UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH
Centrum informačných a komunikačných technológií

Úsek informačnej a kybernetickej bezpečnosti
Tím na riešenie počítačových bezpečnostných incidentov (CSIRT-UPJS)
Šrobárova 2, 041 80 Košice
VoIP: +421 (055) 234 2425, IČO: 00397768
csirt@upjs.sk, https://csirt.upjs.sk/

TLP:GREEN

Stanovisko k bezpečnostnému riziku spojenému s preposielaním emailových správ do externých emailových služieb

Preposielanie emailových správ (emails forwarding) je funkcionalita emailového servera, ktorá umožňuje používateľom nastaviť preposlanie všetkých emailových správ do externej emailovej služby (napr. zo služby Office365 do služby Gmail). V rámci univerzity je táto funkcionalita povolená.

Na jeseň 2020 došlo k zmene používania tejto funkcionality. Spoločnosť Microsoft z bezpečnostných dôvodov zablokovala túto funkcionalitu (predvolené nastavenie) a umožnila administrátorom ju následne povoliť[1,2]. Zablokovanie preposielania emailových správ sa u používateľov prejavuje obdržaním odpovede v nasledujúcom znení:

550 5.7.520 Access denied, Your organization does not allow external forwarding. Please contact your administrator for further assistance. AS(7555)

Preposielanie emailových správ predstavuje zaujímavú funkcionalitu pre používateľov, ale súčasne vysoké bezpečnostné riziko pre organizáciu[3]. Dôvodom je možné zverejnenie citlivých informácií, vrátane osobných údajov. Týmto môže dôjsť k porušeniu povinností organizácie v oblasti ochrany osobných údajov, resp. môže dôjsť k úniku iných citlivých údajov. V rámci emailových správ môže dochádzať k zasielaniu veľkého množstva osobných údajov, či už z oblasti personalistiky alebo z oblasti vzdelávania.

Preposielanie emailových správ je bežnou technikou útočníkov v rámci zberu emailových adries (Email Collection: Email Forwarding Rule)[4]. Útočníci môžu zneužívať pravidlá zasielania emailových správ na sledovanie činnosti obete, odcudzenie informácií a ďalšie získavanie informácií o obeti alebo organizácii obete, ktoré môžu použiť ako súčasť ďalších zneužití alebo operácií[5]. Napríklad odoslanie emailovej správy obsahujúcej informáciu o obnovení hesla do

[1] https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/external-email-forwarding?view=o365-worldwide
[2] https://www.linkedin.com/pulse/why-email-forwarding-office-365-doesnt-work-anymore-rand-morimoto/
[3] https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/external-email-forwarding?view=o365-worldwide
[4] https://attack.mitre.org/techniques/T1114/003/
[5] https://us-cert.cisa.gov/ncas/alerts/TA18-086A

Úsek informačnej a kybernetickej bezpečnosti
Tím na riešenie počítačových bezpečnostných incidentov (CSIRT-UPJS)
Šrobárova 2, 041 80 Košice
VoIP: +421 (055) 234 2425, IČO: 00397768
csirt@upjs.sk, https://csirt.upjs.sk/

TLP:GREEN

interných systémov organizácie[6]. Z týchto dôvodov nie je odporúčané mať túto funkcionalitu zapnutú[7].

Súčasne vnútorný predpis univerzity - Príkaz rektora č. 12/2015 na zjednotenie formátu e-mailových adries na Univerzite Pavla Jozefa Šafárika v Košiciach a jej súčastiach upravuje používanie univerzitných emailových adries. Podľa odseku 3 tohto príkazu zamestnanci a študenti univerzity majú povinnosť pre pracovné a študijné účely na UPJŠ používať výlučne univerzitnú emailovú adresu. Máme za to, že preposielanie emailových správ a používanie iných emailových adries ako univerzitných, je v rozpore s týmto ustanovením.

Vzhľadom na vyššie uvedené, **vysoko odporúčame minimalizovať bezpečnostné riziká** spojené s preposielaním emailových správ k externým poskytovateľom emailových služieb, a to **zakázaním tejto funkcionality v rámci organizácie**. Iné bezpečnostné opatrenia (ako napr. šifrovanie emailovej komunikácie) len minimalizujú bezpečnostné riziko, keďže neumožňujú zabezpečiť všetky prípady zasielaných citlivých údajov (emailové správy prijaté používateľom, automaticky generované emailové správy obsahujúce prihlasovacie údaje a pod.).

V Košiciach dňa 31.5.2021.

Pavol Sokol
2021.05.31
12:04:11
+02'00'

RNDr. JUDr. Pavol Sokol, PhD.

vedúci UIKB ClaKT

[6] https://thibaultchatiron.fr/2020/07/29/office-365-atp-external-email-forwarding-controls-and-policy-change/
[7] https://www.linkedin.com/pulse/why-email-forwarding-office-365-doesnt-work-anymore-rand-morimoto/