Nárůst kyberútoků na malé a střední firmy přes Excel

4.7.2024 - Darko Natalic | PROTEXT

Podle nejnovější, dnes zveřejněné zprávy společnosti Kaspersky, jsou malé a střední podniky stále častěji cílem kyberzločinců. Nejrozšířenější formou útoku zůstávají trojské koně, které jsou obzvláště nebezpečné, protože často napodobují legitimní software. Jejich přizpůsobivost a schopnost vyhnout se tradičním bezpečnostním opatřením z nich činí rozšířený a účinný nástroj záškodníků.

Společnost Kaspersky zaznamenala v období od ledna do dubna 2024 celkem 100.465 útoků trojských koní, což představuje 7% nárůst oproti stejnému období v roce 2023 a o 83.145 útoků více než u další největší naměřené hrozby typu DangerousObjects, u které bylo zaznamenáno 17.320 útoků – o 6994 více než v roce 2023.

Na pozici prvního kanálu útoku se vrátil Microsoft Excel, který se mezi lety 2023 a 2024 posunul ze čtvrtého na první místo. Na druhém místě byl Microsoft Word a na třetím místě skončily Microsoft PowerPoint a Salesforce.

Analytici společnosti Kaspersky prozkoumali telemetrii Kaspersky Security Network (KSN) v souvislosti s vybranými aplikacemi, jako jsou MS Office, MS Teams, Skype a další programy používané v malých a středních podnicích. To jim umožnilo získat informace o hrozbách v tomto sektoru a zjistit výskyt škodlivých souborů a nežádoucího softwaru s vazbou na sledované aplikace, jakož i počet uživatelů napadených těmito soubory.

Pro malé a střední podniky je stálou hrozbou phishing a může pro ně mít katastrofální následky. Zaměstnanci dostávají odkazy na zdánlivě známé a legitimní webové stránky, které napodobují oblíbené služby, firemní portály a platformy online bankovnictví. Jakmile se cíl přihlásí, nechtěně tím prozradí uživatelská jména a hesla kyberzločincům nebo spustí automatické kybernetické útoky, čímž ohrozí citlivé informace a bezpečnost podniku.

„Naše průzkumy ukazují, že pro podniky zůstává významnou zranitelností lidská chyba. Všudypřítomné používání aplikace Microsoft Excel v kancelářských prostředích navíc poskytuje živnou půdu pro kyberzločince, kteří mohou skrývat a šířit škodlivá data ve velkých souborech, jež jsou pak sdíleny v rámci celého podniku,“ uvádí Vasilij Kolesnikov, expert na kybernetickou bezpečnost ve společnosti Kaspersky.

Ochrana sektoru malých a středních podniků před rostoucími zájmy kyberzločinců má zásadní význam pro globální hospodářské, sociální a environmentální výzvy, které doléhají zejména na rozvíjející se ekonomiky. Podle údajů OSN je 7 z 10 pracovních míst v těchto ekonomikách v sektoru malých a středních podniků, které mají ztížený přístup k financování, což jim znesnadňuje také ochranu před kyberútoky.

Celou zprávu si můžete přečíst na Securelist.com.

Při ochraně vašeho podniku před kybernetickými hrozbami mějte na paměti následující doporučení:

• K ochraně před širokou škálou hrozeb použijte EDR a XDR řešení z produktové řady Kaspersky Next, která dokážou zajistit ochranu v reálném čase, přehled o hrozbách, jejich vyšetřování a příslušné reakce na ně pro všechny typy organizací.

• Zapojte zaměstnance jako další vrstvu ochrany proti kybernetickým útokům souvisejícím s lidským faktorem pomocí řešení Kaspersky Automated Security Awareness Platform. To lidem vštěpuje pravidla bezpečného chování na internetu a obsahuje také nácvik simulovaného phishingového útoku, aby se naučili, jak rozpoznat phishingové e-maily a další nástrahy sociálního inženýrství.

• Optimalizujte pracovní zátěž poddimenzovaných oddělení IT pomocí služby Kaspersky Professional Services. Odborníci společnosti Kaspersky posoudí stav vašeho současného zabezpečení IT a pak rychle a přesně nasadí a nakonfigurují software Kaspersky, aby zajistili hladký nepřetržitý chod vašeho podniku. Rychlejší řešení technických incidentů a jejich menší dopad na provozní procesy nabízí služba Kaspersky Premium Support.

• Zajistěte svým zaměstnancům základní školení o hygieně kybernetické bezpečnosti. Proveďte simulovaný phishingový útok, abyste se ujistili, že vědí, jak rozeznat phishingové e-maily.

• Nastavte zásady přístupu k firemním prostředkům, včetně e-mailových schránek, sdílených složek a online dokumentů. Udržujte je aktuální a zrušte příslušný přístup, když zaměstnanec již tyto údaje ke své práci nepotřebuje nebo odejde. Používejte software pro zprostředkování zabezpečení přístupu ke cloudu, který vám pomůže spravovat a monitorovat činnost zaměstnanců v rámci cloudových služeb a prosazovat bezpečnostní pravidla.

https://www.ceskenoviny.cz/tiskove/zpravy/kaspersky-narust-kyberutoku-na-male-a-stredni-firmy-pres-excel/2539980