

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **37** ze dne **18.5.2023**

Antivirový program Microsoft Defender označoval legitimní adresy na webu jako škodlivé

Vývojáři Microsoftu řešili další nepříjemný problém – antivirový program Defender totiž mylně označoval legitimní odkazy, směřující například na Google či Zoom, jako škodlivé. Microsoft následně na sociální síti Twitter tento problém potvrdil a uvedl, že pracuje na jeho vyřešení, informoval Bleeping Computer.

"Prověřujeme problém, kdy jsou legitimní odkazy URL službou Microsoft Defender nesprávně označovány jako škodlivé. Kromě toho se u některých upozornění nezobrazuje obsah dle očekávání. Další podrobnosti naleznete pod číslem DZ534539 v centru pro správu," uvedl účet Microsoft 365 Status.

Splašený antivir

Po necelých dvou hodinách Microsoft konstatoval, že přes falešně pozitivní výstrahy mají uživatelé k webům na postižených adresách přístup. *"Zjišťujeme, proč a která část služby nesprávně identifikuje legitimní adresy URL jako škodlivé. Prověřujeme diagnostické informace, jako jsou síťové telemetrické údaje, abychom zjistili hlavní příčinu a našli řešení."*

V aktualizaci na portále Microsoft 365 Admin Center redmondská společnost zmínila, že administrátoři budou pravděpodobně dostávat zvýšený počet e-mailových zpráv s vysokou závažností, ve kterých se uvádí, že *"bylo zjištěno potenciálně škodlivé kliknutí na adresu URL"*. Kromě toho také potvrdila informaci o problémech s přístupem k podrobnostem o výstrahách po kliknutí na odkaz *"Zobrazit výstrahy"* v těchto e-mailech.

Příčina odhalena

Během pátrání po příčinách falešných poplachů se ukázalo, že za vším stojí nedávná aktualizace funkce SafeLinks. Jedná se o součást Microsoft Defenderu pro Office 365, která kontroluje, zda adresy v e-mailových zprávách nesměřují na potenciálně škodlivý obsah. Cílem je snaha chránit před škodlivými odkazy používanými při phishingových útocích.

"Zjistili jsme, že nedávné úpravy funkce SafeLinks vedly k falešným upozorněním. Následně jsme tyto úpravy vrátili, čímž jsme problém odstranili," uvedl Microsoft na Twitteru. Od nahlášení problému do jeho vyřešení tak uplynulo necelých sedm hodin.

Dva měsíce před tímto incidentem musel Microsoft řešit jiný problém týkající se jeho antiviru. Uživatelé tehdy hlásili, že Defender for Endpoint samovolně odstraňoval ikony a zástupce aplikací z hlavního panelu a nabídky Start ve Windows 10 i Windows 11.

Zdroj: Živě.cz