Miskonfigurace v Exchange Online

> Aktualizováno 23. srpna: Podle dalších informací poskytnutých belgickým Centre for Cybersecurity Belgium společnost Microsoft nebude tento problém proaktivně řešit – řešení problému je na každém zákazníkovi, který musí aplikovat vhodná opatření. Informace o této zranitelnosti by měly být zveřejněny v průběhu měsíce září – poté se dá očekávat masivnější zneužívání pro rozesílání phisngových zpráv, případně pro obcházení bezpečnostních řešení a zasílání škodlivých souborů.

Upozorňujeme na miskonfiguraci v produktu společnosti Microsoft Exchange Online (někdy označované jako Microsoft 365, MS365 nebo O365), kvůli níž může potenciální útočník podvrhnout odesilatele e-mailové zprávy a obejít ochrany SPF, DKIM a DMARC.

Tato zranitelnost byla nahlášena Centre for Cybersecurity Belgium (CCB), přiložený dokument (v angličtině) obsahuje nejen technický popis miskonfiguace, ale takté způsob, jak tuto miskonfiguraci opravit a taktéž jak ověřit, že oprava byla úspěšná. Podle CCB se tato zranitelnost týká přibližně poloviny belgických subjektů ze sektoru kritické infrastruktury. **NÚKIB potvrzuje reálnost této zranitelnosti.**

Dovolujeme si připomenout, že zmíněný dokument je vám sdílen s klasifikací TLP:AMBER:

> Informace může být sdílena v rámci organizace příjemce a jejím partnerům, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.

Dále připomínáme, že NÚKIB již v říjnu 2021 vydal ochranné opatření, které nařizuje správcům e-mailových systémů podléhající regulaci dle zákona o kybernetické bezpečnosti využívat technologie SPF, DKIM a DMARC jak při příjmu, tak při odesílání e-mailových zpráv.

Klasifikace

TLP:AMBER

Autor

Národní úřad pro kybernetickou a informační bezpečnost

Datum

07. 08. 2024

Přílohy

Misconfiguration in Microsoft mail flow.pdf

Reakce

7