzdělávání všech uživatelů. Jaká však bude realita je těžké predikovat zejména s ohledem na další faktory (např. konflikty na Ukrajině, Blízkém východě), které mohou významně ovlivnit výsledky.

Vzdělávání uživatelů v organizacích



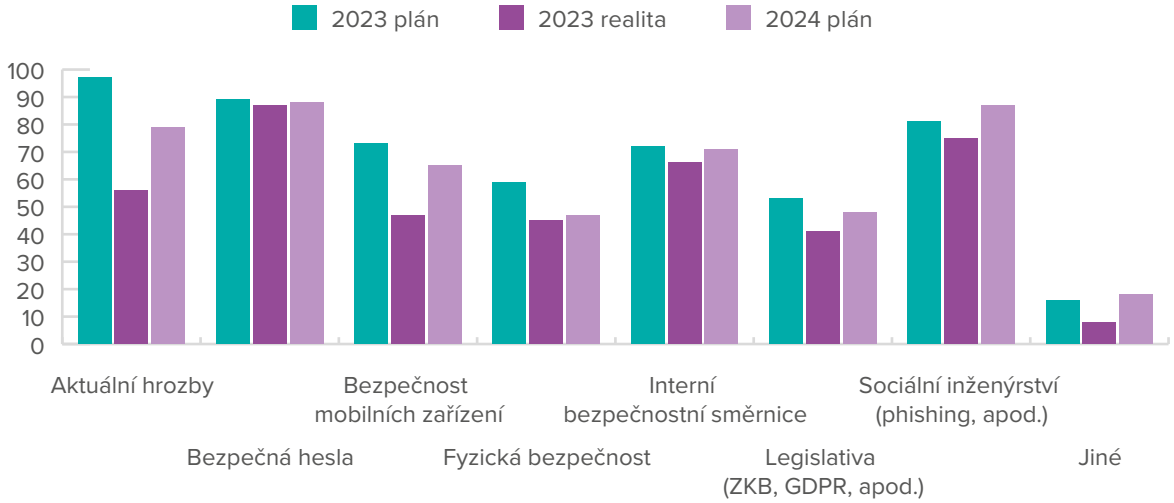
Zatímco vzdělávání uživatelů obecně nemá v posledních letech velké odlišnosti, jak bylo demonstrováno v předchozím grafu, pojďme se podívat, zda je tomu jinak u plánovaných a realizovaných forem vzdělávání uživatelů. Jak je patrné z obrázku níže, v roce 2023 došlo k omezení prezenčních standardizovaných školení ve prospěch na míru vytvořených oproti plánu stanoveném na konci roku 2022. Obdobná situace je patrná i v případě e-learningové formy vzdělávání, kde plánované stadardizované formy ustoupily na míru vytvořeným e-learningům. Z odpovědí týkajících se plánu na rok 2024 je možné predikovat pokračující trend migrace a odklon od standardizovaných vzdělávacích aktivit k na míru vytvořeným studijním formám vzdělávání. Jako pozitivní můžeme vnímat fakt, že plánované formy aktivit ve vzdělávání uživatelů jsou s ohledem na předchozí roky poměrně ambiciózní.

Realizované/plánované formy vzdělávání uživatelů



Za nepříliš optimistický je možné pokládat vývoj v oblasti zaměření vzdělávání pro uživatele. Oproti plánovaným aktivitám došlo ve všech kategoriích k významnému poklesu v počtu firem zaměřujících se na danou oblast. Největší zájem byl jako tradičně spojen s problematikou bezpečných hesel a sociálním inženýrstvím. Naopak méně organizací se soustředilo na oblast legislativy a fyzické bezpečnosti. Plán zaměření vzdělávacích aktivit pro uživatele na rok 2024 se příliš neliší od plánu pro rok 2023, bohužel však s mírně klesajícím trendem téměř ve všech oblastech výzkumu.

Zaměření vzdělávacích aktivit pro uživatele

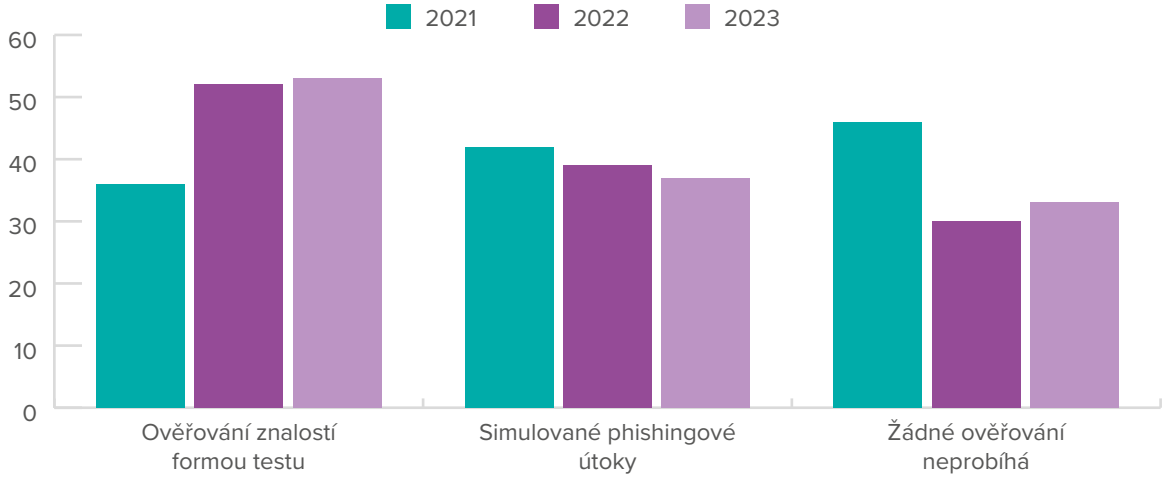


Velice efektivní, ale zároveň také mezi zaměstnanci málo oblíbené, jsou aktivity spojené s ověřováním znalostí a ostražitosti uživatelů v oblasti kybernetické bezpečnosti. Obrázek níže ilustruje aktuální rozložení využívání těchto aktivit u sledovaného vzorku subjektů.

Bohužel celkový trend spojený s těmito aktivitami nevykazuje jednoznačně pozitivní vývoj. Ověřování znalostí formou testů sice využívá meziročně stále více organizací, meziroční nárust v posledním sledovaném období je však zanedbatelný. Počet organizací, zaměřujících se na ostražitost uživatelů pomocí simulovaných phishingových útoků klesá meziročně o 2-3 %. Negativní trend je možné po-

zorovat i na počtu organizací kde žádné ověřování ostražitosti uživatelů neprobíhá. Hodnota za rok 2022 sice překonala výsledek z roku 2021, nicméně v roce 2023 počet organizací, které těmto aktivitám nevěnují pozornost, opět vzrostl. Mírný optimismus může být spojen alespoň s výhledem na rok 2024, kdy 79 % organizací plánuje zavést alespoň nějaké aktivity zaměřené na ověřování znalostí uživatelů v oblasti kybernetické bezpečnosti.

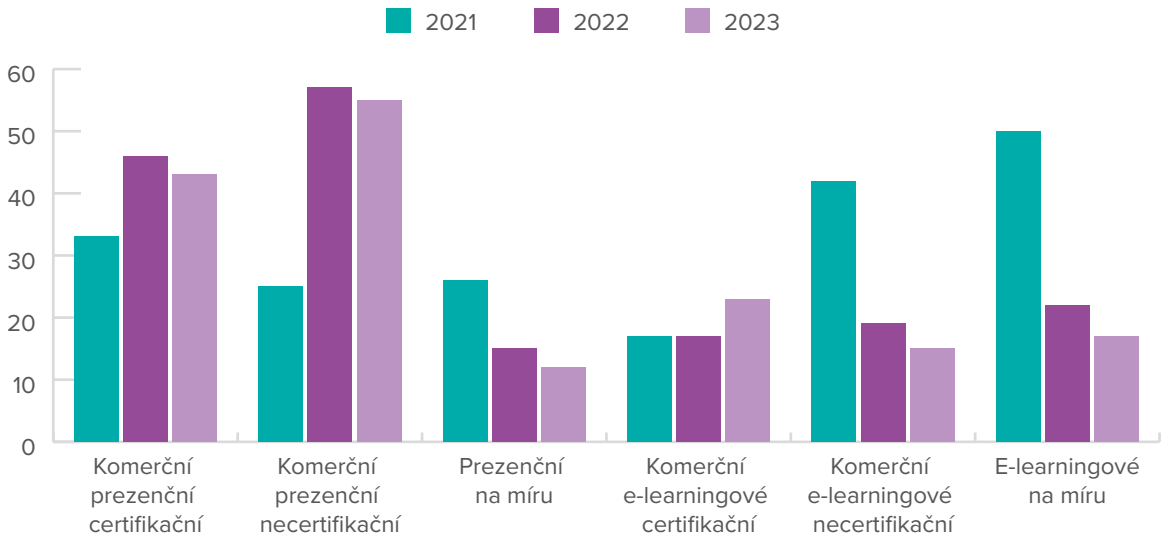
Ověřování znalostí a ostražitosti uživatelů



Vzdělávání odborných rolí

Zaměstnanci na pozicích administrátorů a bezpečnostních expertů jsou klíčoví pro plánování, realizaci a udržitelnost bezpečnostních pravidel v organizaci. Jejich znalosti a dovednosti mohou mít významný dopad na efektivitu zvládání bezpečnostních incidentů. Na grafu níže je zobrazeno meziroční porovnání realizovaných forem vzdělávání bezpečnostních rolí v organizacích. Na první pohled je patrný meziroční pokles téměř ve všech kategoriích e-learningových kurzů včetně certifikačních. Jedinou výjimkou jsou komerční e-learningové certifikační kurzy, jejichž využití vzrostlo meziročně o 6 %. Dlouhodobě však můžeme sledovat odklon od e-learningových vzdělávacích aktivit, které byly logicky preferované v době pandemie.

Realizované formy vzdělávání bezpečnostních rolí

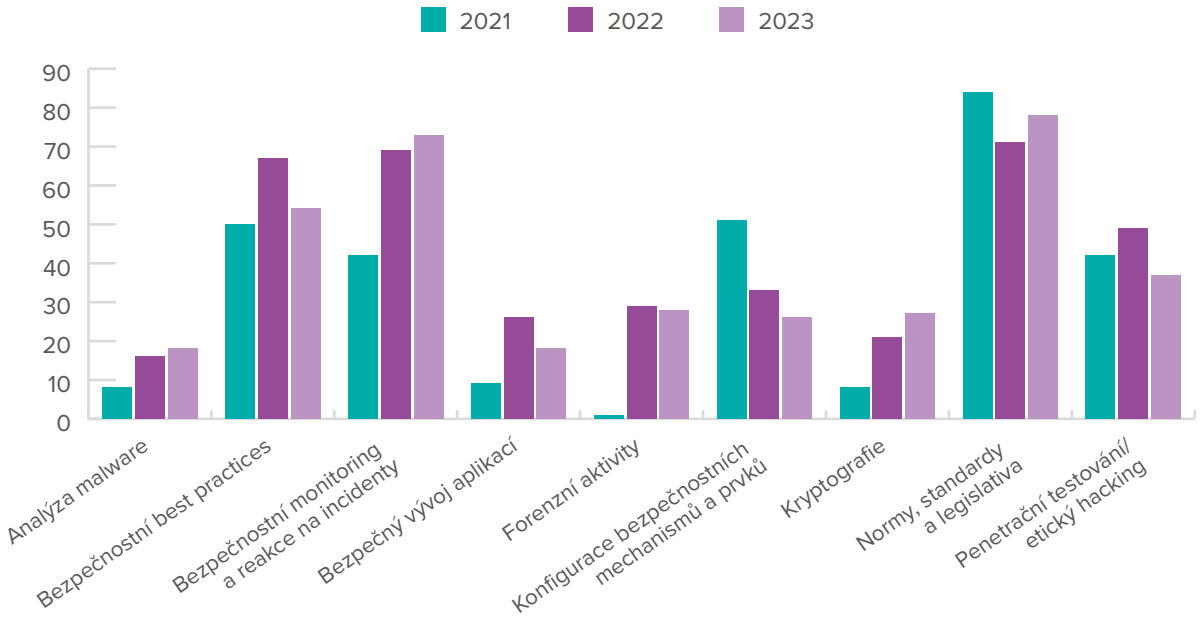


Vzdělávání odborných rolí bývá na rozdíl od vzdělávání uživatelů mnohem specifičtěji zaměřeno. Z průzkumu vyplývá, že největší zájem v roce 2023 byl o školení v oblasti legislativy, pravděpodobně s ohledem na transpozici NIS2 do české legislativy.

Mezi další atraktivní oblasti vzdělávání pro odborné role evidentně patří bezpečnostní monitoring a reakce na bezpečnostní incidenty a bezpečnostní best pactices. Každé z výše vyjmenovaných zaměření vzdělávání bylo využito v roce 2023 téměř polovinou respondentů.

Mezi dlouhodobě „slabá“ témata z hlediska vzdělávání bezpečnostních rolí je možné zařadit oblasti analýzy malware a bezpečného vývoje aplikací, které nedosáhly z hlediska využití nad testovacím vzorkem hranice dvaceti procent, jak je patrné z grafu níže. Naopak dlouhodobě podceňované téma kryptografie zažilo meziročně lehké oživení zájmu, tak uvidíme, jak tomu bude napřesrok.

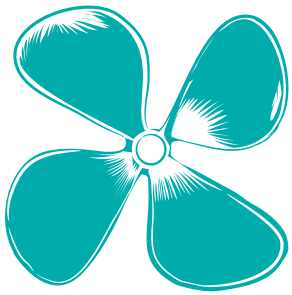
Zaměření vzdělávacích aktivit pro bezpečnostní role



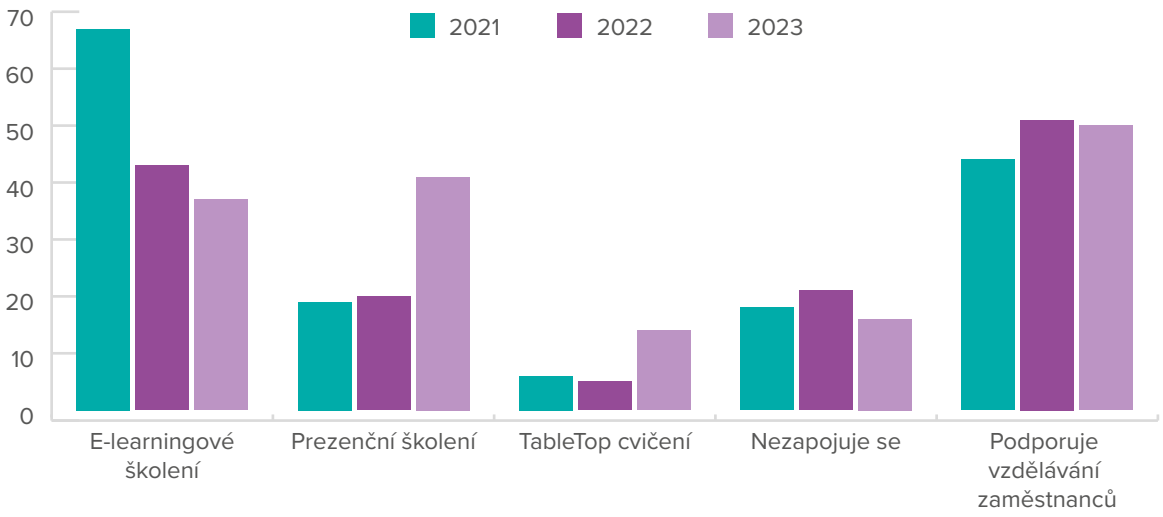
Zapojení top managementu do vzdělávacích aktivit

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

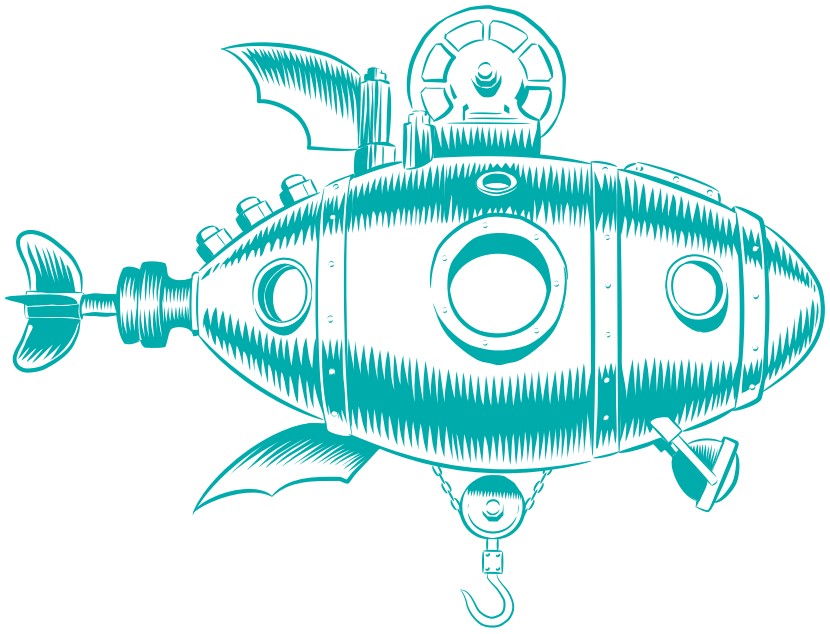
Zajímalo nás tedy, jak se top manažeři vypořádávají s touto problematikou. Pozitivní zprávou je, že meziročně klesl počet manažerů, kteří se vůbec nezapojují do vzdělávacích aktivit. Zároveň výrazně vzrostl podíl vedoucích pracovníků, kteří se vzdělávají prezenční formou školení. Dříve preferovaná forma e-learningových školení naopak ustupuje ve prospěch již zmíněných prezenčních forem školení, ale i TableTop cvičení. Podpora vzdělávání v oblasti kybernetické bezpečnosti ze strany top manežerů se drží na úrovni 50 %. Optimisticky je možné pojmout fakt, že účast vrcholového managementu na TableTop cvičeních vzrostla meziročně více než dvojnásobně.



Zapojení top managementu do vzdělávacích aktivit v oblasti kybernetické bezpečnosti



Závěr tohoto příspěvku je obohacen o zajímavé odpovědi z řad respondentů, týkající se top managementu a jeho orientace v kybernetické bezpečnosti a také vlivu konfliktu na Ukrajině na organizace. Celkem 87 % respondentů je přesvědčeno, že vyšší vzdělanost vrcholového managementu v kybernetické bezpečnosti má pozitivní vliv na rozvoj bezpečnosti v organizaci. Více než 50 % účastníků průzkumu souhlasí s názorem, že hlavním faktorem pro ochotu managementu investovat zdroje do kybernetické bezpečnosti jsou medializované kybernetické incidenty, případně interní incidenty. Zároveň 43 % dotázaných odpovědělo, že hybnou silou pro investice do kybernetické vzdělanosti je právě úroveň orientace top managementu na poli kybernetické bezpečnosti. Přibližně polovina respondentů jako důsledek kofliktu na Ukrajině vyzdvihuje promítnutí souvidejících hrozeb do interních procesů a vzdělávacích aktivit. U druhé poloviny respondentů nebyly zaznamenány žádné změny v přístupu k bezpečnosti v souvislosti s tímto konfliktem. Nechme se tedy překvapit, jak se bude vyvíjet řízení bezpečnosti v roce příštím. Například v souvislosti s novými ohnisky konfliktů na Blízkém východě.



Budoucnost začíná nyní. Predikce pro rok 2024

Jan Hrubý

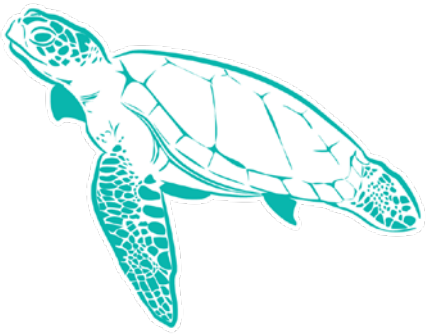
Co byste měli vědět podle společnosti Splunk, která se zabývá big data analýzou o podnikání v době umělé inteligence?

Jsme na začátku nové éry. Pro některé je umělá inteligence splněným snem: Umožňuje autonomním vozidlům vozit lidi po rušných městských ulicích a generuje podrobný itinerář pro vaši nadcházející dovolenou. Pro jiné však umělá inteligence klade otazníky ohledně budoucnosti jejich kariéry.

Navzdory veškerému rozruchu kolem umělé inteligence budou mít vedoucí pracovníci v příštím roce v agendě mnoho dalších věcí. Rok 2024 bude rokem transformace – budou se řešit témata od udržitelnosti, přes konsolidaci nástrojů s cílem zjednodušit a snížit náklady na IT infrastrukturu, až po kyberbezpečnost s nadcházející účinností NIS2. Uvidíme také dramatické změny v prioritách vedení firem, protože vlády po celém světě přijímají přísnější zákony týkající se ochrany dat, kybernetické bezpečnosti a digitální odolnosti.

Výzkum od společnosti Splunk ukazuje, že organizace zažívají průměrně 10 dní neplánovaného výpadku každý rok. Cílem nařízení, které se týkají kybernetické odolnosti je toto číslo stlačit blíže nule, zejména pro kritické služby. Globálně budeme svědky trendu, kdy po firmách bude požadováno, aby hlásily úroveň své kybernetické odolnosti nad rámec plánu kontinuity podnikání a řízení rizik. Firmy budou muset prokázat, že mají schopnost reagovat na přírodní katastrofy, další případnou pandemii a na regionální poruchy infrastruktury.

V této nové éře je jedno jisté: Vedoucí pracovníci z byznysu budou budovat hlubší vztahy s lidmi od technologií, aby společně navigovali firmu v neznámých vodách.



Předpověď: Umělá inteligence

Umělá inteligence přinese postupné zisky v efektivitě a produktivitě v krátkodobém horizontu, ovšem vedoucí pracovníci budou muset nejprve vidět, aby uvěřili. Zásadní změny v dopadu na podnikání jsou tedy stále 12 až 24 měsíců vzdáleny. Umělá inteligence bude mít na podnikání tak velký vliv jako internet, ale podle generálního ředitele společnosti Splunk Garyho Steela to ještě chvíli potrvá.

Každopádně to začne automatizací. Automatizace se stane velkým zaměřením ve vývoji umělé inteligence, protože bude důležitým motorem produktivity v podnikání. Ale to není vše - umělá inteligence také pomůže společnostem řídit rizika, poněvadž tento rok ukáže větší potenciál při ochraně organizací před kybernetickými útoky. Využívání prediktivních a generativních modelů umělé inteligence poskytne bezpečnostním týmům získávat informace, hledat mezi nimi vzory a stanovovat prioritní hrozby.

„Krása umělé inteligence spočívá v tom, že proniká do každého typu organizace," říká Steele. „Takže ji uvidíme využívanou napříč odvětvími s rovnocenným dopadem," dodává.

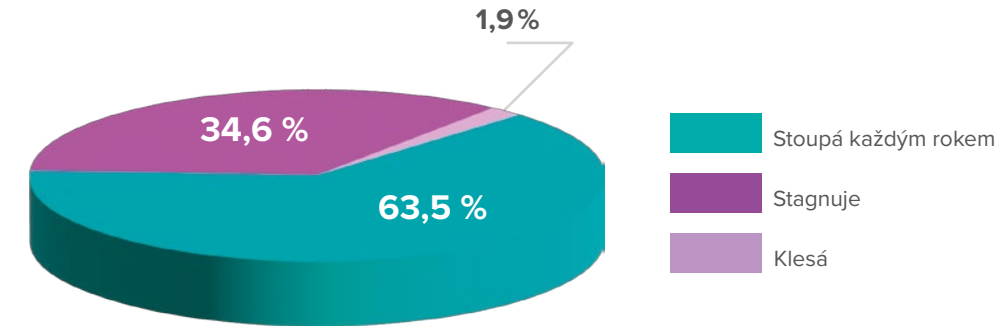
Předpověď: Odolnost

Odolnost se stane neoddiskutovatelnou, poněvadž vlády po celém světě ji budou nařizovat.

V reakci na vzestup nových hrozeb a současně klíčový význam digitálních systémů pro ekonomiku začínají regulátoři zavádět přísné rámce toho, jak by se firmy měly připravit a chovat se při bezpečnostních incidentech.

A jak to vypadá v České republice?

63,5 % firem říká, že počet bezpečnostních událostí posledních 5 let stoupá každým rokem



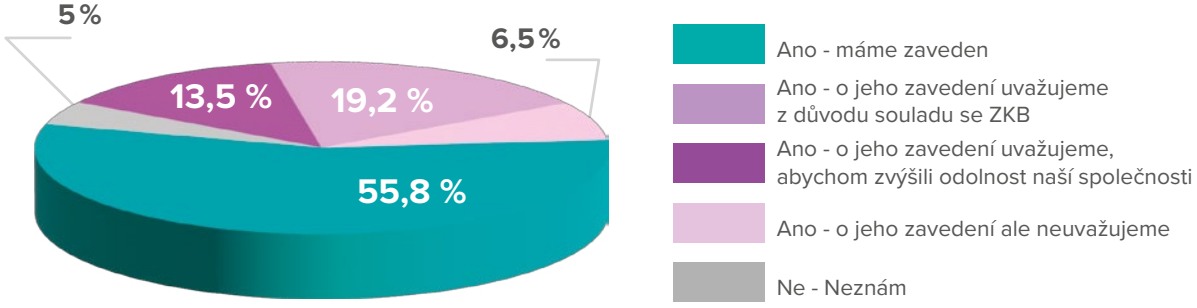
V EU existují nařízení pro konkrétní odvětví, jako je Nařízení EU o digitální provozní odolnosti finančních institucí (DORA). A v tomto roce se bude napříč členskými zeměmi implementovat směrnice o síťové a informační bezpečnosti NIS 2.

Kybernetické riziko se stává existenčním rizikem a kybernetická odolnost organizace může být klíčovým aspektem, který rozhodne nejen o krátkodobé ztrátě obchodu, ale i o zániku firmy, což znamená, že se do řešení budou muset zapojit všichni členové nejužšího vedení. Správní rady firem v USA nyní vytvářejí výbory zahrnující bezpečnost, odolnost a dodržování pravidel v organizaci. „Když výbor posuzuje kybernetické postavení společnosti, potřebuje komplexní pohled na riziko napříč celým podnikem," říká hlavní strategický ředitel Splunku Ammar Maraqa. Takže role CISO, CTO a CIO se rozšíří a stanou se strategičtějšími a vedoucí právních oddělení a finanční ředitelé se budou muset stát odborníky na kybernetickou bezpečnost.

Jedním ze základních nástrojů kybernetické bezpečnosti je SIEM (Security Information and Event Management). Přes 80 % českých firem zapojených v našem průzkumu již má tento nástroj zaveden, nebo o něm uvažují, což dokazuje, že dané společnosti berou svou bezpečnost vážně.

Tento rok bude největší výzvou pro vedoucí technologických oddělení zlepšit vzdělání nejužšího vedení o rizicích, kterým organizace čelí, aby mohli efektivně prioritizovat a budovat strategie k jejich řešení. Správní rady ocení pevná data a technologičtí vedoucí musí předkládat jasné záměry pro své investice opřené o předchozí debatu s dalšími klíčovými odděleními v rámci organizace.

Znáte bezpečnostní nástroj SIEM (Security information and event management)?

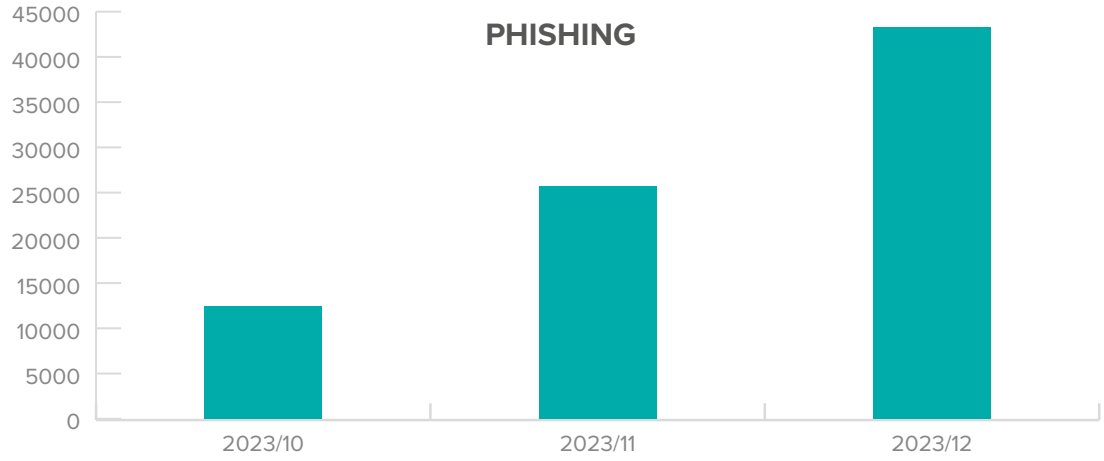


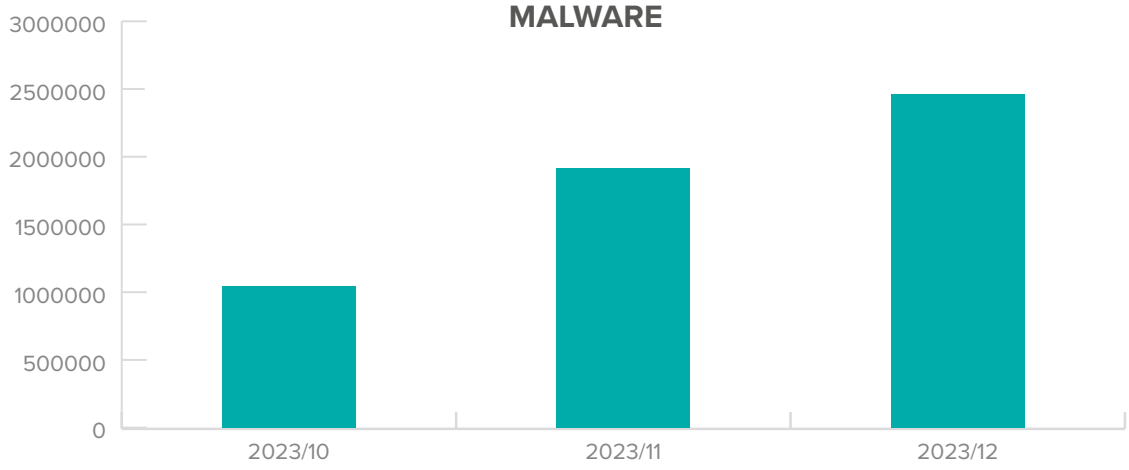
Analýza událostí zachycených IPS sondami

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 posledního kvartálu roku 2023.

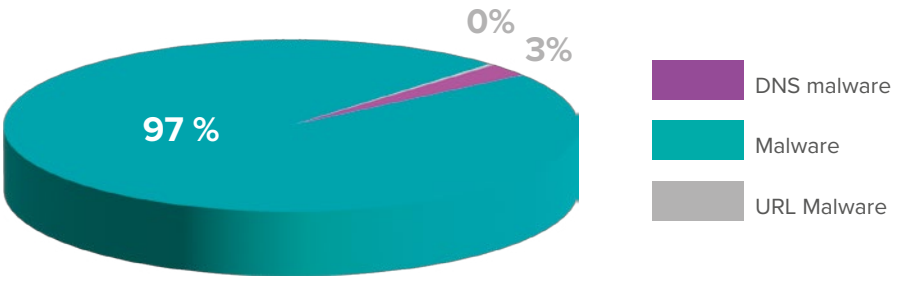
V první části analýzy se nejprve podíváme na phishing. IPS sondy detekovaly incident vždy, když se uživatel pokusil navštívit blokované phishingové stránky. Největší počet incidentů z minulého roku byl zaznamenám v prosinci. Bylo detekováno přes v 43 tisíc incidentů, což je o více než 2 tisíce incidentů více oproti předchozímu roku za totožný měsíc. Ke konci roku 2023, obdobně jako v minulých letech, došlo k postupnému nárustu phishingových útoků související s vyšší aktivitou uživatelů na internetu.





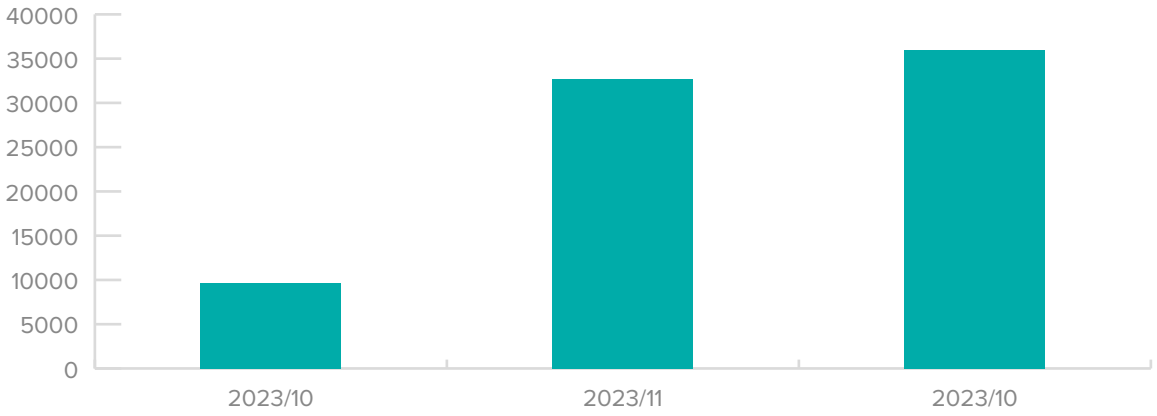
Za poslední tři měsíce roku 2023 bylo největší množství incidentů spojených s malwarem zachyceno IPS systémy v měsíci prosinci, šlo o více než 2,4 miliónu událostí. Jedná se o stonásobný nárůst oproti předchozímu roku za totožné období. Vyšší četnost těchto útoků je dána vyšší uživatelskou aktivitou na internetu spojenou s koncem roku. K obdobnému, ale ne tak razantnímu zvýšení počtu detekovaných incidentů v tomto období dochází pravidelně, jak ukazují mimo jiné i data z předešlých let.

MALWARE STRUKTURA



Detekce spojené se škodlivým kódem člení sledované IPS systémy do tří základních kategorií. V kategorii malware se nacházejí události, při kterých byla identifikována shoda s reputační databází IPS, která obsahuje IP adresy, na nichž se vyskytuje nebo vyskytoval malware. Porovnává se při tom jak zdrojová, tak i cílová IP adresa. Kategorie URL malware obsahuje pouze adresy, na nichž byl zaznamenán výskyt malwaru. Samotnou detekci provádí sondy na základě analýzy webového provozu s pomocí kontroly URL. Poslední kategorií je DNS malware, reputační databáze v tomto případě obsahuje seznam domén, u kterých byl detekován malware. Událostmi jsou v takovém případě detekované DNS dotazy na škodlivé domény, o jejichž překlad se pokusil malware nacházející se uvnitř chráněných sítí. Za sledované období posledního kvartálu roku 2023 byla struktura detekcí malwaru následující: z 97 % byly detekce výskytu malwaru realizovaného pomocí reputační databáze, ze 3 % se jednalo o detekci využívající kontrolu DNS a ve zbylých detekcích okolo 0,04 % byl malware odhalen prostřednictvím provedené URL kontroly (viz. graf Detekce škodlivého kódu).

CRYPTOMINING



Jednotlivé „Cryptomining“ události jsou detekovány pomocí reputační databáze IP adres, u nichž byly v minulosti a současnosti vedeny pokusy o těžbu kryptoměn. Detekce se dále zaměřuje na stahování a analyzování binárních dat, webových klientů, těžebních protokolů, black-list domén a SSL certifikátů. V prosinci 2023 byl zachycen nejvyšší počet pokusů o těžbu kryptoměn o celkovém množství 35966 pokusů. V pořadí druhým měsícem s nejvyšším množstvím pokusů o těžbu kryptoměn byl měsíc listopad, kdy bylo zablokováno přes 32 655 pokusů. Za měsíc říjen bylo detekováno jen přes 9 tisíc pokusů o těžbu kryptoměn, což je o více než 20 tisíc pokusů méně oproti posledním dvěma měsícům v roce 2023. Vyšší četnost těchto detekovaných událostí je do jisté míry spojena s vyšší uživatelskou aktivitou na internetu, spojenou s nákupy vánočních dárků a aktivitami uživatelů spojenými s koncem roku.

Rok 2023 a Kybernetická Bezpečnost: Ransomware, Umělá Inteligence a Evoluce Hrozeb

Stanislav Novotný

V rámci neustále se vyvíjející kybernetické scény přinesl rok 2023 příběh neúnavného úsilí orgánů činných v trestním řízení a dynamických výzev, s nimiž se musely organizace vypořádat.

Sledovat jsme mohli nejen úspěchy v boji proti organizovaným skupinám, ale i odolnost ransomwarových skupin, které se často dokázaly vrátit zpět do provozu. Ransomware zažívá vzestup a umělá inteligence se stala jak nástrojem, který pomáhá při obraně, tak i zbraní kyberzločinců. V tomto článku se tak blíže podíváme na prominentní trendy v kyberprostoru a jejich dopad na vývoj bezpečnosti.

Policejní orgány pracovaly přesčas.

V minulém roce jsme mohli sledovat stále častější a úspěšnější akce policejních orgánů proti organizovaným skupinám operujícím v kyberprostoru. Nutno podotknout, že ransomwarovým skupinám se často dařilo svou činnost obnovit, a to buď pod jiným jménem, nebo připojením pod jinou skupinu.

Příkladem může být skupina HIVE a dění okolo ní v lednu minulého roku. Europol podpořil německé, nizozemské a americké úřady při likvidaci infrastruktury této plodné ransomwarové skupiny. Orgány získaly dešifrovací klíče a poskytly je mnoha obětem, čímž jim pomohly získat zpět přístup k jejich datům, aniž by musely zvažovat platbu výkupného. V listopadu ale nová skupina s názvem Hunters International získala zdrojový kód. Infrastrukturu z operace Hive, která byla tou dobou již zrušená a zahájila své vlastní úsilí v oblasti kyberkriminality.

Ke konci minulého roku se pokusily policejní složky v čele s FBI zničit infrastrukturu za skupinou ALPHV, která ale dokázala svoji operaci udržet funkční.

Při hledání šéfa skupiny za ransomwarem Ragnar Locker napomáhala také česká policie. V česku probíhaly domovní prohlídky, protože zde údajně měl mít domov. Nalezen a zatčen byl nakonec v Paříži. Skupina Ragnar Locker byla zodpovědná za řadu významných útoků na kritickou infrastrukturu po celém světě. Mezinárodním orgánům se také podařilo zlikvidovat síť malwaru Qakbot.

Ransomware na vzestupu... stále.

Ransomware byl analyzován ve zprávě společnosti Corvus Insurance. Podle této zprávy aktivita ransomwaru za celý rok překonala celkové hodnoty oproti roku 2022 o 68 %. Byl také zaznamenán nový rekord v počtu ransomware útoků - celkem 4 496 obětí, zatímco v roce 2022 jich bylo evidováno 2670 a v roce 2021 o něco více, tedy 3048.

Rok	Počet obětí dle stránek s úniky
2023	4 496
2022	2 670
2021	3 048

Jedná se ale pouze o částečný obrázek reality. Oběti ransomwaru, které rychle zaplatí výkupné, se nemusí objevit na stránkách s úniky, a proto je možné, že zde nebyly započítány. Přesné číslo sice nikdo nezná, ale podle odhadů spol. Corvus spadá do této kategorie 27 % až 41% obětí ransomwaru, které zaplatí výkupné. To znamená, že křivka celkového počtu obětí ransomwaru se bude v roce 2023 pohybovat mezi 6 100 a 7 600 organizací.

Počet aktivních skupin ransomwaru se mezi 1. a 4. čtvrtletím 2023 zvýšil o 34 %. Tento nárůst lze přičíst rozpadu známých skupin, které na dark web vypustily své vlastní šifrovací programy, čímž je zpřístupnily novým aktérům, kteří následně zahájili vlastní operace s ransomwarem. Nejméně 10 nových skupin ransomwaru například použilo šifrátor Babuk, který unikl v roce 2021.

Bezmála 36 % organizací utrpělo v roce 2023 ransomwarové útoky kvůli zneužitým zranitelnostem. Druhou nejčastější příčinou úspěšných ransomware

útoků byla krádež pověření, zatímco na třetím místě se umístil škodlivý e-mail. Průměrné celosvětové náklady spojené s narušením dat v roce 2023 lehce přesáhly 100 milionů CZK, což představuje 15% nárůst za poslední tři roky. Tři nejaktivnější ransomware skupiny v roce 2023 byly LockBit, ALPHV/BlackCat a CL0P.

Za zmínku stojí i větší důraz ransomwarových skupin na krádež dat, oproti pouhému zašifrování. Skupiny pochopily, že pro jejich oběti je to často daleko větší problém, za jehož vyřešení jsou ochotni zaplatit. Nárůst obliby mezi kyberzločinci zaznamenal také koncept služeb. Ransomware jako služba (Ransomware-as-a-Service) je například obchodní model, v jehož rámci jednotlivec zaplatí zkušenému vývojáři ransomwaru za to, že k provedení útoku použije jeho hotový ransomware. Na stejném principu pak také fungují další služby, například phishing jako služba.

Umělá inteligence, kam se podíváš.

Generativní umělá inteligence vzala svět útokem na konci roku 2022 a v roce 2023 zažila obrovský růst na popularitě a s tím se objevily nové obavy a výzvy.

Počátkem roku 2023 se objevily důkazy o používání modelu ChatGPT ke škodlivým účelům, například k vytváření malwaru nebo přípravě phishingových e-mailů. To vedlo organizace OpenAI a Google, který spustil konkurenční model Bard, k zavedení ochranných opatření, která mají takovému zneužití zabránit.

Kyberzločinci začali vytvářet své vlastní škodlivé modely umělé inteligence, jako WormGPT, FraudGPT, WolfGPT, XXXGPT, PoisonGPT nebo DarkBard. Podle zjištění služby Digital Footprint Intelligence společnosti Kaspersky z roku 2023 zaznamenali bezpečnostní výzkumníci pozoruhodný nárůst diskusí na temném webu týkající se používání ChatGPT a dalších velkých jazykových modelů ke škodlivým účelům. Bylo identifikováno téměř 3 000 příspěvků, které se zaměřovaly na spektrum kybernetických hrozeb, od vytváření škodlivých verzí chatbotů až po zkoumání alternativních projektů, jako jsou XXXGPT a FraudGPT.

Zatímco vrchol zažily chatboti v březnu loňského roku, probíhající diskuse naznačují trvalý zájem zločinců o využívání technologií umělé inteligence k nelegálním aktivitám. V budoucích letech se také očekává nárůst u útoků, které využívají tzv. deepfakes.

Nový zákon o kybernetické bezpečnosti.

Evropská unie v prosinci roku 2022 schválila novou bezpečnostní směrnici NIS2. Její zavedení do českého právního řádu je tak jedním z hlavních úloh připravovaného zákona.

Návrh počítá s několikanásobným rozšířením počtu regulovaných subjektů. Předpokládá se, že z nynějších přibližně 400 tento počet stoupne na více než 6 000 subjektů. Ty se pak budou rozdělovat na poskytovatele v režimu vyšších povinností a poskytovatele v režimu nižších povinností. Toto rozdělení ovlivní např. i povinnost hlášení kybernetických incidentů. Návrh zákona také obsahuje mechanismus prověřování bezpečnosti dodavatelského řetězce. Návrh nového zákona o kybernetické bezpečnosti Národní úřad pro kybernetickou a informační bezpečnost odeslal v prosinci na Legislativní radu vlády. Odvedená práce na tomto zákonu je bezesporu pozitivním krokem pro Českou republiku, protože jak řekl sám ředitel NÚKIB Lukáš Kintr: „Bez kvalitní a moderní právní úpravy v oblasti kybernetické bezpečnosti se Česká republika v budoucnu neobejde. Práce spojená s přípravou nového zákona byla náročná. Vytvořili jsme však normu, která státu a občanům zajistí vyšší ochranu.“

A co u nás v Česku?

NÚKIB zaznamenal za rok 2023 celkem 262 incidentů. V roce 2022 jich zaznamenal pouze 146. Dva z těch loňských incidentů navíc NÚKIB klasifikoval jako velmi významné. Jeden z nich se týkal významné strategické státní instituce a druhý neregulovaného subjektu z obranného sektoru. Rekordní číslo mají ale na svědomí zejména DDoS útoky, které probíhaly z velké části jako odveta podpory České republiky pro Ukrajinu a kromě dočasné nedostupnosti určitých služeb nezpůsobily vážnější následky.

Závěrem.

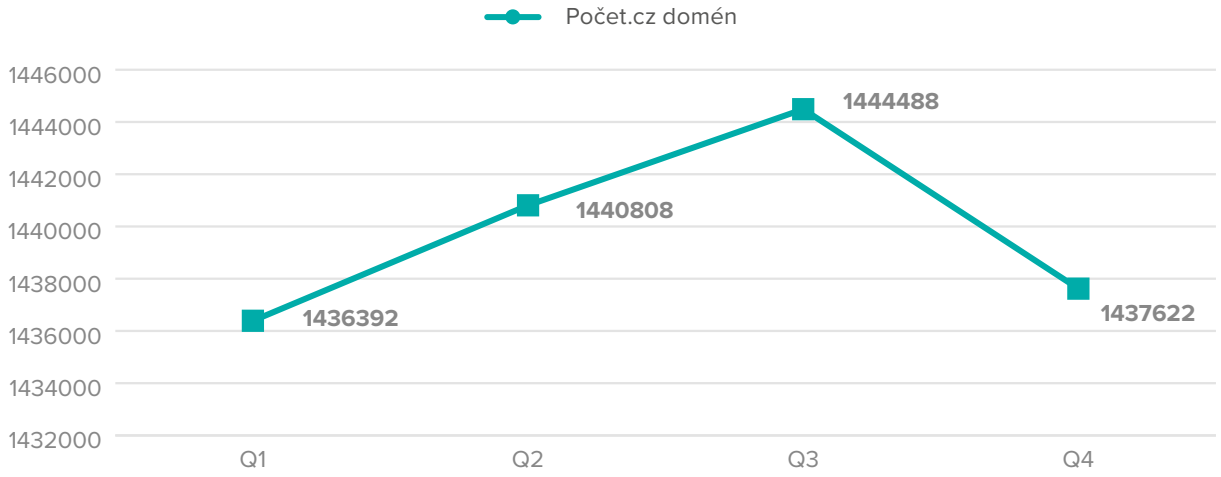
Pokud bych měl popsat kyberzločince v roce 2023, použil bych jediné slovo: odolnost. Rok 2024 bezpochyby přinese další překvapení, nové skupiny, rebrandy a spoustu nových zranitelností. Zdokonalování řemesla ransomwaru dominovalo roku 2023 a vše nasvědčuje tomu, že tento příběh bude pokračovat i v roce 2024. Ačkoli akce orgánů činných v trestním řízení dokázaly často úspěšně házet klacky pod nohy velkým skupinám i jedincům, útočníky to nezastavilo. Zůstává tak na samotných organizacích, aby posílily zabezpečení svých vlastních sítí a zaměřily se na odolnost vlastní.

Stav adopce bezpečnostních mechanismů SPF, DKIM a DMARC v ČR

Milan Habrcetl

Bezpečnostní mechanismy Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) a Domain-based Message Authentication, Reporting and Conformance (DMARC) umožňují, při korektní konfiguraci, organizacím zamezit podvrhování jejich domén při posílání e-mailových zpráv. Útočníci tedy nemohou zneužít doménu organizace, která má správně nastavené bezpečnostní mechanismy SPF, DKIM a DMARC, a tím lze zabránit phishingovým útokům, které by zneužívaly legitimní doménu a které by si tímto způsobem jednoduše zvýšily důvěryhodnost e-mailových zpráv u uživatelů. Data, která byla využívána v rámci analýzy, byla sesbírána na konci každého čtvrtletí roku 2023, kromě posledního čtvrtletí, u kterého byl zaznamenán problém se sběrem dat a data tak byla převzata z poloviny ledna roku 2024 (17. 1. 2024). Na základě takto sesbíraných informací bylo zjištěno, že se počet .cz domén v průběhu roku téměř nemění. Na začátku roku probíhá zřejmě mazání domén, kdy počet domén klesl o necelých 7 tisíc oproti třetímu čtvrtletí roku 2023.

POČET.CZ DOMÉN V PRŮBĚHU ROKU 2023



Mechanismus DKIM nelze ověřovat bez interakce a spolupráce s vlastníky domén a z toho důvodu není tento mechanismus zahrnut do analýzy níže. Avšak pro fungování mechanismu DMARC je nutné mít nastaveny mechanismy.

Sender Policy Framework

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

1. *„-all“*, což se označuje jako politika *„fail“*, podle které se e-mailová zpráva zahodí
2. *„~all“*, což se označuje jako politika *„softfail“*, podle které se e-mailová zpráva vloží do karantény, nebo se označí, ale přepošle uživateli

3. *„?all“*, což se označuje jako politika *„neutral“*, podle které se s e-mailovou zprávou nestane nic
4. *„+all“*, což se označuje jako politika *„pass“*, podle které mohou odesílat všechny servery zprávy s doménou, u které je nastaven tento SPF záznam

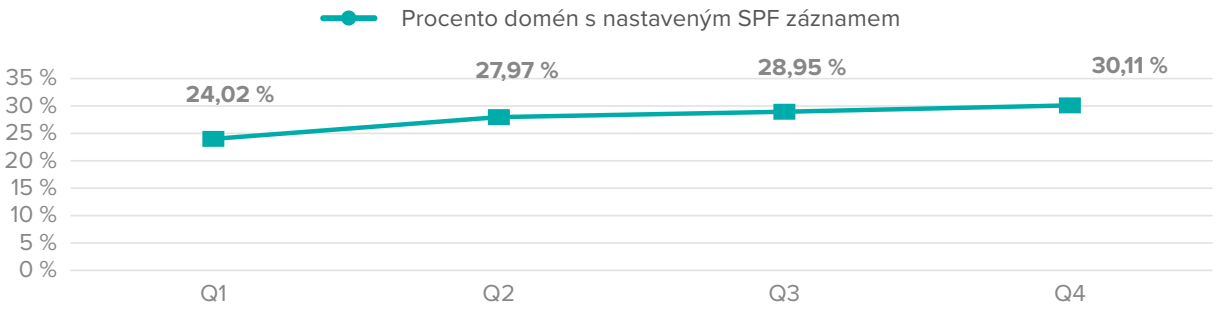
Příjemce si samozřejmě může upravit, co přesně se s e-mailovými zprávami na e-mailové bráně provede, například jestli se vloží do karantény i zprávy, které neprojdou SPF kontrolou s „fail“ politikou apod.

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

Český internet a SPF záznamy

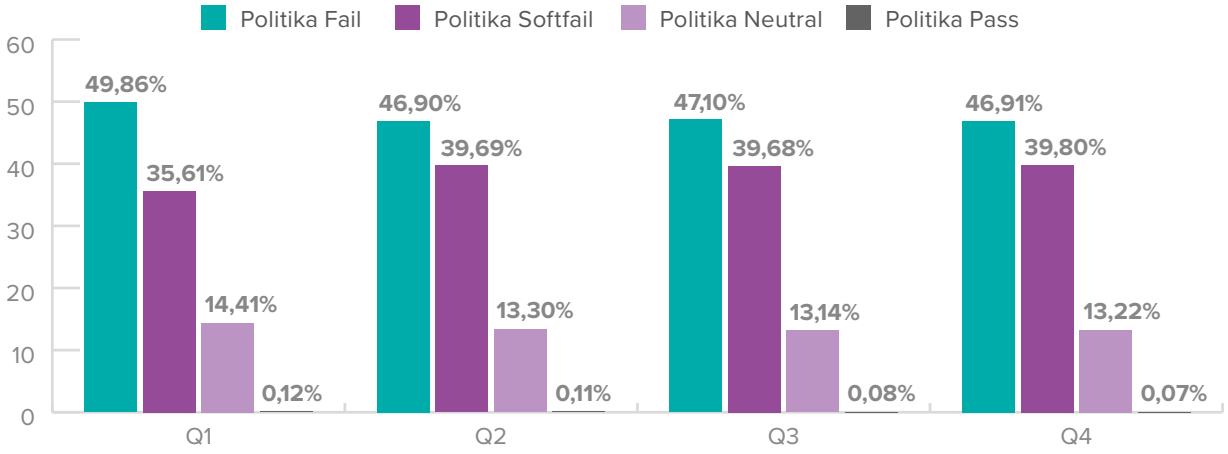
Adopce SPF mechanismu na doménách České republiky se průběžně během roku zvyšovala a na začátku roku 2024 byl mechanismus SPF adoptován na téměř jedné třetině domén, přesněji na 30,11 procentech .cz domén, což je o více než 120 tisíc domén více, než tomu bylo na konci minulého roku.

PROCENTO DOMÉN S NASTAVENÝM SPF ZÁZNAMEM



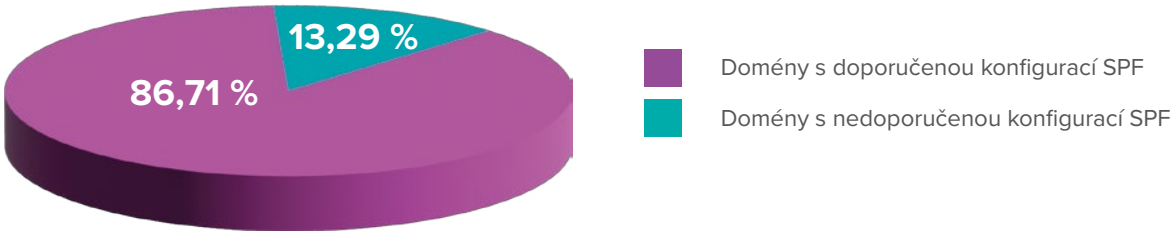
Domény s nastaveným SPF záznamem pak byly rozděleny do čtyř skupin, dle pravidel pro ostatní, v SPF záznamu nespecifikované servery, tato pravidla jsou popsána výše. Většina domén, která měla nastaven nějaký SPF záznam, používala první dva popsané typy tohoto pravidla. Zbytek těchto domén měl většinou nastaven třetí typ tohoto pravidla a několik málo domén používalo silně nedoporučovaný typ pravidla, kde na začátku roku 2024 takto bylo nastaveno 0,07 procent českých domén. Na následujícím grafu je znázorněn procentuální poměr těchto metrik.

POMĚR POUŽITÝCH SPF POLITIK



Většina domén tedy používá doporučenou politiku fail nebo softfail. Na následujícím grafu je znázorněn poměr použití doporučené konfigurace SPF pravidel oproti použití nedoporučené konfigurace v konečném stavu roku 2023.

POMĚR POUŽITÍ DOPORUČENÉ A NEDOPORUČENÉ KONFIGURACE SPF ZÁZNAMU NA KONCI ROKU 2023

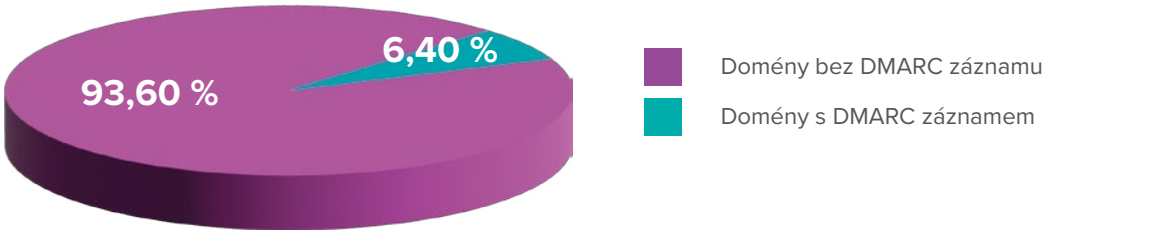


Český internet a adopce DMARC

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

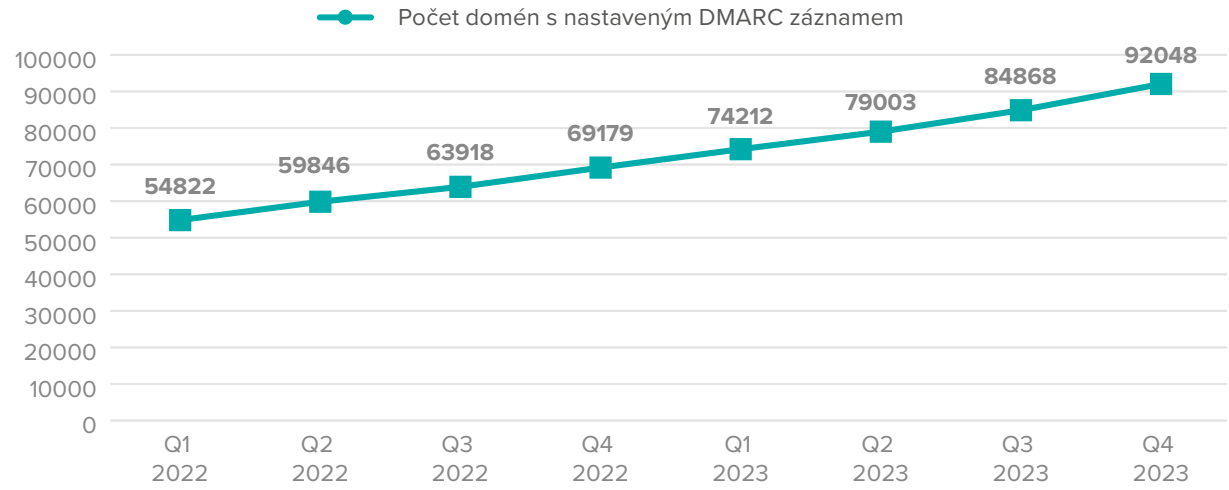
Z téměř jednoho a půl milionu (1437622).cz domén byl na začátku roku 2024 nastavený DMARC záznam pouze u necelých 100 tisíc (6,40 %) z nich.

POMĚR ČESKÝCH DOMÉN S DMARC ZÁZNAMEM A BEZ NĚJ NA ZAČÁTKU ROKU 2024



Zvyšování adpoce DMARC záznamů je však možné pozorovat v průběhu posledních několika let. V následujícím grafu je možné vidět celkem markantní nárůst počtu domén s nastaveným DMARC záznamem od roku 2022 na téměř dvojnásobek.

POČET DOMÉN S NASTAVENÝM DMARC ZÁZNAMEM



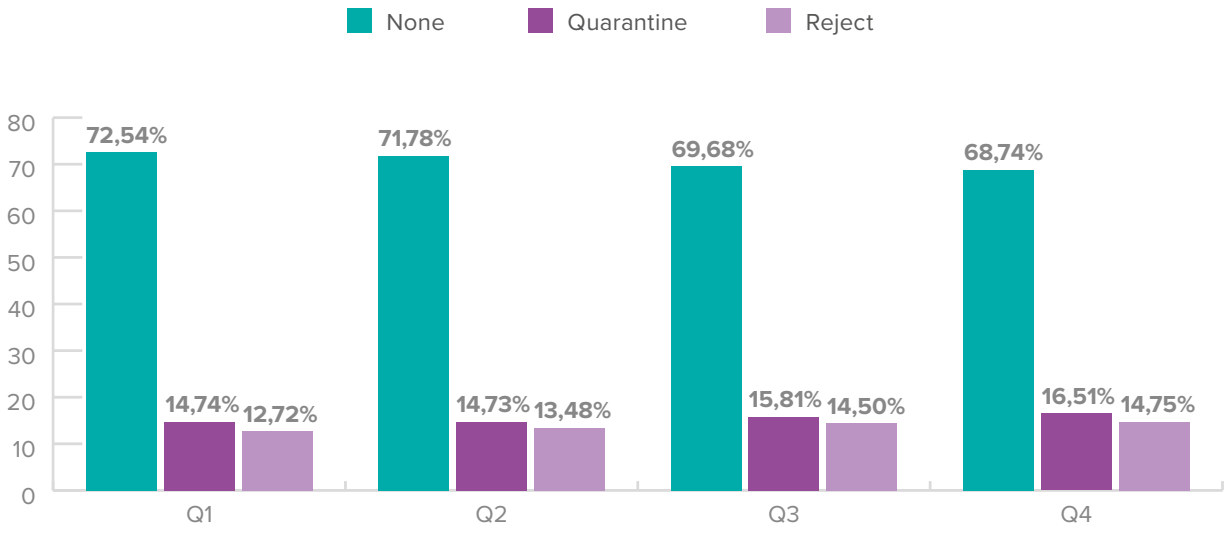
V rámci statistických dat získaných z českých domén dále byly analyzovány dva parametry v DMARC záznamech, které jsou pro správné fungování DMARC mechanismu nutné.

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

1. *None* – tato hodnota určuje, že se nelegitimní e-mailová zpráva nebude blokovat. Tuto hodnotu je doporučeno využívat po dobu několika měsíců po prvotním nastavení mechanismu DMARC a po vyhodnocení doručených DMARC reportů přepnout tuto hodnotu na jednu z následujících.
2. *Quarantine* – Tato hodnota způsobí to, že nelegitimní e-mailová zpráva bude označena jako spam a vložena do karantény, případně do adresáře se spamem.
3. *Reject* – Tato hodnota způsobí nedoručení nelegitimní e-mailové zprávy uživateli.

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

V následujícím grafu je vyobrazen poměr využití těchto parametrů v jednotlivých kvartálech roku 2023:



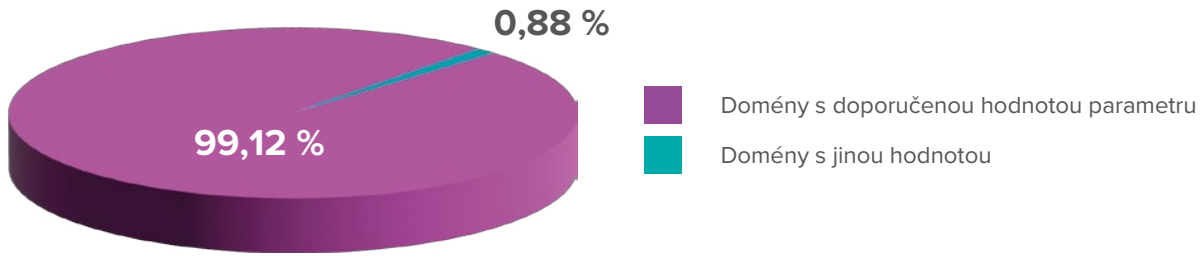
Druhým ze sledovaných parametrů je parametr *pct*, který určuje na kolik procent e-mailových zpráv, které neprošly kontrolou mechanismy SPF a DKIM má být aplikována politika z parametru popsaného výše. Doporučená hodnota tohoto parametru je 100, což znamená stoprocentní blokace nelegitimních e-mailových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

V naší analýze jsme rozdělili hodnoty tohoto parametru na dvě skupiny:

1. Hodnota nenastavena nebo nastavena na 100
2. Hodnota nastavena v rozmezí 0-99

V průběhu roku se počet českých domén, které mají definovaný tento parametr s doporučenou hodnotou, pohyboval kolem 99 procent z domén, které DMARC záznam mají nastaven. Toto lze vypozorovat v následujícím grafu, který znázorňuje stav na začátku roku 2024:

POMĚR ČESKÝCH DOMÉN S DMARC ZÁZNAMEM S DOPORUČENOU HODNOTOU PARAMETRU PCT NA KONCI ROKU 2024



Závěr

Adpoce SPF mechanismu na českých doménách (.cz) se stále zvyšuje (za rok 2023 se zvýšil počet serverů s nastaveným SPF záznamem o 6 procent). Velký nárůst je také možné vypozorovat, pokud se podíváme na stav adopce SPF mechanismu, který od začátku roku 2022 narostl z 268 tisíc na 432 tisíc domén s nastaveným SPF záznamem, tedy o více než 164 tisíc.

Adopce mechanismu DMARC má procentuálně téměř stejný nárůst, jako je v případě mechanismu SPF, avšak co se týče počtů se jedná za stejné období (od začátku roku 2022 do začátku roku 2024) o nárůst pouze o 37 tisíc domén (přibližně o 68 % od roku 2022).

Jako jednu z hlavních příčin tohoto nárůstu, lze považovat **vydání ochranného opatření (https://www.nukib.cz/cs/infoservis/aktuality/1758-spravci-klicovych-systemu-musi-zabezpecit-sve-e-mailove-schranky/)** Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB) dne 11. října 2021, které pojednává o povinnostech zabezpečení e-mailové komunikace a mimo jiné popisuje povinnost a náležitosti implementace SPF, DKIM a DMARC mechanismů.

SASE: Konec komplikované kyberbezpečnosti?

Jiří Herzig

Znáte pojem SASE? Možná ano, možná ne. Ale nebojte se, v tomto článku si ho společně vysvětlíme. Dnes se budeme zabývat otázkami, které pravděpodobně trápí mnoho z vás. Jak efektivně ochránit vaše uživatele při práci na dálku, aniž byste jim zároveň komplikovali život a tím podporovali hledání alternativních, méně bezpečných řešení? Možná se potýkáte s výzvami moderní kyberbezpečnosti v cloudovém prostředí a hledáte inspiraci, jak s nimi efektivně zacházet. Pokud ano, jste na správném místě. V následujícím článku se zaměříme na praktické řešení těchto problémů a na to, jak vám může koncept SASE pomoci v boji proti kybernetickým hrozbám. Získáte nové informace a nápady, které vám mohou pomoci zlepšit kyberbezpečnost vaší společnosti.

Secure Access Service Edge (SASE) je koncept, který se i v našem kraji začíná stále častěji objevovat. Není divu, jelikož tento koncept je pojmenovaný již od roku 2019, kdy jej Gartner, americká společnost zabývající se výzkumem a poradenstvím v oblasti IS/ICT technologií, popsal takto:

„Secure Access Service Edge (SASE) poskytuje konvergované schopnosti sítě a bezpečnosti jako služby, včetně SD-WAN, SWG, CASB, NGFW a přístupu k síti na principu nulové důvěry (ZTNA). SASE podporuje užití pro pobočky, vzdálené pracovníky a bezpečný přístup on-premise. SASE je primárně poskytováno jako služba a umožňuje přístup založený na nulové důvěře na základě identity zařízení nebo entity, kombinovaný s aktuálním kontextem a politikami bezpečnosti a dodržování předpisů.“ - *Gartner*

Tato definice nám poskytuje jasný obraz toho, co SASE představuje a jaké jsou jeho klíčové prvky. Ale co to znamená pro naše uživatele a pro nás, administrátory bezpečnostních řešení? Můj pohled na tuto problematiku se dozvíte dále v článku.

SASE lze podle svého zaměření rozdělit na dvě hlavní části: transportní a bezpečnostní. Transportní část je řízena především technologií SD-WAN, zatímco v bezpečnostní části hrají klíčovou roli komponenty jako Secure Web Gateway (SWG), cloudový firewall jako služba (FWaaS), Cloud Access Security Broker (CASB) a princip Zero Trust Network Access (ZTNA). V tomto článku se budeme věnovat pouze bezpečnostní části, která má jako samostatný koncept název Security Service Edge (SSE).

Cesta k bezpečnější budoucnosti

Implementace SASE může vyžadovat významné investice do přestavby infrastruktury a bezpečnostních systémů, což může být nákladné. Avšak díky flexibilitě SSE lze proces zavádění rozložit do několika fází. Je dokonce možné začít pouze s implementací bezpečnostní části a transportní část, tedy SD-WAN odložit na později. To umožňuje začít s menšími, specifickými skupinami uživatelů, kteří pracují mimo bezpečné prostředí firmy, a postupně rozšiřovat pokrytí. Můžeme také využít tunelování mezi lokalitami a bezpečnostním cloudem pro bezpečné připojení menších poboček, čímž dosáhneme vyšší úrovně bezpečnosti nejen pro internetovou komunikaci.

Výhodou je možnost využití cloudových služeb a existující infrastruktury pro postupné začleňování konceptu SSE. Klíčovým benefitem je modulární povaha SSE, díky které můžeme nejprve implementovat nejdůležitější komponenty a v průběhu času přidávat další služby dle aktuálních potřeb.

Zavádění SASE ale není jen o implementaci nových technologií, je především o posunu v našem myšlení o bezpečnosti a přístupu k síti. Jak jsme si již řekli, Security Service Edge (SSE) představuje bezpečnostní složku SASE a klade důraz na ochranu uživatelských dat, aplikací a identit v jakémkoliv prostředí, od kanceláře po cloud. Proč je důležité se nad tímto novým konceptem zamýšlet? V dnešní

době digitalizace, kdy se hranice tradiční kanceláře rozplývají a aplikace i data migrují do cloudu, se tradiční bezpečnostní modely stávají neefektivními. SSE nabízí řešení, které se přizpůsobuje dynamickému pracovnímu prostředí a poskytuje konzistentní ochranu bez ohledu na to, odkud uživatelé přistupují k podnikovým zdrojům.

SASE a SSE nám usnadňují práci tím, že:

Zjednodušují přístup

Uživatelé potřebují bezpečný přístup k aplikacím a datům, ať jsou kdekoli. SASE a SSE eliminují složité VPN nastavení a poskytují jednodušší, a přitom bezpečnější metody přístupu.

Zvyšují bezpečnost

Integrací Zero Trust Network Access (ZTNA) a dalších pokročilých bezpečnostních technologií SSE se zajišťuje, že pouze ověření uživatelé a zařízení mohou přistupovat k citlivým podnikovým zdrojům, což minimalizuje riziko úniku dat.

Podporují flexibilitu a škálovatelnost

Cloudové služby umožňují organizacím snadno škálovat bezpečnostní služby podle aktuálních potřeb, což je ideální pro podniky, které se rychle rozvíjejí, nebo procházejí digitální transformací.

Uživatel vs. administrátor

Vezměme si příklad firmy, která využívá datové centrum pro provoz svých privátních aplikací. Některé z těchto aplikací mohou být starší, vytvořené před lety a nejsou vybaveny moderními metodami přihlašování. Na druhé straně, firma využívá i moderní aplikace, podporující současné způsoby autentizace a aplikace hostované v public cloudovém prostředí. Představme si uživatele, který pracuje na dálku - ať už z domova, nebo hotelového pokoje. Když potřebuje přistoupit ke cloudové aplikaci, jednoduše spustí aplikaci a na svém mobilním telefonu potvrdí přihlášení prostřednictvím MFA push notifikace. Ale když se pokusí o přístup k aplikaci v privátním datovém centru, narazí na problém - aplikace nefunguje. Uvažuje o tom, zda by měl kontaktovat IT oddělení, protože přístup k první aplikaci fungoval bez problémů. Po nějaké době si ale uvědomí, že pro přístup k této konkrétní aplikaci potřebuje aktivovat VPN.

SASE má za cíl právě tyto situace ulehčit tím, že odstraňuje nutnost uživatelů přemýšlet, jaký typ připojení by měli použít pro přístup k různým aplikacím. Navíc, s využitím přístupu Zero Trust Network Access (ZTNA), je možné zvýšit bezpečnost tím, že uživatele ověříme již při prvním otevření notebooku nebo spuštění aplikace. To umožňuje aplikovat přísnější pravidla pro ověřování a přístup, zejména pokud se uživatel připojuje z neobvyklé lokace. Tímto způsobem SASE nejen zjednodušuje a zefektivňuje pracovní procesy vzdálených pracovníků, ale také posiluje celkové bezpečnostní postavení organizace tím, že zavádí dynamické a kontextuální zabezpečení, které se přizpůsobuje aktuálním podmínkám a potřebám uživatele.

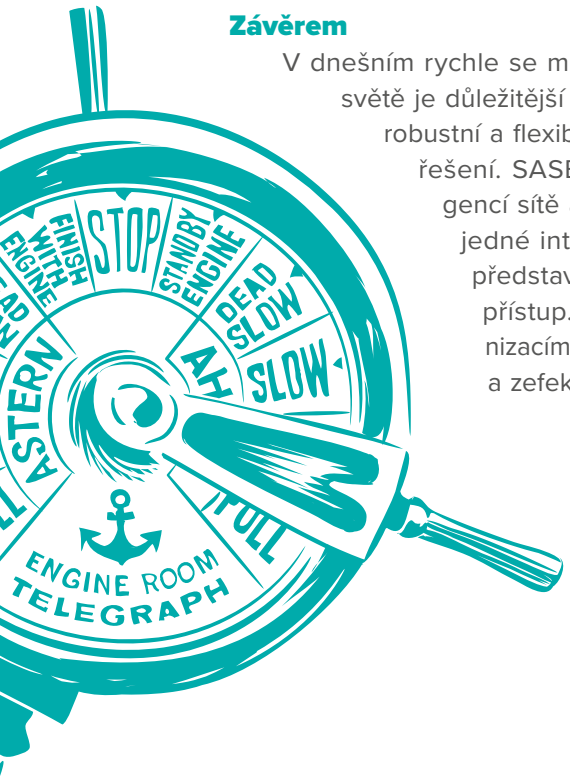
Teď si představme administrátora, který v této společnosti řeší přístupy k aplikacím a jejich zabezpečení. S příchodem SASE se mu může práce značně usnadnit a zefektivnit. Díky centralizovanému dashboardu SASE, může nyní administrátor spravovat všechny bezpečnostní politiky a přístupy z jednoho místa, automatizovat rutinní úkoly a snadno aplikovat aktualizace bezpečnostních pravidel napříč celou společností. Zatímco dříve musel balancovat mezi několika rozdílnými nástroji pro zabezpečení a síťové operace, nyní má vše pod kontrolou v jednom rozhraní. Toto zjednodušení nejen snižuje riziko chyb, ale také umožňuje rychlejší reakci na bezpečnostní incidenty a poskytuje lepší přehled o síťovém provozu a aktivitách uživatelů. SASE tedy pro našeho administrátora představuje revoluční nástroj, který mění způsob, jakým lze bezpečnostní výzvy řešit – efektivně, flexibilně a s větší jistotou.

Náš administrátor nyní disponuje předem definovanými skupinami uživatelů, aplikacemi, které každá skupina může, nebo naopak nesmí využívat, a zná umístění těchto aplikací, ať už jsou hostovány v privátním, nebo veřejném cloudu. K dispozici má také seznam internetových domén nebo konkrétních webových stránek a aplikací. Pro přidělení přístupu k aplikacím stačí, aby administrátor vybral skupinu uživatelů a přiřadil jim potřebné aplikace, přičemž může jednoduše omezit, nebo

povolit přístup k nim. Při nástupu, nebo odchodu zaměstnance je změna ve skupině uživatelů otázkou několika kliknutí. Nová aplikace nebo změna jejího umístění vyžaduje pouze aktualizaci v dashboardu. V případě specifických požadavků může administrátor rychle nastavit výjimky pro jednotlivé uživatele. Je také možné určit preferovaný způsob připojení k aplikacím, ať už skrze VPN, nebo ZTNA. Díky jednotnému klientu na koncovém zařízení se všechna nastavení automaticky promítají do zařízení uživatele, což eliminuje potřebu instalace dodatečných aplikací a zjednodušuje celý proces.

Závěrem

V dnešním rychle se měnícím digitálním světě je důležitější než kdy jindy mít robustní a flexibilní bezpečnostní řešení. SASE, s jeho konvergencí sítě a bezpečnosti do jedné integrované služby, představuje právě takový přístup. Umožňuje organizacím nejen zjednodušit a zefektivnit správu bezpečnosti a přístupů, ale také zvýšit ochranu proti kybernetickým hrozbám v dnešním proměnlivém pracovním prostředí. S postupnou implementací a modulární strukturou je SASE přístupný pro všechny organizace, bez ohledu na jejich velikost nebo odvětví. Jako živoucí, dýchající framework, který se přizpůsobuje potřebám a výzvám současnosti, SASE není jen dalším buzzwordem, ale klíčem k budoucnosti kybernetické bezpečnosti. Ať už o SASE přemýšlíte, či je to pro Vás nový pojem, vězte, že Alef je připraven pomoci. Na závěr mi nezbývá než dodat: Buďte v bezpečí a „Trust the Strong“.



Co nám prozradí webové hlavičky českého internetu?

Michal Frýba

HTTP hlavičky jsou nedílnou součástí webové komunikace a umožňují klientovi a serveru spolu s HTTP požadavkem nebo odpovědí předávat další dodatečné informace. Zajišťují kromě jiného například autentizaci a udržování relace mezi klientem a serverem, vytváření cookies souborů nebo specifikaci použitých technologií, obsahu a kódování. Speciální skupinou jsou takzvané bezpečnostní HTTP hlavičky, které jsou odesílány spolu s HTTP odpověďmi ze serveru na klienta a které poskytují dodatečná bezpečnostní pravidla a informace o zabezpečení a chování aplikace. Tyto hlavičky jsou navrženy tak, aby chránily webovou aplikaci před různými bezpečnostními hrozbami a útoky. Často se ale stává, že jsou nesprávně nastaveny, a tak nemohou plnit svůj účel nebo dokonce poskytnout potenciálnímu útočníkovi užitečné informace pro případný útok.

V tomto článku se podíváme na nastavení vybraných HTTP hlaviček na webech českých domén. Především se analýza zaměří na správnost jejich nastavení a zda neprozrazují více informací, než by měly. Za data poskytnutá pro analýzu patří velký dík kolegům z CZ.NIC.

Krátce o HTTP hlavičkách

Při návštěvě webové stránky na internetu pomocí webového prohlížeče Vám server společně s požadovaným HTML obsahem vrátí v odpovědi také sadu HTTP hlaviček. Ty následně využije prohlížeč například k úpravám svého chování na stránkách a také mohou chránit uživatele před snadno odstranitelnými zranitelnostmi. Konkrétně mohou například zabraňovat vkládání škodlivých skriptů, clickjackingu, vynucovat komunikaci přes zabezpečený protokol HTTPS a informovat správce o porušení definovaných pravidel. Jedná se tedy o poměrně užitečný, ale často také přehlížený nástroj pro zvýšení bezpečnosti. Častým problémem u starších hlaviček také bývá nestandardizovaná implementace napříč hlavními moderními prohlížeči.

Právě na hlavičku vrácené webovými servery se v tomto článku blíže podíváme. Konkrétně se bude jednat o:

- Strict-Transport-Security HTTP Response Header
- X-XSS-Protection HTTP Response Header
- X-Frame-Options HTTP Response Header
- Server HTTP Response Header
- X-AspNet-Version HTTP Response Header
- X-Powered-By HTTP Response Header

Některé ze zmíněných hlaviček jsou již v „důchodu“, stále nám mohou ale poskytnout užitečný obrázek o nastavení webových serverů na českém internetu. Funkci zastaralých hlaviček na moderních webech přebraly novější standardy, jako je například Content-Security-Policy (CSP). Vzhledem ke komplexnosti její implementace a tomu, že se může nacházet i přímo v HTML kódu by ale byla analýza této konkrétní vrstvy zabezpečení poměrně složitá. Poslední tři zmíněné hlavičky zase často uživateli sdělují zbytečně rozsáhlé informace o back-endových technologiích a operačním systému webového serveru.

Analýza – co uživatel nevidí, ale útočníkovi neunikne

V rámci analýzy byly zkoumány HTTP odpovědi celkem 1437622 webů na doménách registrovaných pod doménou nejvyššího řádu.cz. Jak již bylo zmíněno, cílem analýzy je vyhodnotit u vybraných HTTP hlaviček jejich správnost, přítomnost, chyby v zápisu a odhalit případné vyzrazení potenciálně citlivých informací o webových serverech. Ověření správnosti implementace webových hlaviček je důležité nejen pro administrátory webových serverů, ale jedná se také o jednu z prvních aktivit u penetračních testů webových aplikací. V rámci penetračních testů se analytici snaží simulovat postup reálného útočníka, a právě správná implementace HTTP hlaviček je jedna z věcí, která může omezit množinu škodlivých akcí, které může útočník využít při útocích na webový server nebo uživatele webové aplikace.

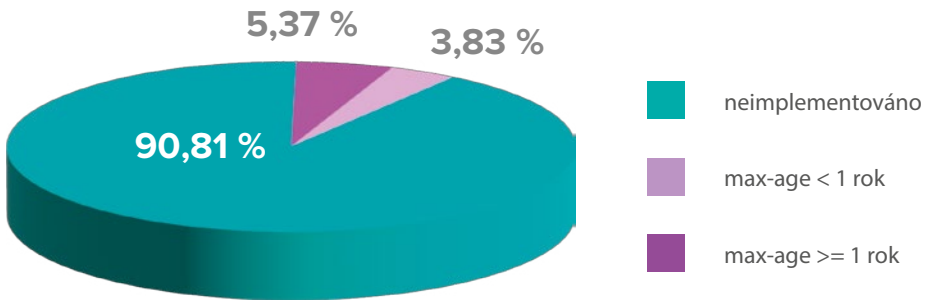
Strict-Transport-Security HTTP Response Header

HTTP Strict Transport Security (zkráceně HSTS) je mechanismus, který pomáhá chránit webové stránky před útoky zahrnující snížení úrovně šifrovacího protokolu a odcizení cookies souborů. Webový server, který správně nastavenou hlavičku vrátí, nařizuje webovému prohlížeči, že ke komunikaci s webem musí využívat pouze zabezpečené připojení pomocí HTTPS. Veškerá případná připojení přes HTTP by pak měla být povýšena na HTTPS bez nutnosti provádět přesměrování, kde je prvotní HTTP požadavek náchylný k man-in-the-middle útokům, a tedy čtení a změně dat mezi klientem a serverem (útoky typu SSL-Stripping, Session Hijacking a další).

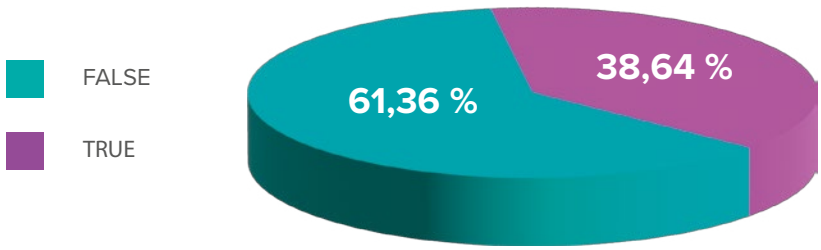
Tato hlavička umožňuje tři základní nastavení – max-age, includeSubDomains a preload. Direktiva max-age udává dobu v sekundách, po kterou si má prohlížeč pamatovat, že na web lze přistupovat pouze pomocí protokolu HTTPS. Obecně doporučovaná hodnota by měla být alespoň 31536000 sekund (1 rok). Druhé zmíněné nastavení includeSubDomains rozšiřuje nastavení i na všechny subdomény webu a není povinné. Poslední direktiva preload dává prohlížeči pokyn, aby vždy přistupoval k webu pomocí protokolu HTTPS a zahrnul ho do svého Strict-Transport-Security preload seznamu.

Z dostupných dat vyplývá, že HTTP Strict Transport Security implementuje 9,2 % analyzovaných webů a pouze 5,37 % má direktivu max-age nastavenou alespoň na doporučovanou hodnotu 1 rok. Z těchto webů 38,64 % rozšiřuje toto nastavení také na všechny své subdomény a 31,81 % využívá možnost zařazení do HTTPS preload seznamu prohlížeče

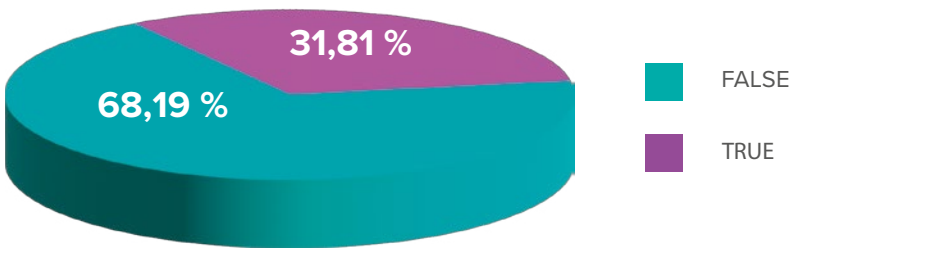
HSTS max-age



HSTS includeSubDomains



HSTS preload



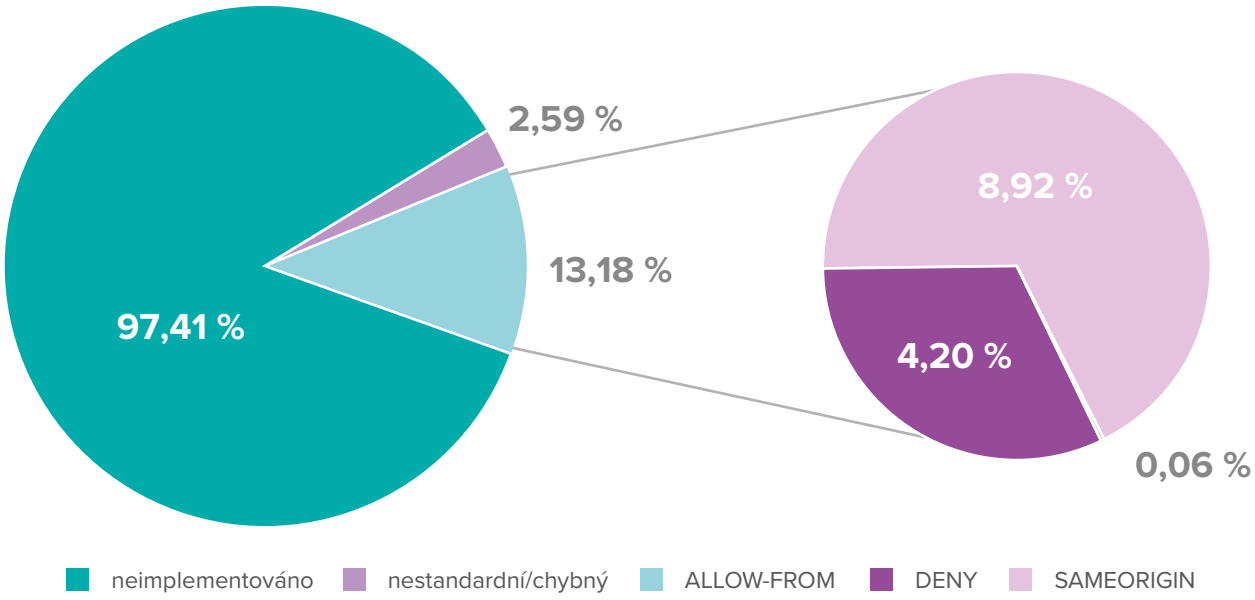
X-Frame-Options HTTP Response Header

V rámci webů je často potřeba na stránky vložit obsah třetích stran. Tuto funkcionalitu můžete znát například ze situací, kdy na nějakém webu narazíte na prvek s Google mapami, YouTube videem nebo reklamními banery. Je to ale možné pouze proto, že vlastníci vkládaného obsahu tuto akci umožňují. Úkolem bezpečnostní hlavičky X-Frame-Options je sdělit prohlížeči, zda je možné stránku na jiných webech vykreslovat, například v HTML prvcích <frame>, <iframe> nebo <object>. Weby ji mohou využít k tomu, aby se vyhnuly útokům typu clickjacking, při kterém je uživatel například nalákán ke kliknutí na akční obsah na skryté legitimní webové stránce kliknutím na jiný obsah na nevinně vypadající podvodné stránce, která působí jako „návnada".

Nastavení X-Frame-Options je opět poměrně jednoduché, jelikož povoluje pouze 3 možnosti – DENY, SAMEORIGIN a ALLOW-FROM. Použitím hodnoty DENY se zakazuje jakékoliv vkládání do elementů, což zabraňuje neoprávněnému zobrazení obsahu na jiných webových stránkách. Možnost SAMEORIGIN povoluje vkládání pouze na stejnou doménu, což snižuje riziko načítání stránky kamkoliv jinam. Poslední možností je ALLOW-FROM doplněná o doménu, která umožňuje vložení stránky pouze na určenou doménu. Je dobré podotknout, že hlavičku X-Frame-Options ruší modernější hlavička Content-Security-Policy, pokud obsahuje direktivu frame-ancestors, která plní podobnou funkci. Využití CSP je aktuálně preferované a doporučované řešení, především proto, že umožňuje povolit více domén a že možnost ALLOW-FROM je zastaralá a v moderních prohlížečích již nefunguje.

Na základě analyzovaných dat správně implementuje hlavičku X-Frame-Options pouze 13,18 % z celkového počtu zkoumaných webů. Z těchto webů většina používá direktivu SAMEORIGIN (67,69 %, což odpovídá 8,92 % celkového počtu), přibližně třetina direktivu DENY (31,83 %, což odpovídá 4,2 % celkového počtu) a pouze půl procenta má validně definovanou možnost ALLOW-FROM (0,06 % z celkového počtu). Dále pak 2,59 % z celkového počtu serverů mělo v hlavičkách syntaktické chyby nebo neodpovídaly specifikaci a 97,41 % webů tuto hlavičku vůbec nevrací. Velký počet webů, jejichž odpovědi hlavičku neobsahují, nemusí ale znamenat špatnou zprávu. Můžeme předpokládat, že část z nich využívá alternativu v podobě CSP.

X-Frame-Options



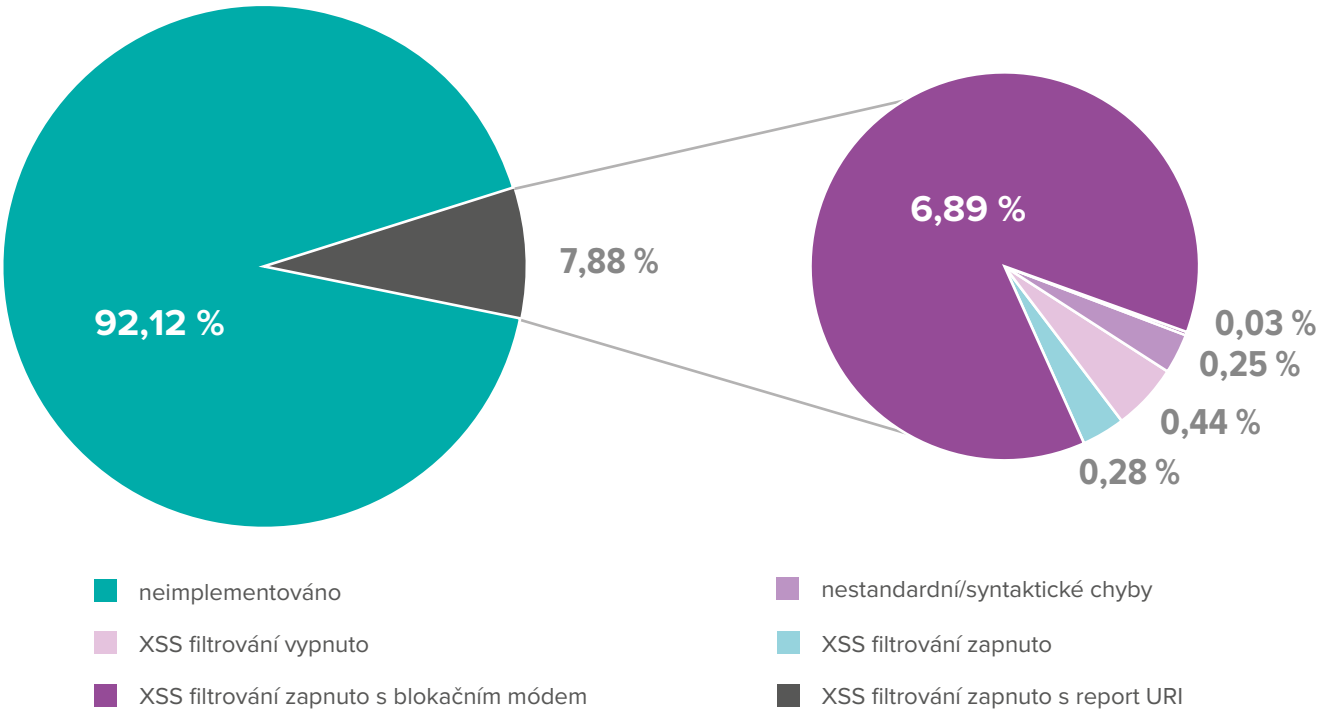
X-XSS-Protection HTTP Response Header

Další z bezpečnostních hlaviček, na kterou se podíváme, je X-XSS-Protection. Tato hlavička byla kdysi doporučeným standardem pro prevenci cross-site scripting útoků (XSS). Postupem času však zastarala a většina populárních prohlížečů ji již nepodporuje. Místo toho se nyní doporučuje používat k ochraně před XSS útoky Content Security Policy (CSP), která zakazuje používání inline JavaScriptu ("unsafe-inline").

Značná část webů tuto hlavičku ale stále podporuje, a to pravděpodobně z historických důvodů nebo pro ochranu uživatelů starších prohlížečů, které nepodporují CSP. V některých případech ale filtrování vynucované hlavičkou může do jinak bezpečných webových stránek zavléct právě XSS zranitelnosti. Hlavička X-XSS-Protection nabízí několik možností nastavení pro ochranu před zmíněnými XSS útoky. Ty zahrnují možnost vypnutí XSS filtrů, zapnutí filtrů s automatickou sanitací stránky, aktivaci režimu blokování vykreslování stránky při detekci útoku a možnost reportování porušení pravidel na zadanou adresu, která je dostupná pouze v prohlížeči Chromium.

V rámci analýzy se objevil podobný trend jako v předchozím případě, valná většina 92,12 % serverů tuto hlavičku neimplementuje a vrací ji pouze 7,88 %, což může opět souviset s vhodnější alternativou ve formě CSP. Ze serverů, které hlavičku vrací má filtrování 5,61 % vypnuté, což je doporučované, pokud web správně vynucuje CSP. Dále 3,11 % vrací hlavičku chybnou nebo v nestandardním formátu a na straně prohlížeče by pak byla ignorována anebo vyhodnocena jinak, než bylo pravděpodobně zamýšleno. Většina zbylých serverů (87,41 %) pak využívá filtraci v blokačním módu (X-XSS-Protection: 1; mode=block), 3,54 % potenciálně škodlivý obsah pouze sanitizuje (X-XSS-Protection: 1) a pouze 0,33 % využívá možnost pro nahlášení nebo logování přes definovanou URI.

X-XSS-Protection



Server HTTP Response Header

Následující zbylé hlavičky se již vyloženě neřadí mezi bezpečnostní, ale při neideálním nastavení mohou potenciálnímu útočníkovi poskytnout užitečné informace. Jednou z těchto hlaviček je Server. Hlavička popisuje software použitý serverem pro vlastní běh webu (Apache, NGINX a další) a informace o back-endových technologiích (PHP, OpenSSL, Python a další). Příliš detailní informace mohou útočníkům usnadnit zneužití známých bezpečnostních děr. Často se stává, že server v této hlavičce vyzradí nejen verzi vlastního webového serveru ale i typ OS, který na něm běží. Ideální je webový server nastavit tak, aby vracel pouze obecné informace bez detailů o verzi nebo OS.

Administrátoři, kteří chtějí útočníkům práci ještě o něco ztížit mohou na serveru zahrnutí hlavičky v odpovědi vypnout nebo ji dokonce podvrhnout.

Ne úplně ideálně nastavená hlavička pak může vypadat například následovně:

Server:
Apache/1. 3. 33 (Debian GNU/Linux) mod_python/2. 7. 10 Python/2. 3. 4 PHP/4. 3. 10-16 mod_ssl/2. 8. 22 OpenSSL/0. 9. 7e mod_perl/1.29

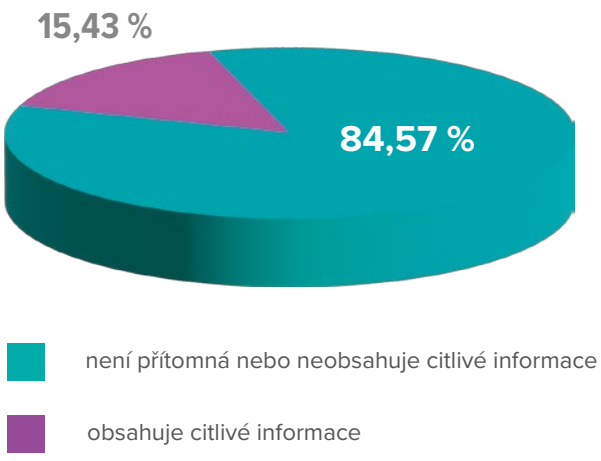
Útočník pouze navštívením webu zjistí, že verze softwaru na serveru jsou poměrně zastaralé a trpí potenciálními zranitelnosti, jako je vzdálené spuštění kódu, útoky typu odepření služby a další známé chyby zabezpečení.

Ideálně by hlavička mohla vypadat následovně:
Server: Apache

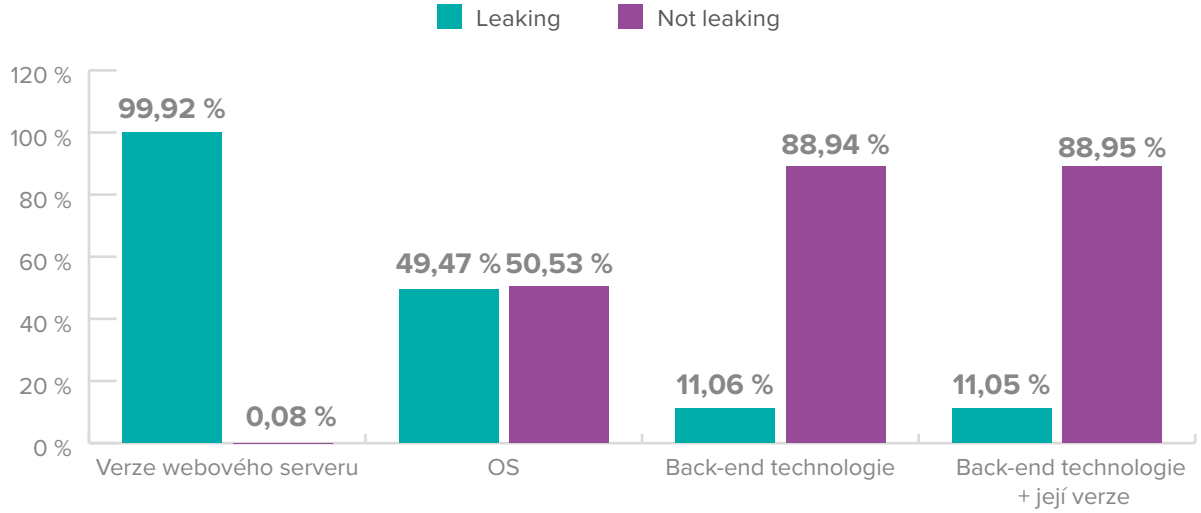
Toto nastavení nevyzrazuje potenciálnímu útočníkovi žádné podrobné informace a nalezení zranitelností by vyžadovalo další úsilí z jeho strany.

Z analýzy vyplývá, že 15,43 % zkoumaných webů prozrazuje návštěvníkům nějaké citlivé informace o používaných technologiích. Z toho 99,92 % prozrazuje verzi webového serveru, 49,47 % zahrnuje typ podkladového operačního systému a 11,05 % sděluje alespoň jednu back-endovou technologii včetně verze.

Server



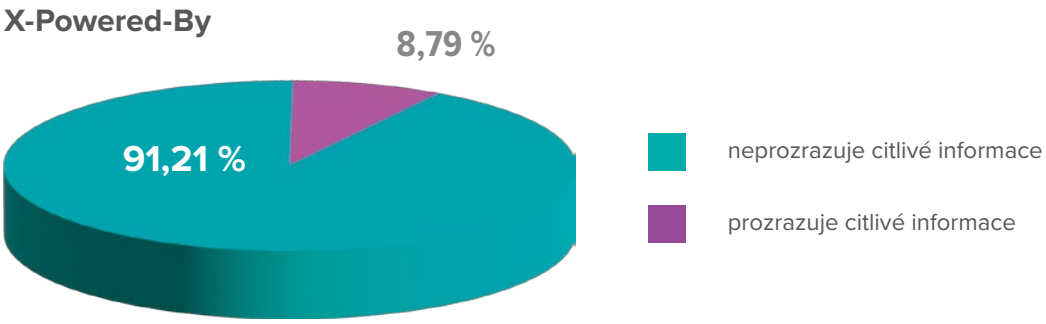
Leaking distribution

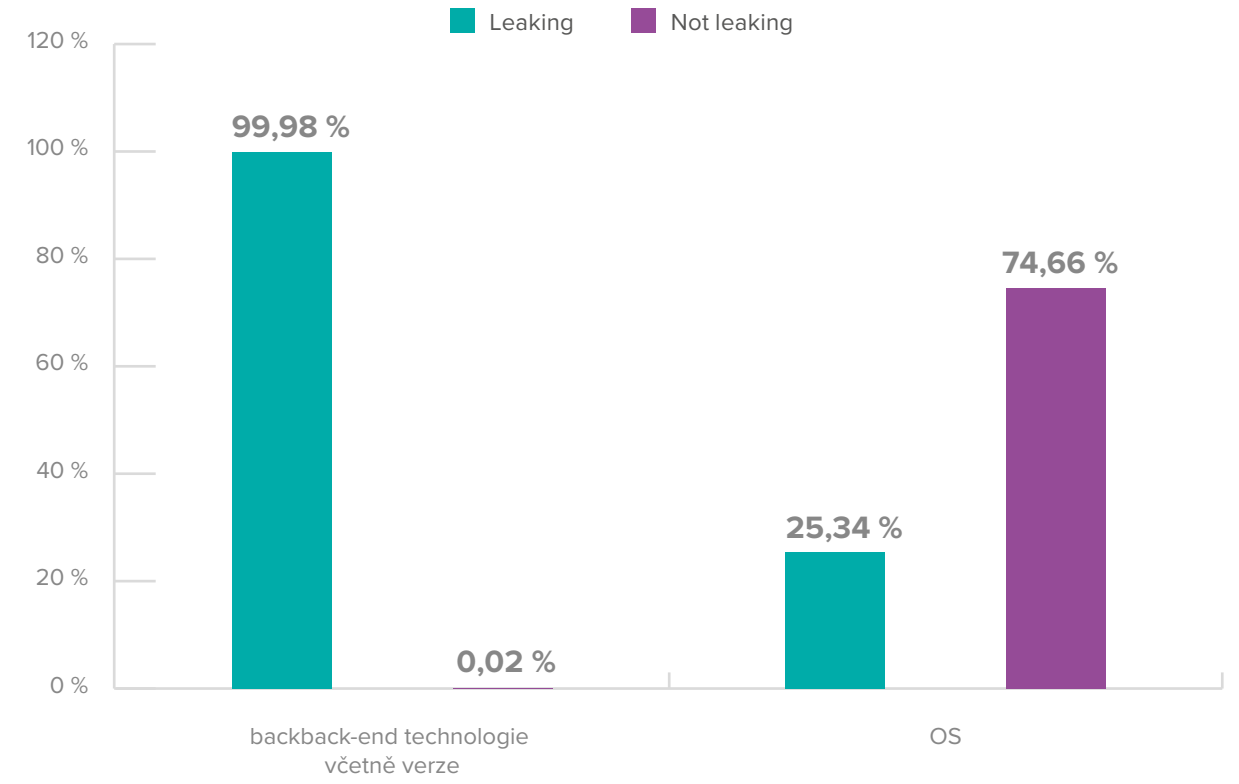


X-Powered-By HTTP Response Header

Předposlední zkoumaná hlavička, stejně jako v předchozím případě může odhalit citlivé informace o konfiguraci serveru. Často je ve výchozím nastavení obsažena v odpovědích vytvořených pomocí využívané skriptovací technologie nebo samotného webového serveru a může obsahovat název a číslo verze technologie použité při generování odpovědi. Stejně jako v předchozím případě může být zakázána nebo omezena. Administrátoři webových serverů ale často nechávají v tomto směru server ve výchozím nastavení a prozrazují tak návštěvníkům více informací, než by pravděpodobně chtěli. Doporučení u této hlavičky je nakonfigurovat server tak, aby hlavičku buď vůbec nevracel, nebo aby obsažené informace byly minimální.

Po provedení analýzy odpovědí bylo zjištěno, že 8,79 % zkoumaných webů v rámci hlavičky připojí nějaké citlivé informace o používaných technologiích. Z toho 99,98 % se týká alespoň jedné použité technologie včetně verze a 25,43 % prozrazuje typ operačního systému.





X-AspNet-Version HTTP Response Header

Poslední hlavička, na kterou se podíváme, se týká webů postavených na frameworku ASP.NET. Webový server může v hlavičce odpovědi odhalit verzi zmíněného frameworku, což může útočníkům potenciálně poskytnout cenné informace. Stejně jako v předchozím případě lze webový server nakonfigurovat tak, aby hlavičku v odpovědi nevracel.

Po analýze vyšlo najevo, že z celkového počtu zkoumaných odpovědí webových serverů, prozrazuje verzi ASP.NET frameworku pouze 0,81 % celkového počtu. Velmi malé množství serverů (asi 0,0003 %) hlavičku vrací ale s nevalidní hodnotou. Vzhledem k proporčnímu rozdělení skupin se tentokrát obejdeme bez grafu.

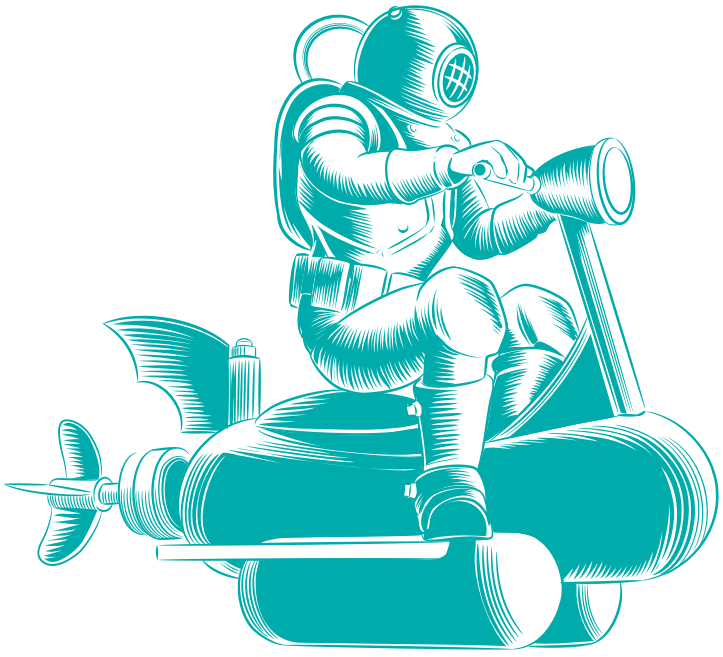
Vyhodnocení

Z analýzy vyplývá, že ne všechny weby na českém internetu jsou nastaveny ideálně. Většina uživatelů webové banery ignoruje, s výjimkou těch, kteří mají nějaké škodlivé úmysly. I když se nutně nemusí jednat o zranitelnosti, odhalení informací prostřednictvím HTTP hlaviček může poskytnout přesné informace o verzi webového serveru nebo webových technologií na základě kterých je následně možné identifikovat zranitelnosti v tomto softwaru a vyhledat případný veřejně známý exploit pro jejich zneužití. Útočníci mohou provádět sběr bannerů i automatizovaně pomocí jednoduchých nástrojů, jako je netcat nebo telnet. Poté provedou cílené útoky na zranitelnou verzi webového serveru. To může vést ke kompromitaci citlivých informací nebo v krajních případech k úplnému ovládnutí podkladového serveru webu. Tyto informace také hrají důležitou roli při určování útočných technik útočníků.

Mnoho serverů je ve výchozím nastavení nakonfigurováno tak, aby v rámci hlaviček zobrazovaly informace webového serveru. Na závěr lze tedy doporučit nakonfigurovat webový server tak, aby nevystavoval žádné informace o své značce, verzi nebo operačním systému. Pokud chcete zkontrolovat, zda váš webový server nějaké informace zveřejňuje, můžete to udělat manuálně, ale mnohem jednodušší je provést kontrolu napříč všemi webovými servery, stránkami a webovými aplikacemi pomocí automatického skeneru zranitelností. Takový skener najde i všechny další chybné konfigurace a potenciálně kritické zranitelnosti.

Zdroje:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers

https://owasp.org/www-project-secure-headers



Zálohování a obnova dat

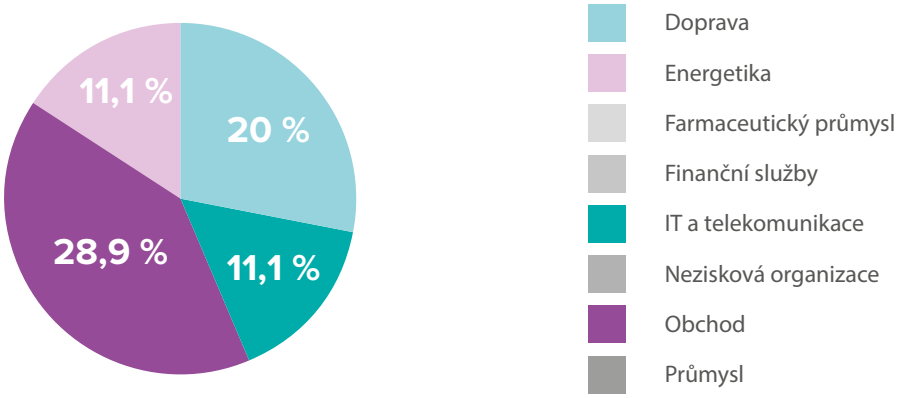
Pavel Dočkal

Geopolitický a bezpečnostní vývoj (včetně IT světa) v několika posledních letech zásadně proměnil požadavky na provozování informačních a komunikačních systémů. Celá společnost se stále více stává závislejší na internetu a technologiích a jejich nedostupnost nebo výpadek způsobený narušením poskytovaných služeb má významný dopad. Podle nedávno zveřejněného reportu Cisco Talos Incident Response za Q4 2023 stojí ransomware za 28% všech útoků (nárůst 17% oproti předchozímu čtvrtletí), proto se v aktuálním reportu budeme věnovat zálohování a obnově dat a dopadům ransomware útoků.

Zálohování a pravidelné testování použitelnosti záloh z pohledu důvěrnosti, dostupnosti a integrity je také jedním z požadavků současného Zákona o kybernetické bezpečnosti. V připravované legislativě transponující evropskou směrnici NIS2 jsou tyto předpisy pro režim vyšších povinností rozpracovány do větší hloubky. Kromě šifrování záloh dle šifrovacích algoritmů a dokumentace výsledků pravidelných testů obnovy dat, bude zapotřebí oddělit zálohovací prostředí od ostatních prostředí. Pokud je zálohovací systém součástí produkčního prostředí, je vystaven stejným hrozbám jako samotná aktiva a riziko kompromitace je tak vysoké.

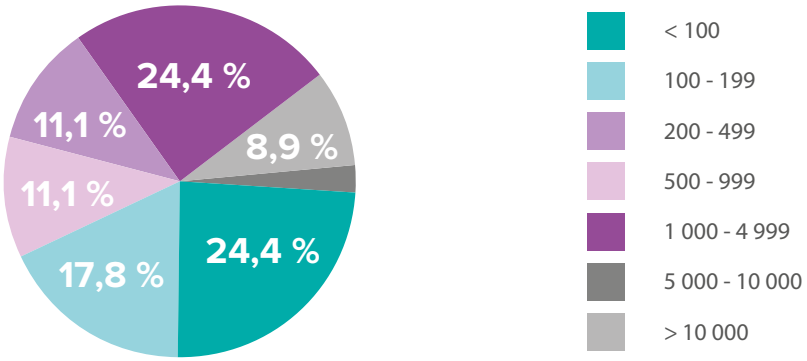
V našem dotazníkovém šetření byli respondenti zastoupeni napříč jednotlivými hospodářskými sektory, jak je patrné z grafu níže (největší podíl je z IT a telekomunikací, následovaný dopravou a energetikou).

V jakém sektoru Vaše organizace působí?



Rovnoměrné rozložení můžeme pozorovat u dalšího ukazatele, kterým je počet zaměstnanců. Méně zastoupenou skupinou respondentů jsou organizace s počtem 5 000-10 000. Nicméně pro tyto účely lze předpokládat, že řízení procesů souvisejících se zálohováním a obnovou dat bude odpovídat velkým společnostem o velikosti >10 000 zaměstnanců a tím by nemělo dojít k významnému zkreslení výsledků celého výzkumu.

Kolik zaměstnanců má Vaše organizace?



Z následujícího grafu je patrné, že pravidelné zálohování se stalo nezbytnou nutností fungování všech organizací a je přirozenou součástí všech IT a business procesů. Zároveň je to povzbudivý výsledek, jelikož si zodpovědné osoby uvědomují důležitost ochrany dat a minimalizaci rizik spojených s jejich ztrátou.

Zálohujete pravidelně data ve Vaší organizaci?

Proces zálohování lze nastavit buď automaticky pomocí specializovaného zálohovacího softwaru (např. Netapp, VEEAM, Veritas, Rubrik atd.) nebo manuálně. Výsledek téměř koreluje s předchozím grafem. U organizací, které zálohují manuálně, lze předpokládat, že tak činí nepravidelně. Výhody sofistikovaných automatických nástrojů jsou zřejmé: odolnost vůči lidské chybě a pravidelnost a spolehlivost záloh.

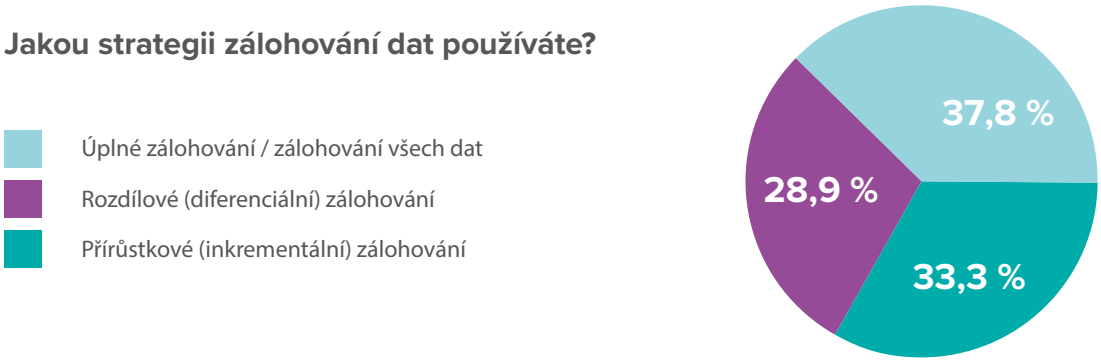
Jaký proces zálohy dat máte nastavený?

V jednotlivých organizacích panuje různorodost v používaných zálohovacích médiích. Každý typ má svoje klady a zápory, nicméně vedoucí pracovníci se obvykle pro každý typ dat rozhodují na základě těchto atributů: životnost zálohovacího média, náklady na jeden megabit, celková kapacita a rychlost zápisu. I když by se dnes mohlo zdát, že magnetické pásky jsou přežitkem z minulého tisíciletí, opak je pravdou. Díky nástupu technologie LTO (Linear Tape-On) nejnovější model LTO-9 nabízí na více než 1 km namotané pásky kapacitu 45 TB nekomprimovaných dat s životností 15-30 let dle podmínek skladování. Z odpovědí je patrné, že tradiční zálohovací metody jsou stále dominantní a cloud je zastoupen pouze z necelých 9 %.

Jaké médium využíváte pro zálohování?

Existuje velké množství zálohovacích strategií. Nejznámější pravidla jsou např. 3-2-1 (3 zálohy, z nichž 2 jsou místní na rozdílných zařízení a 1 mimo domov nebo kanceláře) nebo GFS (grandfather-son rotace denních, týdenních a měsíčních záloh na různých místech a typech médií). V našem dotazníkovém šetření jsme se zaměřili na způsob provádění těchto záloh. Poměrně vyvážený přístup mezi organizacemi panuje mezi úplnou, rozdílovou a přírůstkovou zálohou. Každá tato metoda vyžaduje různé nároky na kapacity zálohovacích médií a počet takových záloh pro úplné obnovení systémů. Respondenti nejvíce důvěřují úplnému zálohování tzn. zálohování veškerých dat.

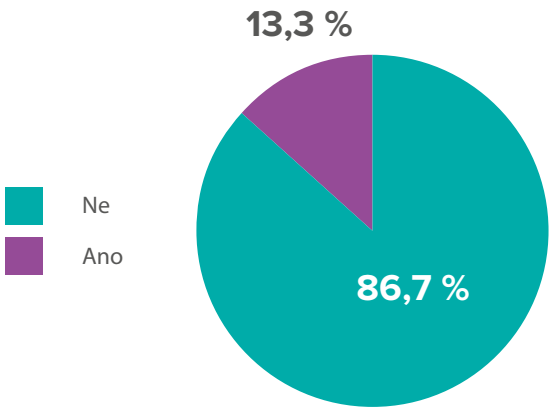
Jakou strategii zálohování dat používáte?



V této sekci se budeme věnovat tématu ransomwaru. Celosvětové škody za rok 2023 způsobené tímto typem malwaru, který zašifruje veškerá data a velmi často kompromituje i zálohy, přesahují 30 miliard USD. Dle výzkumu společnosti Checkpoint bylo nahlášeno za celý rok přes 60 000 útoků, jedná se však o zlomek skutečného počtu. Mnoho společností tato data vůbec nezveřejňuje kvůli obavě ze ztráty reputace. Dle statistik jsou nejvíce postižené Spojené státy americké, následované Velkou Británií a Německem. Obávat bychom se však měli i v České republice, která je zařazena mezi země s vysokou mírou pravděpodobnosti výskytu (Ransomware Risk Index 0,7). O to více jsou výsledky našeho průzkumu znepokojující, jelikož 4/5 organizací zatím ransomware nepocítily nebo

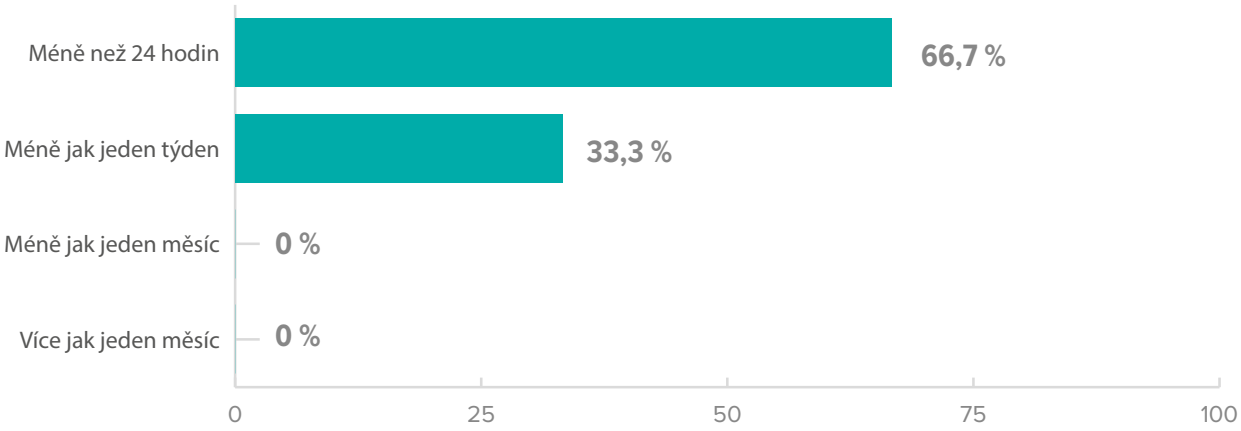
nedetekovaly. Dle zprávy IBM Security Cost of a Data Breach Report z roku 2022 trvá až 200 dní, než dojde k narušení systémů v důsledku aktivace škodlivého kódu, který se do sítě dostane např. díky zranitelnosti nebo phishingu.

Zaznamenali jste ve Vaší organizaci ransomware útok v posledních 2 letech?



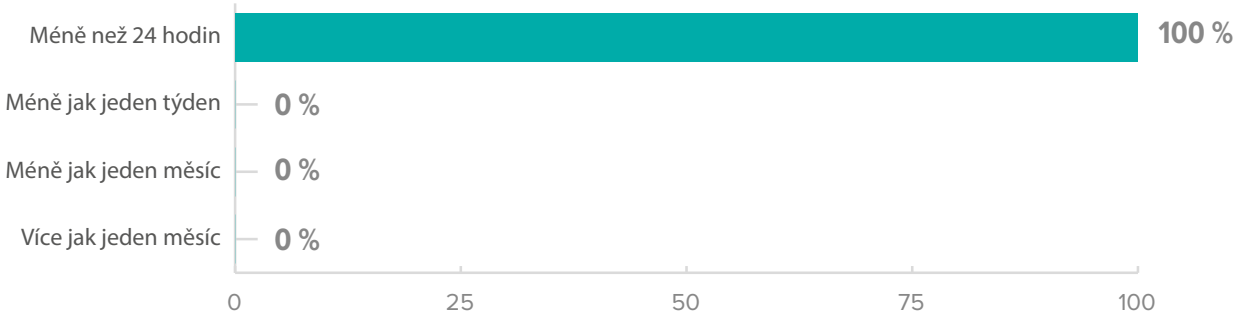
Pokud byla organizace napadena, tak pomocí detekčních nástrojů jako je SIEM, byla schopna velmi rychle reagovat a útok odhalit. U 66% dotazovaných to bylo dokonce za méně než 24 hodin, u zbytku pak za méně jak jeden týden. Rychlé odhalení a okamžitý zásah je základem pro minimalizaci škod a rychlou obnovu systémů do původního stavu. Interní nebo i externí SOC (Security Operations Center) s kvalifikovanými pracovníky, nastavenými postupy a správně nakonfigurovaným nástrojem jsou předpokladem účinného boje proti ransomwaru.

Za jak dlouho byl ransomware útok detekován?



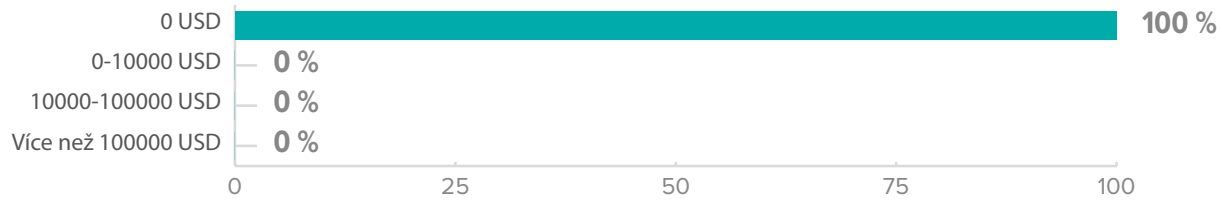
V případě kybernetického útoku se veškeré dostupné zdroje (finanční i lidské) soustředí na co nejrychlejší obnovení běžného provozu. Informační systémy jsou v takové situaci zašifrované a nefunkční. Správně nastavené strategické firemní politiky a procesy by měly zahrnovat predikci a připravenost na kybernetické bezpečnostní incidenty a implementovat Incident Response plán tzn. postupy, jak se chovat v případě kybernetických bezpečnostních incidentů a Disaster Recovery plán, které se zaměřují na obnovení IT infrastruktury a systémů v případě katastrofy. V našem výzkumu u všech napadených organizací proběhlo obnovení systémů do 24 hodin.

Za jak dlouhou dobu se organizace vrátila do plného provozu?



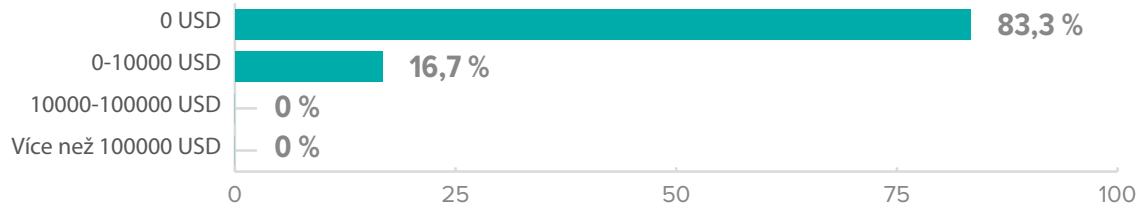
Motivace každého útočníka se liší, ale mezi nejčastější cíle patří zisk. Podle průzkumu, který byl proveden mezi 3000 profesionály ze 14 zemí světa, 46% z nich souhlasilo se zaplacením výkupného. Naše výsledky se zásadně liší od tohoto výzkumu, jelikož masivní útoky jsou, resp. byly vedeny na anglicky mluvící organizace z velkých světových ekonomik. S nástupem generativní umělé inteligence a jazykových modelů se však i toto paradigma postupně mění.

Jakou částku v podobě výkupného jste vynaložili výměnou za dešifrovací klíč?



Náklady za znovuobnovení chodu bývají často nižší než požadavky na výkupné za předpokladu, že organizace má správně nastavenou a zabezpečenou zálohovací strategii. Navíc platba za dešifrovací klíč s sebou nese spoustu rizik a nejistot, např.: organizace získá přístup pouze k části dat, klíč není vůbec poskytnut, data jsou prodána na černém trhu, útok je za nějaký čas proveden znovu, jelikož je zde velká pravděpodobnost vidiny další platby. Celosvětově se průměrné náklady na obnovu systémů pohybují ve výši 1,82 milionů USD (bez započtení výkupného). Výsledek našeho průzkumu nejspíše ukazuje na fakt, že nebyla stanovena metodika na výpočet těchto nákladů v rámci zkoumaných společností nebo IT oddělení zvládla pokrýt zprovoznění vlastními silami v rámci své běžné denní činnosti.

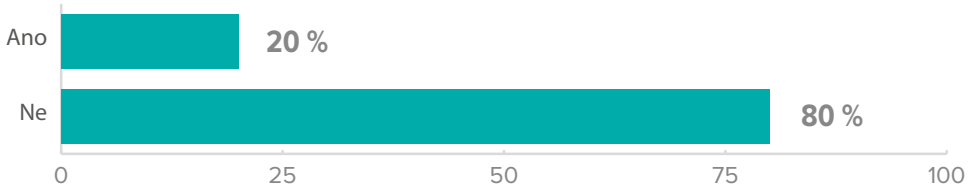
Kolik finančních prostředků jste vynaložili na obnovu dat (bez výkupného?)



Aby byla organizace schopna se vrátit ke své běžné činnosti, je naprosto nezbytným předpokladem pravidelně provádět a zabezpečit zálohy. Pokud jsou zálohy umístěny ve stejné síti, kde jsou provozní data, velmi pravděpodobně budou kompromitovány taktéž. Možností, jak efektivně zálohovat do

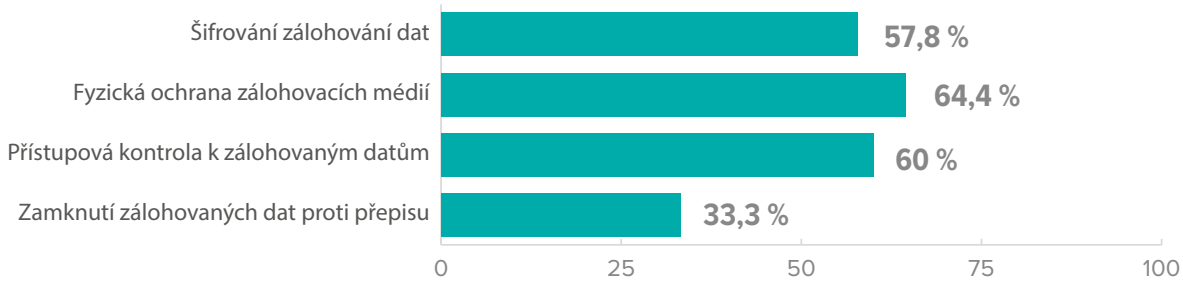
lokálních, hybridních nebo cloudových prostředí, je na trhu k dispozici celá řada. V prostředí firem v České republice se 80 % útoků nepropsalo do těchto záloh. Celosvětově je toto číslo vyšší – 39 % společností přišlo kompletně o své zálohy v důsledku ransomware útoku.

Propsal se ransomware útok do záloh a ovlivnil jejich kvalitu?



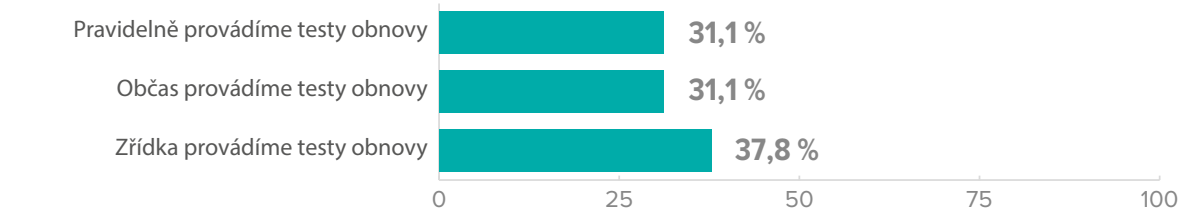
Jak už bylo zmíněno výše, nutnost ochrany záloh je zcela zásadní a níže jsou zobrazeny nejčastější způsoby, jakými odpovědní pracovníci přistupují k této problematice. Pomocí správně nastavené strategie je pak možné bez minimálních ztrát pokračovat tam, kde jsme před útokem skončili. Záleží na důležitosti zálohovaných dat a z toho vyplývajících hodnot Recovery Time Objective tzn., maximální doba, za kterou dojde k zotavení po výpadku a Recovery Point Objective tzn., do jakého bodu v minulosti lze data obnovit. Jednotlivá opatření se dají kombinovat. Například data na magnetických páskách jsou už při zápisu šifrována a následně zamčena do trezoru. V rámci autorizačních a autentifikačních mechanismů musí být zajištěno, že přístup k záloze budou mít pouze oprávnění administrátoři a uživatelé.

Jak chráníte zálohovaná data před neoprávněným přístupem nebo ztrátou integrity?



Součástí zálohování je i pravidelné testování obnovy dat. Pokud si organizace není jista, že je schopna během definovaného času v rámci Disaster Recovery plánu obnovit svůj provoz, pak s největší pravděpodobností budou celkové škody významně vyšší. Tímto přístupem se zároveň otevírá možnost včasného odhalení již probíhajícího útoku v latentní fázi, kdy útočník již proniknul do vnitřního prostředí, nahrál škodlivý malware, který se ale zatím nijak neprojevuje. České společnosti by tak měly zapracovat na tomto aspektu a lépe se tak chránit před budoucími hrozbami.

Jak často testujete proces obnovy dat?



Analýza dat z e-mailových bran

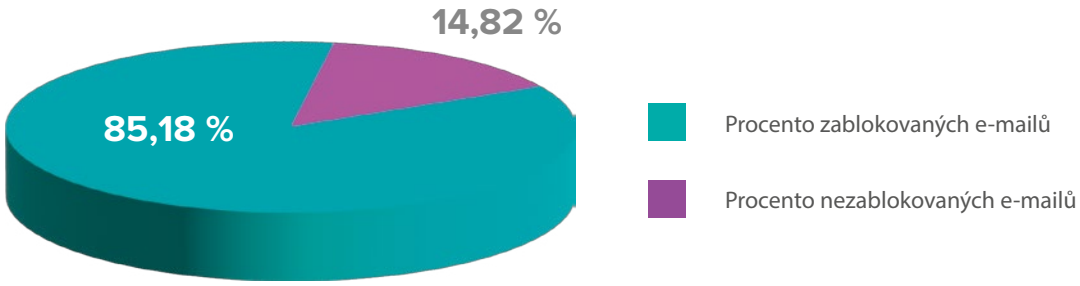
Martin Lusňák

Tato část analýzy probíhala nad daty příchozích e-mailových zpráv, které byly přijaty vybranými e-mailovými branami v roce 2023.

V průběhu roku 2023 bylo zablokováno více než 85,1 % všech příchozích e-mailových zpráv. To znamená nárůst o téměř 10 % oproti předchozímu roku.

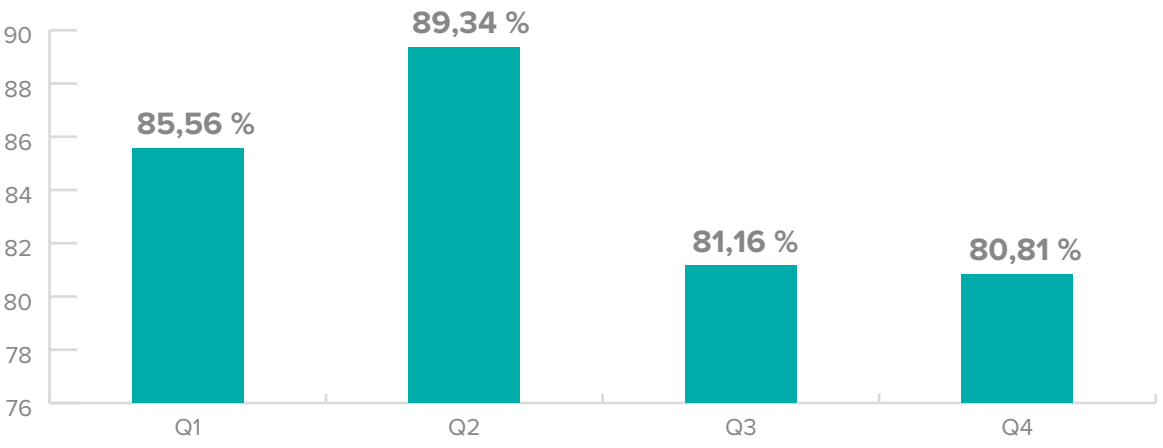
Zvýšení počtu zablokovaných e-mailových zpráv může být způsobeno různými faktory. Některé z nich mohou být například rostoucí digitalizace kde s nárůstem digitálních komunikací a online aktivit se zvyšuje i povědomí o možnostech útoků. Případně kvůli rostoucí globalizaci jsou phishingové útoky často mezinárodního charakteru.

Zablokované vs. nezablokované e-mailové zprávy



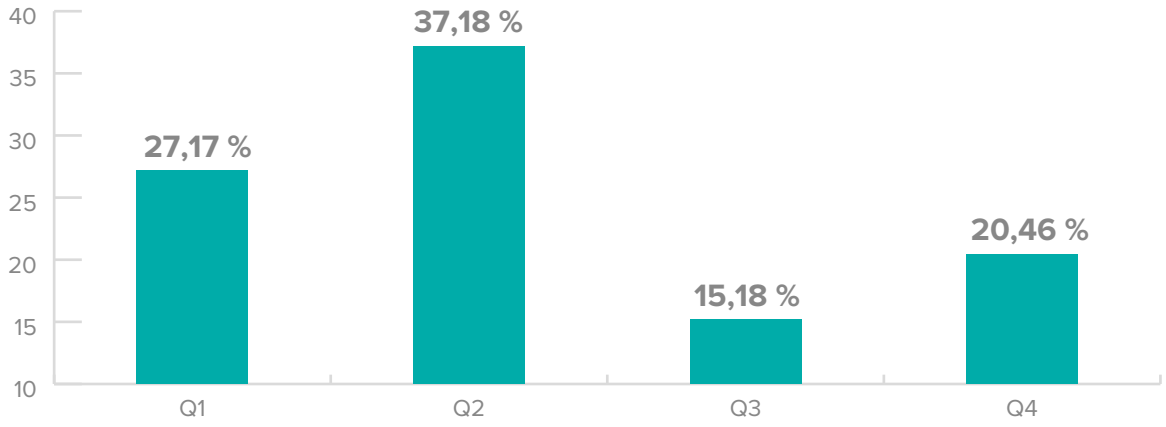
Průměrně bylo v každém čtvrtletí roku 2023 zablokováno e-mailovými branami 84,22 % zpráv. Nejvyšší procento blokovaných zpráv bylo zaznamenáno ve druhém čtvrtletí, které zahrnuje měsíce duben, květen a červen. V této době se počet zablokovaných zpráv vyšplhal na 89 procent.

Procento zablokovaných e-mailových zpráv v jednotlivých čtvrtletích



Níže prezentovaný graf poskytuje podrobný přehled o podílu zablokovaných zpráv v jednotlivých čtvrtletích, což usnadňuje důkladnější identifikaci odchylek nebo vzorů.

Procentuální rozdělení všech zablokovaných e-mailů do jednotlivých čtvrtletí



Období dovolených a pokles počtu zablokovaných e-mailových zpráv

Graf zřetelně ukazuje, že existuje značný rozdíl mezi druhým a třetím čtvrtletím. Tato odchylka může být interpretována jako důsledek specifické dynamiky v rámci těchto období. Je možné, že výraznější podíl zablokovaných zpráv ve druhém čtvrtletí souvisí s charakteristickou situací, jako jsou dovolené, což může ovlivnit chování uživatelů a útočníků kdy útočníci pravděpodobně intenzivněji využívají toto období.

Tento trend se odráží i v počtu zablokovaných zpráv, který ve stejném období výrazně klesá. Pravděpodobně je to z důvodu, že pro útočníky není efektivní posílat velké množství zpráv obsahujících škodlivý obsah, protože uživatelé na dovolené s nimi neinteragují. Další možné vysvětlení spočívá v tom, že samotní útočníci jsou pravděpodobně také na dovolených a nezasílají spamové a phishingové zprávy.

Analýza důvodu blokace e-mailových zpráv

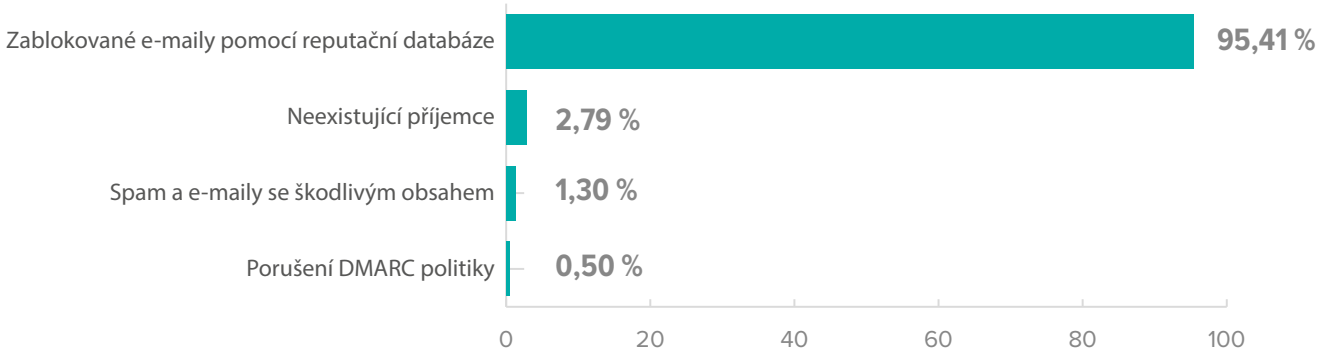
Během analýzy příčin blokování e-mailových zpráv na e-mailových branách jsme zjistili, že většina zablokovaných e-mailů byla zastavena díky reputační databázi (95,41 %). Tato databáze přiřazuje serverům hodnocení. Pokud je toto hodnocení nízké nebo negativní, pak je komunikace z daného serveru blokována.

Další kategorií, která byla blokována, zahrnovala e-maily označené jako spam a zprávy se škodlivým obsahem, což představovalo 1,30 % všech zablokovaných e-mailů. Tyto zprávy obsahovaly odkazy vedoucí na škodlivé webové stránky, a pouze malá část z nich obsahovala přílohu s nebezpečným softwarem.

Dalším faktorem vedoucím k blokování jsou neexistující příjemci (2,79 %), což může být způsobeno chybou při zadávání e-mailové adresy nebo také tím, že daná e-mailová adresa již neexistuje. Někdy se může stát, že e-mailová adresa zůstává v seznamu útočníků nebo je stále uvedena na webových stránkách společnosti, i když už není platná.

Posledním důvodem, který vedl k blokování e-mailů je porušení DMARC politiky, což se týkalo přibližně 0,50 % všech zablokovaných zpráv. DMARC politika funguje na základě stanovení pravidel pro ověřování a ochranu před podvrženými e-maily. Tato politika je nastavena na doménovém jméně v adrese odesílatele a provádí kontrolu na legitimní i podvržené e-maily. V případě, že e-mail nesplňuje DMARC politiku, může být označen jako podezřelý nebo, jak tomu bylo v našem případě, zablokován na e-mailové bráně.

Zablokované e-mailové zprávy podle kategorií



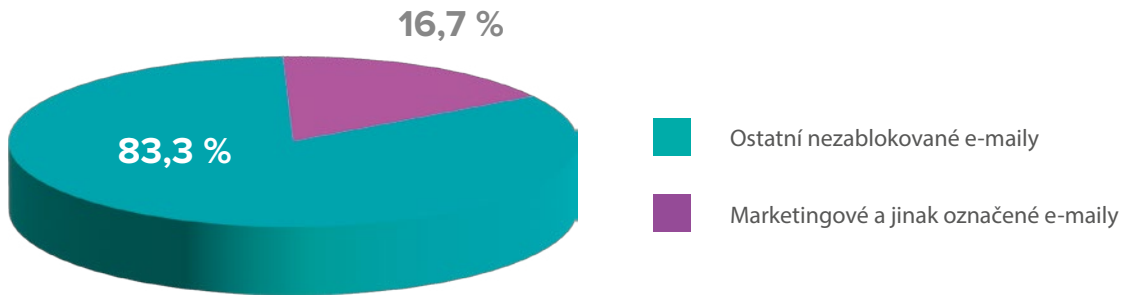
Marketingové a jinak označené e-mailové zprávy (Graymail)

E-mailové brány jsou schopny identifikovat a označovat e-mailové zprávy, které obsahují marketingové informace nebo jsou zasílány ze sociálních sítí. Tato kategorie zpráv je běžně označována jako "Graymail". Někteří uživatelé mohou považovat tyto zprávy za nevyžádanou poštu, ale existují i ti, kteří si je vyžádali. V důsledku toho se tyto zprávy nacházejí v nejisté "šedé zóně" mezi spamem a legitimními e-maily. Je důležité si uvědomit, že označení těchto e-mailů jako "Graymail" je složitý proces, a nelze jednoznačně určit, zda se jedná o nevyžádanou poštu. Z celkového počtu analyzovaných zpráv představovaly 4,78 %.

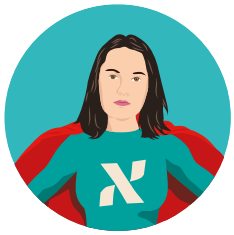
Z toho plyne že e-mailové brány tyto zprávy automaticky neblokují, ale identifikují je různými způsoby, jako je například vložením textu "[Marketing]" do předmětu e-mailové zprávy. Ve vzorku dat z e-mailových bran bylo 24,34 % z celkového počtu identifikovaných graymailů označeno tímto způsobem. Hromadné zprávy tvořily 66,48 % graymailů a zprávy ze sociálních sítí tvořily 9,18 %. Procentuální zastoupení graymailu (tj. výše uvedených kategorií) ve vzorku neblokovaných zpráv bylo 16,7 %.

Zbývajících 83,3 % neblokovaných zpráv bylo považováno za legitimní e-maily, což odpovídalo 12,35 % celkového počtu všech zpráv. V roce 2022 tvořily graymaily 8,03 % neblokovaných zpráv, což odpovídalo 4 % celkového počtu. Data pro rok 2023 tedy ukazují významný nárůst.

Zablokované vs. nezablokované e-mailové zprávy



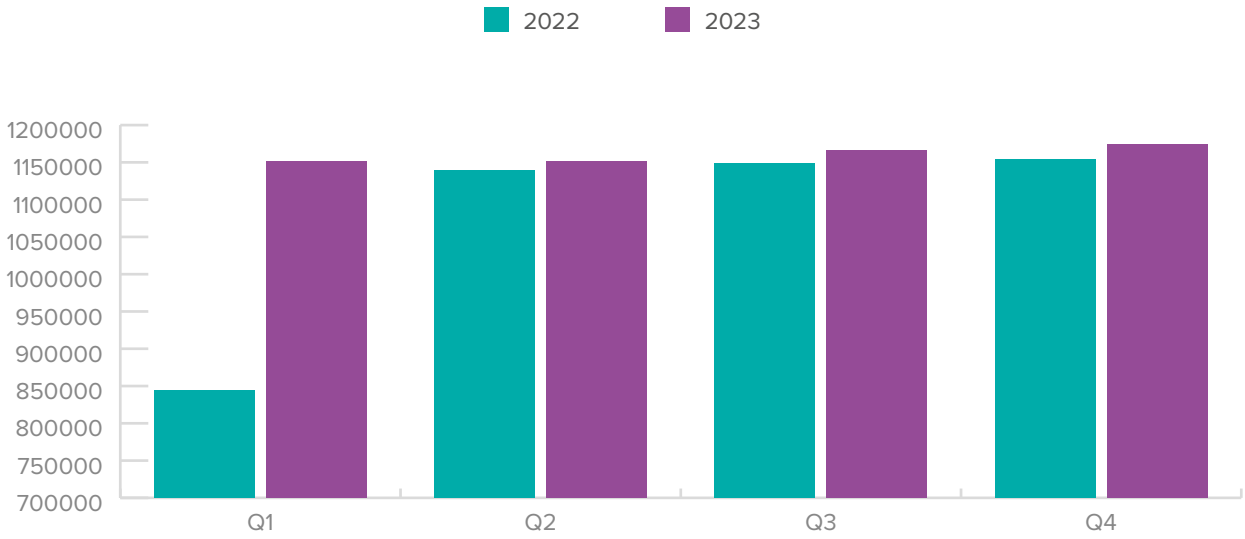
Úroveň šifrování webserverů na českém internetu



Oleksandra Kocyba

Tak jako minulý rok se podíváme na úroveň šifrování webových serverů na českém internetu za rok 2023. Z dat nahromaděných v minulém roce se nejdříve podívejme na celkový počet detekovaných webových serverů, podporujících jak šifrovaný, tak i nešifrovaný provoz. Z grafu můžeme pozorovat jen velmi mírný nárůst v celkovém počtu detekovaných webových serverů oproti minulému roku. Kromě značného rozdílu mezi prvními kvartály se jedná o navýšení průměrně o 16 000 webových serverů v jednotlivých kvartálech.

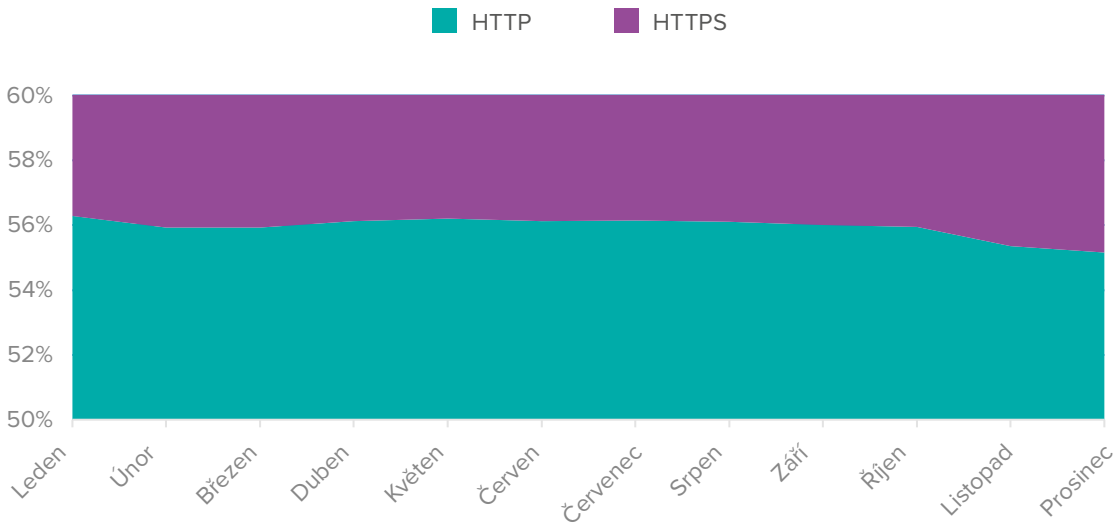
Porovnání počtu detekovaných webových serverů



Na dalším grafu můžeme tak, jako i minulý rok vidět vychýlení v poměru webových serverů ve prospěch těch, které podporují nešifrovaný provoz. Je důležité zmínit, že podpora protokolů HTTP i HTTPS není vzájemně exkluzivní. Mnoho webových serverů má otevřený jak port 80 (HTTP) používaný pro prvotní spojení s klientem, tak i port 443 (HTTPS), na který je klient následně přesměrován a kde poté probíhá komunikace šifrovaně.

U detekovaných webových serverů podporujících protokol HTTP se udržujeme stále přibližně na hodnotě 56 %. Podobnou hodnotu můžeme pozorovat i z minulého roku, a tak se poměr serverů podporujících šifrovaný nebo nešifrovaný provoz udržuje přibližně stejný. Až ke konci roku můžeme pozorovat drobný nárůst webových serverů podporujících HTTPS protokol v poměru oproti webovým serverům podporujícím protokol HTTP.

Poměr služeb HTTP a HTTPS na českém internetu

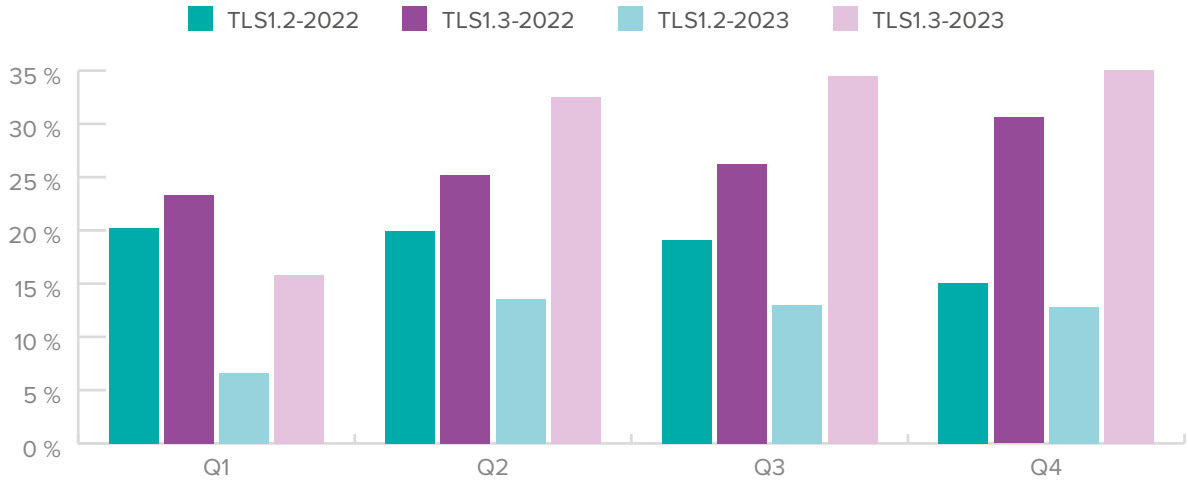


Analýza TLS a šifrovacích sad

Webová komunikace je šifrovaná pomocí protokolů TLS a SSL. Protokol SSL je předchůdcem TLS, a jelikož obsahuje známé zranitelnosti, tak by se z bezpečnostních důvodů již neměl používat. Nahradil jej právě protokol TLS, který prochází vývojem již od roku 1999, od verze TLSv1.0 až po současnou verzi TLSv1. 3. , přičemž mezi doporučované verze od roku 2020 patří pouze TLSv1.2 a TLSv1. 3. Na českém internetu se tato doporučení dle dat nahromaděných za rok 2023 projevují.

I v tomto roce docházelo k postupnému snižování webových serverů podporujících již nedoporučované protokoly TLS1.0 a TLS1. 1. V případě TLS1.0 až na hodnotu 0,004 % z původních 0,2 % z minulého roku a v případě TLS1.1 na hodnotu 0,0009 % z 0,001 %. Zároveň pokračoval i trend v nárustu webových serverů podporujících TLS1.3, kdy ke konci roku 2023 více než třetina všech webových serverů na českém internetu podporovala tuto verzi TLS. V případě porovnání hodnot mezi webovými servery podporujícími šifrovanou komunikaci, podporovalo více než 66 % z nich právě TLS verze 1. 3.

Podpora TLS 1.2 a TLS 1.3 v letech 2022 a 2023

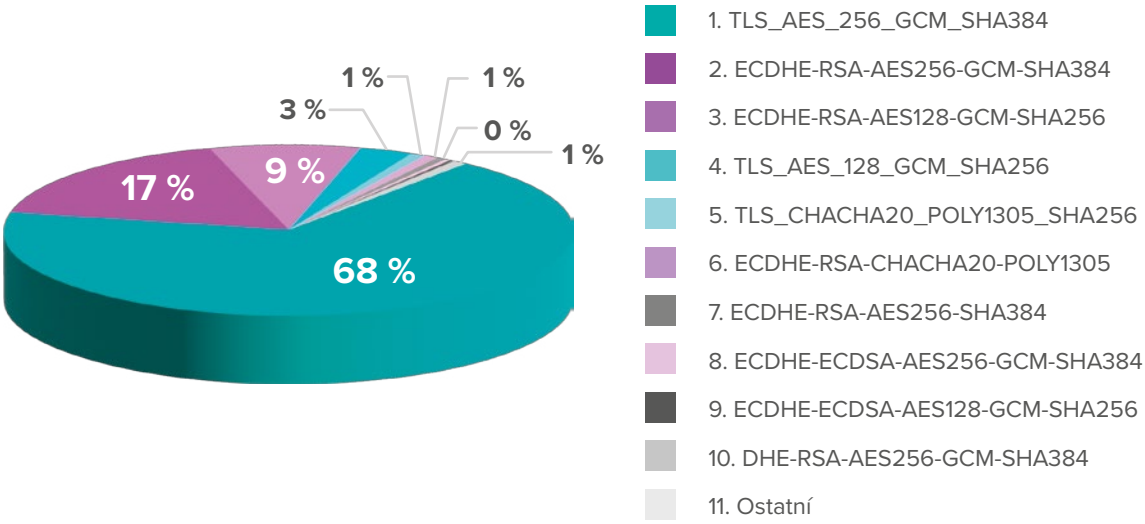


Při navazování komunikace je nutné určit také šifrovací sadu, ta určuje nejen algoritmus použitý při šifrování komunikace ale i algoritmus pro výměnu klíčů, algoritmus sloužící k autentizaci a MAC algoritmus zajišťující integritu přenášených dat. Vybraná šifrovací sada poté určuje jak bezpečná,

kompatibilní a rychlá bude komunikace mezi klientem a serverem.

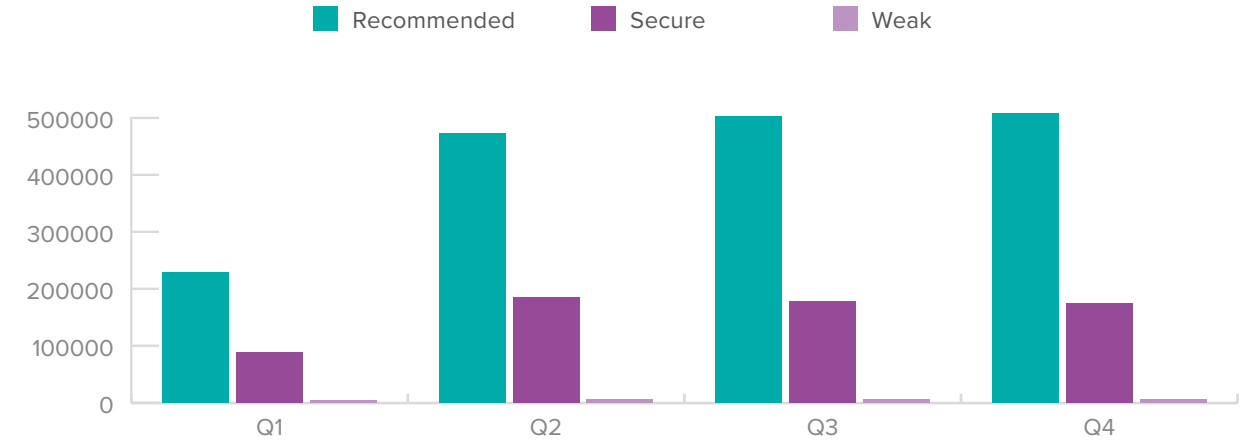
Šifrovacích sad je velké množství a pro tento report bylo vybráno 26 nejčastěji používaných. Jsou rozděleny do kategorií: Recommended (např. TLS-AES-256-GCM-SHA384), Secure (např. ECDHE-RSA-AES128-GCM-SHA256) a Weak (např. ECDHE-RSA-AES256-SHA384). Jako v minulém roce byla nejpoužívanější šifrovací sadou sada TLS_AES_256_GCM_SHA384, která byla použita na 68 % všech webových serverů podporujících šifrovanou komunikaci.

Top 10 nejpoužívanějších šifrovacích sad



V grafu níže jsou poté znázorněny počty webových serverů podporujících danou kategorii šifrovacích sad. Můžeme tak vidět nárůst serverů podporujících šifrovací sady kategorizované jako Recommended a snížení počtu serverů podporujících sady spadající do zbylých dvou kategorií.

Webové servery podporující šifrovací sady dle kategorií



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

Zabezpečení WiFi

Martin Šišmiš

Zabezpečení Wi-Fi a jeho testování

Wi-Fi se stalo nedílnou součástí našeho každodenního života, ať už jsme doma, v kavárně, nebo v práci. Díky tomu jsou útoky na Wi-Fi oblíbeným útočným vektorem a také vstupním bodem do vnitřního prostředí organizace. Správné nastavení a zabezpečení Wi-Fi sítí a návazné infrastruktury se tak stává jedním z klíčových prvků kybernetické obrany organizace. Pro implementaci zabezpečených Wi-Fi sítí je nutné správně rozvrhnout architekturu, porozumět různým bezpečnostním technologiím obsažených ve standardu 802.11, pravidelně i ad-hoc instalovat záplaty a patche výrobce a dále pak testovat bezpečné nastavení a možnosti výskytu zranitelností.

Základem bezpečného přenosu dat přes Wi-Fi síť jsou šifrovací protokoly, které zajišťují důvěrnost a zabezpečení komunikace. Dva nejpoužívanější standardy jsou WPA2 a novější WPA3.

WPA2 (Wi-Fi Protected Access 2)

byl dlouhou dobu považován za zlatý standard zabezpečení Wi-Fi (je tu s námi již od roku 2004). Využívá šifrování CCMP, které je založené na AES standardu a stále poskytuje relativně bezpečné připojení. Nicméně, s rostoucí výpočetní kapacitou se stal zranitelnější vůči útokům, jako jsou metody "brute force" při zachycení 4-way handshake a není složité útočit na dostupnost, či provést MitM útoky (Man-in-the-Middle) za pomoci frame injection.

WPA3 (Wi-Fi Protected Access 3)

představuje výrazný pokrok v oblasti zabezpečení Wi-Fi. Zahrnuje individuální šifrování připojení (Forward Secrecy), odolnější šifrovací standard (GCMP-256) a zabezpečení výměny šifrovacích klíčů (Simultaneous Authentication of Equals – SAE) což dále zvyšuje kryptografickou odolnost sítě. Dále za pomoci ochrany management framů chrání proti injection útokům (Management Frame Protection – MFP, je podporován i na WPA2 zařízeních dle implementace výrobce, ale certifikovaná WPA3 zařízení ji musí umět podporovat) a přináší ochranu na otevřených sítích za pomoci oportunistického šifrování (Opportunistic Wireless Encryption – OWE).

Pro podnikové sítě je ve standardu 802.11 specifikována forma autentizace **WPA Enterprise**, která do Wi-Fi sítí přidává implementaci standardu 802.1x, tedy užití autentizačního (například Radius) serveru. Tato autentizace umožňuje používat a vytvářet přihlašovací identity pro jednotlivé uživatele a používá autentizační metodu EAP v různých typech implementace (například EAP-TLS, PEAP, apod.).

Důležitou součástí zabezpečení Wi-Fi sítí je pravidelná aktualizace firmware daných zařízení a používání nejnovějších bezpečnostních protokolů (viz. rozdíl WPA2 oproti WPA3). Firmware aktualizace často zahrnují opravy bezpečnostních chyb a vylepšení, která jsou klíčová pro stabilitu a bezpečnost celé sítě. Je důležité sledovat kritické zranitelnosti na konkrétních Access Point (AP) zařízeních, pro možnost urychlené aktualizace v případě vydání bezpečnostních záplat. Při výběru nového zařízení je také důležité zajistit, aby podporovalo nejnovější bezpečnostní standardy, protokoly (pokud možno certifikované) a vyhodnotit náchylnost produktů daného výrobce k výskytu zranitelností, což samozřejmě může pomoci s odolností sítě vůči kybernetickým hrozbám.

Proaktivní testování zabezpečení, monitoring a správa přístupů jsou důležité komponenty pro identifikaci a eliminaci potenciálních rizik:

- Penetrační testování simuluje útoky na Wi-Fi síť a její klienty za účelem odhalení možných zranitelností. Testovací metody zahrnují útoky na autentizační metody (a to jak WPA Personal, tak WPA Eneterprise), zranitelnosti AP, útoky na standard 802.11 (MitM, Dos, a jiné). Jak bylo zmíněno, lze také k testování zahrnout i klienty sítě, kde například IOT a OT zařízení mohou být poměrně náchylná ke zranitelnostem, či sociální inženýrství (za pomoci Captive Portal).

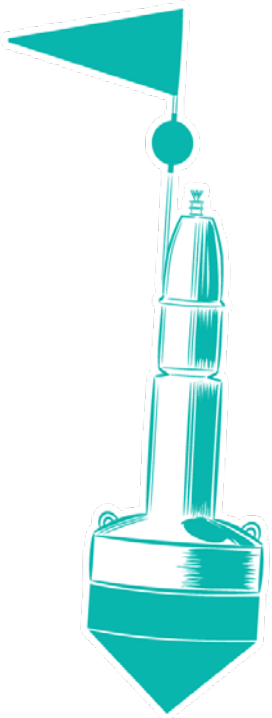
- Monitorování síťového provozu – pravidelné monitorování síťového provozu umožňuje odhalit neobvyklé aktivity nebo podezřelá zařízení (rouge access point, evil twin). Zde je možné využít nativních nástrojů výrobce (pokud takové má, bývá součástí licence pro WLC, Wireless Controler), open source nástrojů (jako například Kismet), či nástroje pro zachytávání a interpretaci síťového provozu (Wireshark) k analýze datového provozu a detekci potenciálních hrozeb.

- Správa hesel – silná a jedinečná hesla jsou základem ochrany proti neoprávněnému přístupu. Občasná změna hesla může v případě WPA Personal pomoci zvýšit úroveň zabezpečení Wi-Fi sítě. Pro WPA Enterprise je důležité implementovat interní politiky pro off-boarding zaměstnanců, kvůli smazání identity odchozího zaměstnance.

V zájmu zachování bezpečnosti infrastruktury by měli administrátoři také dbát na správnou konfiguraci síťových zařízení, jako jsou switche, routery a firewally, do kterých jsou AP připojeny. Správné nastavení může pomoci s minimalizací možností útočníka po proniknutí do Wi-Fi sítě, či s ochranou fyzických portů, ke kterým mohou mít přístup nepovolané osoby (například venkovní AP).

Správné nastavení, pravidelné testování a aktualizace jsou nezbytné pro udržení vysoké úrovně ochrany. Přechod na modernější technologie, jako je WPA3, může poskytnout větší bezpečnostní ochranu v porovnání s předchozím standardem WPA2. V době, kdy se stáváme stále více závislými na bezdrátovém připojení, je kybernetická bezpečnost a minimalizace rizika na tomto vektoru pro potenciální útočníky jedním z klíčových prvků pro ochranu korporátního prostředí a dat v něm se nacházejících.

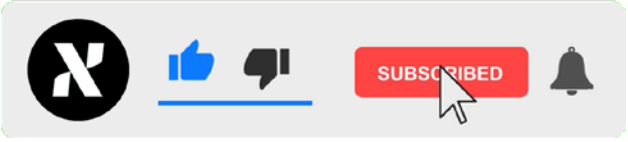
Společnost Alef Nula nabízí v oblasti bezpečnosti Wi-Fi sítí služby komplexního penetračního testování se specializovaným vybavením. Dále pak poskytuje dvoudenní školení pro úvod do bezpečnosti a testování Wi-Fi sítí, které může pomoci administrátorům či začínajícím testerům zkontrolovat nastavení Wi-Fi sítě a může sloužit ke zjištění základních nedostatků v případě, kdy není možné v krátké době poskytnout plnohodnotný penetrační test.



Novinky, rozhovory, doporučení.

Sledujte náš kanál ALEF Security zaměřený na kybernetickou bezpečnost!

YouTube



ALEFNULA

Pro více informací kontaktujte cz-sales@alef.com