Hackeři opět útočí na Windows Exchange server, v Česku je jich zranitelných na 600

23.6.2023 - | BDO

Windows Exchange server se potýká s novou vlnou útoků.

Hackeři pomocí zranitelnosti v zabezpečení Proxyshell zasílají phishingové zprávy obsahující malware. E-maily psané v angličtině přicházejí ze skutečných stránek uživatelů a je takřka nemožné je zachytit antispamovými filtry. Upozornil na to Národní úřad pro kybernetickou bezpečnost s tím, že momentálně je v Česku na 600 serverů Windows Exchange bez aktualizací, čímž se útokům vystavují. Podle poradenské společnosti BDO je mezi zaměstnanci firem a institucí stále nedostatečné povědomí o phishingových útocích a až třetina pracovníků je schopna zadat na podvodné stránky své přihlašovací údaje

Zranitelnosti Windows Exchange serveru mají souhrnné označení Proxyshell. Pokud je útočníci zneužijí v kombinaci, mohou vzdáleně získat plnou kontrolu nad serverem. Přes předchozí upozornění je podle NÚKIBu v Česku stále na 600 serverů, u nichž nebyla provedena aktualizace, která tyto chyby opravuje. „Útočníci, kteří získají přístup k e-mailovým schránkám na serveru, mohou navázat na předchozí legitimní konverzace. Následně ze schránek rozesílají phishingové maily s odkazy na stažení malwaru. Pokud uživatel soubor spustí na svém počítači, proběhne kompromitace jeho zařízení a také potenciálně další zařízení v počítačové síti. Technicky vzato, kam je umožněn přístup v rámci sítě, tam se může malware šířit," vysvětluje Martin Hořický, expert na kyberbezpečnost z poradenské společnosti BDO. Národní úřad pro kybernetickou bezpečnost doporučuje všem správcům Exchange Serverů bezodkladnou aktualizaci na verzi z července letošního roku nebo novější.

Dva z pěti zaměstnanců kliknou na odkaz, třetina se pokusí přihlásit

V souvislosti s phishingovými kampaněmi upozorňují odborníci na nízkou připravenost zaměstnanců tyto hrozby rozeznat. Dokládá to i případová studie poradenské společnosti BDO, která několik podobných kampaní připravila. E-maily pracovníky lákaly k registraci do soutěže, upozorňovaly na nová koronavirová opatření s odkazem na přihlašovací formulář nebo žádaly o vyplnění docházky nových zaměstnanců. „Ze stovky náhodně vybraných zaměstnanců firem jich dvě pětiny klikly na odkaz v přiložených souborech a třetina se dokonce do formulářů pokusila přihlásit. Nemalé procento uživatelů provedlo zadání údajů opakovaně. Obdobné praktiky přitom využívají útočníci i v kampaních zaměřených na Windows Exchange Servery, kde se objevují odkazy na nezaplacené faktury nebo pozvánky. Firmy i instituce by měly dbát na pravidelná školení svých zaměstnanců a budovat u nich obezřetnost v této oblasti. Principem těchto útoků je vyvolat pocit nutnosti otevřít daný odkaz, či přílohu. Nutnost, či zvědavost je velmi dobrým nástrojem. Pokud je totiž uživatel vystaven tlaku, mnohdy neuvažuje racionálně," uzavírá expert na kyberbezpečnost z BDO Martin Hořický.

http://www.bdo.cz/cs-cz/novinky/2021/hackeri-opet-utoci-na-windows-exchange-server,-v-cesku-je-jich-zranitelnych-na-600