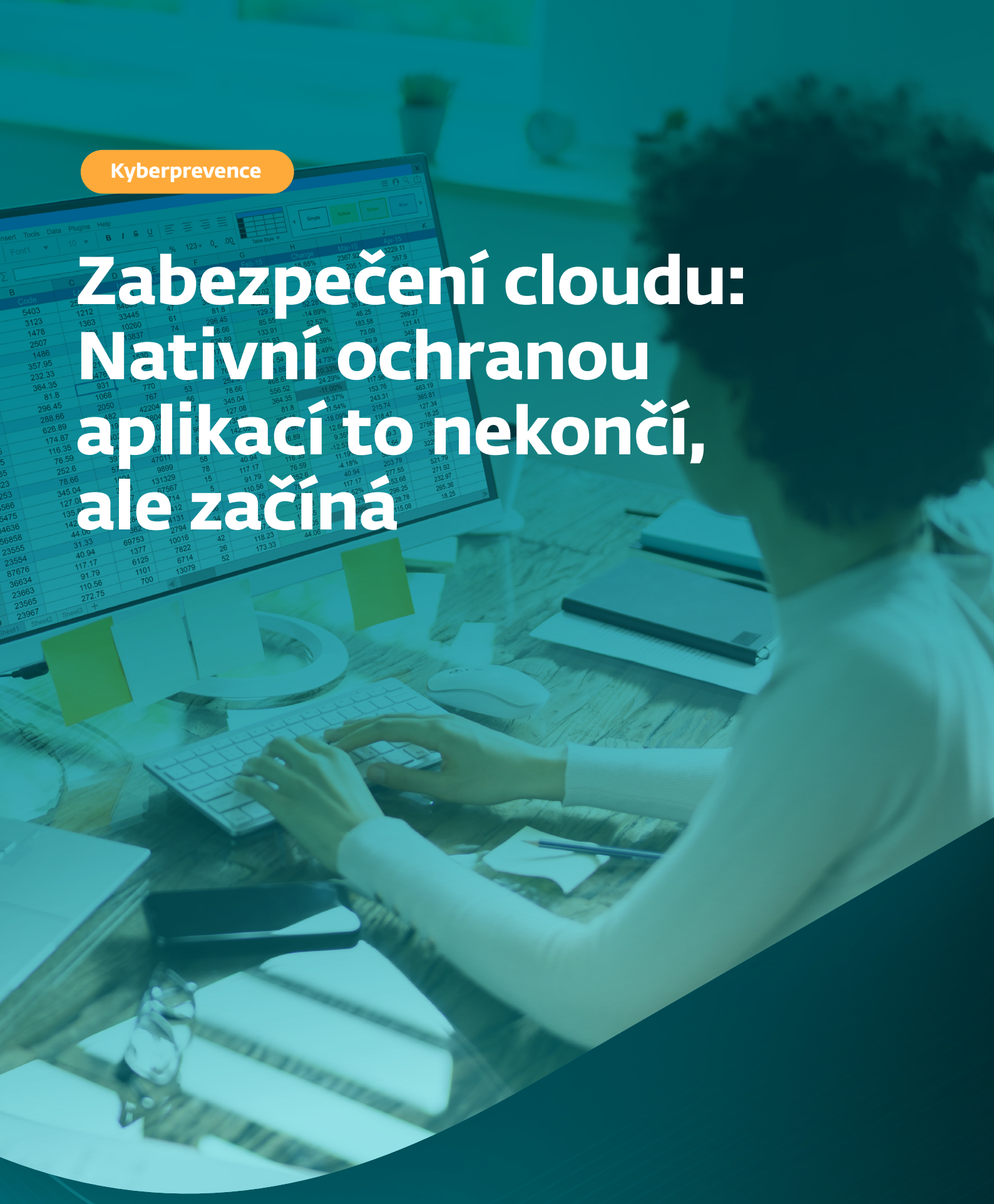
Kyberprevence

Zabezpečení cloudu: Nativní ochranou aplikací to nekončí, ale začíná



ESET Digital Security
Progress. Protected.

IT správci se jistě počítají mezi 3 miliardy uživatelů služby Google Workspace nebo 320 milionů uživatelů aplikace Microsoft Teams. Po úspěšném nasazení a nastavení bezpečnostních pravidel mohou v ideálním světě získat čas na jiné důležité úkoly, zatímco firemní týmy (spolu)pracují v bezpečném prostředí.

Tito technologičtí giganti začlenili špičkové zabezpečení přímo do svých cloudových aplikací, takže se není čeho obávat, že? No, tyto široce používané cloudové aplikace jsou chráněné a pravidelně aktualizované, ale to **neznamená, že jsou imunní vůči všem hrozbám**.

Existuje mnoho případů **zneužití legitimních cloudových aplikací** kyberútočníky. Pokud chcete takovým incidentům ve vaší firmě předcházet, musíte přidat další vrstvy zabezpečení. Se správnými nástroji mohou správci minimalizovat možnosti průniku do společnosti ze svých cloudových služeb a zavést **přístup zaměřený především na prevenci**.

Rostoucí zájem útočníků

Společnosti po celém světě neustále hledají způsoby, jak fungovat efektivněji a nezávisle na lokalitě. Tržby na trhu veřejných cloudů v letech 2019 až 2023 se více než zdvojnásobily a v roce 2024 by měly dosáhnout 690,3 miliardy dolarů.

S růstem trhu však roste i zájem kyberzločinců. Mezi červnem 2021 a červencem 2023 **společnost ESET detekovala a zablokovala miliony hrozeb, které by jinak obešly nativní ochranu cloudových služeb** Microsoft 365 a Google Workspace.

Většinu těchto zablokovaných hrozeb tvořily **phishingové a spamové zprávy**. Nejnovější data ukazují, že tento trend nebere konce. Podle zprávy ESET Threat Report H2 2023 vzrostl objem spamu o 6 % a škodlivé HTML soubory, které směřují oběti na phishingové stránky (trojan HTML/Phishing.Agent), jsou stále zdaleka nejčastěji detekovanou e-mailovou hrozbou.

Celkově tyto **e-mailové útoky tvoří téměř čtvrtinu (23,4 %) všech kybernetických hrozeb** detekovaných společností ESET.

Mezi další cloudové hrozby detekované telemetrií ESET patří různé typy malwaru, jako jsou backdoory, spyware, infostealery a downloadery.

DETEKCE ESET V ČÍSLECH

Rostoucí objem phishingu je důvod, proč firmy potřebují další vrstvy ochrany. Velmi často totiž nativní cloudové kancelářské produkty označí e-mail nebo soubor jako "bezpečný". Skenování bezpečnostními produkty probíhá až poté. Bez ESET Cloud Office Security by se tyto e-maily a soubory pravděpodobně dostaly do schránek uživatelů a nástrojů pro online spolupráci.

1 mil. +

malwarových hrozeb

500 tis. +

phishingových e-mailů

30 mil. +

spamových e-mailů

1000 +

dosud neznámých detekcí pomocí ESET LiveGuard Advanced

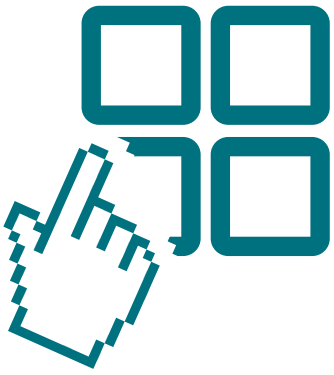
Vaše aplikace nejsou tak bezpečné, jak si myslíte

Příklady z praxe ukazují, že legitimní cloudové aplikace a služby lze zneužít k šíření malwaru, obfuskaci škodlivých procesů nebo vzdálenému přístupu k firemním zařízením.

V druhé polovině roku 2023 zaznamenali bezpečnostní experti společnosti ESET nové phishingové e-mailové kampaně neznámého útočníka, které cílily na firmy v Evropě. **E-maily obsahovaly škodlivé přílohy** vylepšené o tzv. AceCryptor, malware typu cryptor-as-a-service, který je určený ke skrytí jiného škodlivého kódu před detekčními nástroji. V případě úspěchu mohli útočníci nasadit nástroj pro vzdálený přístup Rescoms (známý také jako Remcos) a špehovat své oběti.

V průběhu roku 2022 kyberšpionážní skupina OilRig aktivně vyvíjela a používala řadu downloaderů, které **zneužívaly rozhraní API (Application Programming Interface) legitimních cloudových služeb**, jako jsou Microsoft Graph OneDrive, Microsoft Graph Outlook a Microsoft Office EWS, ke skrytí škodlivé komunikace. Útočníci zneužívali například e-mailové účty k vytváření konceptů zpráv (rozepsaných e-mailů) se skrytými příkazy pro malware, který již byl v napadeném zařízení.

Naštěstí někdy odborníci na kybernetickou bezpečnost najdou zranitelnosti dříve než útočníci. V červnu 2023 objevil Red Team britského poskytovatele bezpečnostních služeb Jumpsec snadný způsob, jak doručit malware pomocí Microsoft Teams prostřednictvím externího účtu. Analytici Red Teamu obešli vestavěnou ochranu a dokázali oklamat systém tak, aby si myslel, že externí uživatel je ve skutečnosti interní.



Další zabezpečení

Z výše popsaných případů je zřejmé, že nativní zabezpečení cloudových aplikací nestačí. Firmy by se měly zaměřit na eliminaci rostoucího počtu způsobů, kterými útočníci mohou proniknout do organizace. Prevence zmírní dopady útoků dříve, než mohou napáchat škody. Jak? Tím, že firmy **rozšíří základní kontroly** společností Microsoft nebo Google o další vrstvy ochrany pro e-mail, nástroje pro spolupráci a úložiště hostované v cloudu.

Jak zlepšit ochranu cloudu:

- **Anti-spam** – Nevyžádané zprávy tvořily v roce 2022 více než 45 % z 333 miliard e-mailů odeslaných a přijatých po celém světě denně. Se správným řešením pro filtrování pošty mohou firmy ušetřit spoustu času zaměstnancům a vyhnout se potížím se škodlivým spamem.
- **Anti-phishing** – U každé čtvrté americká společnosti, která v roce 2022 čelila kybernetickému útoku, stál za počátečním průnikem do společnosti phishing. Mít automatizovaný nástroj, který rozpozná phishingové odkazy připojené k e-mailům, by se mohlo hodit.
- **Anti-malwarová kontrola** – Dobré cloudové bezpečnostní řešení by mělo automaticky kontrolovat všechny nové a změněné soubory ve sdíleném úložišti, aby se zabránilo spuštění nebo šíření malwaru.
- **Analýza chování a sandbox** – V rychle se vyvíjejícím IT světě se neustále objevují nové hrozby. Automatizované nástroje kybernetické bezpečnosti musí být připraveny na dosud nezaznamenané hrozby. K tomu slouží hloubková behaviorální analýza podezřelých vzorků v bezpečném izolovaném prostředí sandboxu.

Jednotná platforma

Mít k dispozici tolik nástrojů může vypadat jako další výzva. Jak spravovat tak robustní bezpečnostní systém?

Už jen množství výstrah, které denně přicházejí do IT týmů, administrátory přetěžuje. Podle studie March 2023 od společností IBM a Morning Consult, se členové týmu Bezpečnostních dohledových center (SOC) dostanou během běžného pracovního dne pouze k polovině výstrah, které mají prověřit.

Vhodné řešení, které umí některé procesy automatizovat, však může ve skutečnosti snížit **složitost bezpečnostních procesů**. Zde je několik příkladů:

- Noví uživatelé nemusí IT správce přidávat ručně v konzoli, ale jsou chráněni automaticky po vytvoření účtu.
- IT správci mohou být okamžitě informováni o nových výstrahách namísto neustálé kontroly situace v ovládacím panelu.
- Podezřelé soubory v karanténě lze snadno spravovat na jednom místě s možností je uvolnit/odstranit nebo je v případě potřeby dále samostatně prošetřit.
- Řešení umožňují správu více tenantů s desítkami tisíc uživatelů včetně účtů vytvořených v rámci dvou nejpoužívanějších platforem – Microsoft 365 a Google Workspace.

Jak ESET pomáhá

Dodatečné zabezpečení nemusí nutně zvyšovat složitost práce IT správce. Společnost ESET, která je již více než 30 let světovým lídrem v oblasti digitální bezpečnosti, si uvědomuje potřeby IT administrátorů a manažerů využívajících cloudové služby.

ESET Cloud Office Security poskytuje pokročilou ochranu pro aplikace Microsoft 365 a Google Workspace se všemi výše uvedenými funkcemi. Firmy tak mohou zavést strategii zaměřenou především na prevenci a minimalizovat počet způsobů, kterými útočníci mohou ohrozit firemní cloud a zároveň ulehčit IT administrátorům díky uživatelsky přívětivé správcovské konzoli.

My jsme ESET

Proaktivní ochrana.

Eliminujeme způsoby, kterými útočníci mohou proniknout do vaší organizace.

Buďte o krok napřed před známými i nově vznikajícími kybernetickými hrozbami a zaměřte se na prevenci. Bezpečnostní řešení od ESETu efektivně **kombinují umělou inteligenci a odborné znalosti našich expertů.**

Zažijte nejlepší ochranu ve své třídě díky **zpravodajství o hrozbách**, které je již více než 30 let hnacím motorem naší rozsáhlé sítě výzkumných a vývojových poboček vedených **uznávanými specialisty v oboru**. ESET chrání vaši firmu, aby mohla naplno využít potenciál technologií.

ZJISTIT VÍCE

ESET®

Digital Security
Progress. Protected.