

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **23** ze dne **7.12.2022**

Dvě třetiny malých a středních firem se v uplynulém roce setkaly s únikem dat

Společnost ESET zveřejnila závěry nejnovějšího průzkumu, SMB Digital Security Sentiment Report 2022, ve kterém zjišťovala vnímání kybernetických hrozeb u malých a středních firem (SMB). Vedoucích pracovníků společností v Evropě a Severní Americe se například ptala, s jakými incidenty se musely jejich firmy v uplynulých 12 měsících vypořádat a kde v rámci svého podnikání vnímají největší rizika do budoucna. Mezi hrozby, kterých se malé a střední podniky nejvíce obávají, přitom vedle ransomwaru čím dál častěji patří útoky dalšími škodlivými kódy či prostřednictvím webových stránek. Průzkumu se mezi ostatními evropskými zeměmi zúčastnili také vedoucí pracovníci z českých společností.

Společnost ESET zveřejnila zprávu SMB Digital Security Sentiment Report 2022, která se zaměřuje na oblast vnímání kybernetických bezpečnostních hrozeb ze strany malých a středních firem (SMB) v širším kontextu událostí posledních měsíců, které ovlivnily bezpečnost po celém světě. Průzkumu se zúčastnilo více než 1 200 vedoucích pracovníků společností v Evropě, včetně České republiky, a Severní Americe.

Podle údajů z průzkumu se více než dvě třetiny malých a středních firem setkaly v posledních 12 měsících s bezpečnostním incidentem souvisejícím s možným narušením bezpečnosti dat. To způsobilo postiženým firmám průměrnou škodu ve výši téměř 220 tisíc eur (5,36 milionu korun). Největší obavy v souvislosti s kybernetickými útoky mají pak společnosti ze ztráty dat (29 %). Přestože si vedoucí pracovníci uvědomují potenciální důsledky kybernetických útoků, až 70 % z nich uvedlo, že investice firem do zabezpečení neudrží krok s nedávnými změnami v režimech fungování společností, jako je například přechod na hybridní model práce.

„Aktuálně jsou v České republice největší hrozbou takzvané infostealery, škodlivé kódy, které se zaměřují na krádeže dat. Riziko představují především pro operační systém Windows. Útoky se navíc stále více objevují v češtině, což s ohledem na velikost České republiky a specifika češtiny jako jazyka, kterým se mluví z celosvětového hlediska jen na malém a omezeném území, svědčí o tom, že Česká republika je v současné době cílem, na který útočníci míří záměrně,“ říká Jakub Souček, výzkumný analytik z pražské pobočky společnosti ESET.

Nejobávanějšími hrozbami jsou malware a útoky přes webové stránky

Data z nejnovější zprávy o stavu kybernetické bezpečnosti ve světě ESET Threat Report ukazují 20% meziroční nárůst detekcí hrozeb. Přitom až 83 % dotázaných vedoucích pracovníků ve firmách se domnívá, že „kybernetická válka je velmi reálnou hrozbou, která může postihnout každého“, což naznačuje, že stále rostoucí hrozby mají významný dopad na myšlení malých a středních podniků. Dále se také až 74 % malých a středních firem domnívá, že jsou vůči kybernetickým útokům na rozdíl od velkých korporací daleko zranitelnější.

Respondenti se v příštích 12 měsících nejvíce obávají následujících bezpečnostních problémů:

- Malware – obává se celkem 70 % dotázaných, se statisticky významným rozdílem ve Švédsku (50 %).
- Útoky prostřednictvím webových stránek – celkem 67 % dotázaných, se statisticky významným rozdílem ve Španělsku (87 %).

MEATEST spol. s r.o. - sdělení pověřence pro ochranu osobních údajů číslo **23** ze dne **7.12.2022**

- Ransomware – celkem 65 % dotázaných, statisticky významný rozdíl byl zaznamenán v Dánsku (80 %).
- Bezpečnostní problémy třetích stran – celkem 64 % dotázaných.
- Útoky DDoS – celkem 60 % dotázaných.
- Útoky přes protokol RDP (Remote Desktop Protocol) – celkově 60 % dotázaných, se statisticky významným rozdílem ve Španělsku (79 %).

„Mezi obávané útoky prostřednictvím webových stránek může patřit například takzvaný BITB útok, z anglického názvu Browser in the Browser. Nejedná se o nový typ útoku, ale v poslední době roste jeho popularita – jednak proto, že roste také popularita využívání webových služeb, a také proto, že vytvořit legitimně vypadající přihlašovací dialog je pro útočníky díky moderním technologiím stále jednodušší,“ vysvětluje Souček. „Nejčastěji se setkáváme s podvrženými přihlašovacími stránkami na webové služby Microsoft, Facebook a Google. Mezi hlavní dopady a rizika tohoto útoku pak patří kompromitace účtu u dotčené webové služby, tedy ztráta přihlašovacích údajů. Následkem toho může dojít ke zneužití identity, profilu či účtu. Kromě ztráty osobních dat se můžeme setkat s tím, že prostřednictvím zcizených profilů dochází ke spamování našich kontaktů, phishingu, snahám o vylákání peněz a podobně,“ dodává Souček.

Dle dalších zjištění vycházejících z aktuální zprávy si společnosti nejsou příliš jisté svou kybernetickou odolností. Pouze 48 % respondentů uvedlo, že se cítí do určité míry jistě nebo velmi jistě, pokud jde o jejich kybernetickou odolnost. Zajímavé je, že skandinávské země (32 %) jsou v tomto ohledu výrazně méně sebevědomé než zbytek Evropy a Severní Ameriky (49 %).

Až 43 % dotázaných vedoucích pracovníků považuje za nejvýznamnější faktor, který aktuálně v období války na Ukrajině a pokračující práce na dálku po pandemii přispívá k riziku kybernetického útoku, nedostatečné povědomí zaměstnanců o digitálních hrozbách. Mezi další hlavní faktory pak patří útoky na úrovni státu (37 %), zranitelnost partnerů a dodavatelského řetězce (34 %), trvalá hybridní práce (32 %) a používání protokolu vzdálené správy RDP (31 %).

„Podle poslední zprávy ESET Threat Report T2 výrazně vzrostly například rizika spojená s podvodnou komunikací. A ačkoli vidíme, že útoky prostřednictvím ransomwaru aktuálně spíše klesají, podle našeho pozorování zároveň roste míra jejich sofistikovanosti. Všechny aktuální hrozby, ať už útoky ransomwarem nebo phishingové podvody, kladou větší nároky na proškolení zaměstnanců firem, protože každý zaměstnanec se zařízením připojeným k internetu může potenciálně vpustit útočníky k firemním datům,“ shrnuje Souček z ESETu.

Zdroj: ESET