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

Opinion on the security risk associated with forwarding email messages to external email services

Email forwarding is an email server functionality that allows users to set up the forwarding of all email messages to an external email service (e.g., from Office365 to Gmail). This functionality is enabled within the university.

In autumn of 2020, there was a change in the use of this functionality. For security reasons, Microsoft has disabled this functionality (the default setting) and allowed administrators to subsequently enable it.[1,2]. Blocking the forwarding of email messages is reflected in users receiving a reply as follows:

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

Email forwarding represents an interesting functionality for users, but at the same time a high security risk for the organization.[3]The reason may be the disclosure of sensitive information, including personal data. This may lead to a breach of the organization's obligations in the field of personal data protection, resp. other sensitive data may be leaked. E-mail messages can send large amounts of personal data, whether in the field of human resources or education.

Forwarding email messages is a common technique for attackers to collect email addresses (Email Collection: Email Forwarding Rulle)[4]. Attackers may abuse e-mail policies to track victim's activities, steal information, and otherwise obtain information about the victim or the victim's organization that they may use as part of other abuses or operations[5].

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

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

For example, sending an email message containing password recovery information to an organization's internal systems[6]. For these reasons, it is not recommended to have this functionality turned on[7].

At the same time, the internal regulations of the university - Rector's order no. 12/2015 to unify the format of email addresses at Pavol Jozef Šafárik University in Košice and its parts regulates the use of university email addresses. According to paragraph 3 of this order, the employees and students of the university are obliged to use exclusively the university email address for work and study purposes at UPJŠ. We believe that the forwarding of email messages and the use of email addresses other than university addresses is contrary to this provision.

In view of the above, **we highly recommend minimizing the security risks** associated with forwarding email messages to external email service providers **by disabling this functionality within the organization**. Other security measures (such as encryption of email communication) only minimize the security risk, as they do not allow to secure all cases of sent sensitive data (email messages received by the user, automatically generated email messages containing login data, etc.).

In Košice 31.5.2021.

RNDr. JUDr. Pavol Sokol, PhD.

Head of UIKB CIaKT

[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/