Top ten ways to protect Office 365 from cyber attacks

1) Enable logging

We recommend that you enable mailbox audit logging. It is very limited what can be detected after an attack, if logging is not enabled. When enabling mailbox audit logging, you can tailor what is to be logged. You should, as a minimum, enable default logging. Audit logs are saved for 90 days and no additional licence is required.

2) Manage your legacy protocols

In Office 365, the following protocols are enabled by default: SMTP, POP3, IMAP, Exchange Web Services (EWS) and Exchange ActiveSync. Cyber criminals use the above protocols to, among other things, conduct password spraying attacks. The challenge of these protocols is that they are so old that they do not support multi-factor authentication ('MFA').

Microsoft recommends disabling all legacy protocols. However, before you do that, you should check whether any services are using SMTP or IMAP, etc.

Specifically, IMAP may be problematic, as this is currently the only way to access shared mailboxes via mobile phones.

3) Enable multi-factor authentication (MFA)

MFA is an extra security layer which in addition to a username and password requires an additional security factor, such as a PIN. Such extra security layer can be added at no additional licence costs. We recommend that all users use MFA whenever possible.

4) Establish rules on conditional access

It is possible to create custom rules for condition access to either force MFA login or not to request MFA login. If the user is using a trusted enrolled device the user may not need to authenticated with MFA. But if the user e.g. logs in from another country and detected by the 'impossible travel' feature then the user will be forced to login using MFA.

Impossible travel is, for instance, where the user logs in somewhere in Denmark via a Danish IP address and shortly afterwards logs in from another country to which it would be impossible for the user to travel in the time period elapsed between the first and the second login attempt. This may be a false positive. In such cases, the user will just need to login using an additional MFA login.

The conditional access function is not just for Office 365, but applies to all Microsoft Azure applications. The conditional access function requires an extra licence.

5) Use the Microsoft Office 365 Secure Score portal

Office 365 Secure Score is a portal where Office 365 admins can check their security score compared to other companies.

You are not supposed to strive for a top score in Secure Score. Instead, you should make efforts to reach as high a score as possible that matches your type of company. Be aware that the implementation of some of the improvements suggested will require you to purchase extra licences.

6) Get the right licence

We often find that many companies do not have the right licence in case of an attack.

Features with the cheapest licences, for instance MFA and audit logging, will be adequate to a large extent, however, anti-phishing functions, safe links and safe attachments are only available with certain types of licences. Also, many of the security solutions in the portal require an extra licence.

We recommend that you consider purchasing additional Office 365 security products. If you can prevent security incidents from happening, you will save a lot of time, money and problems.

It is our experience, that the possibility of solving a security incident increases if you have licences for the security products. At present, these include:

Office 365 Enterprise E3/E5 and Azure AD P1/P2 licences.

7) Evaluate your backup solution

Evaluate the backup solution delivered by Microsoft is sufficient and supports your internal SLA. There are many other vendors who offer backup solutions for Office 365, OneDrive for Business, SharePoint Online, etc.

8) Implement SPF, DKIM and DMARC security measures

These security measures protect the recipient against e-mail spoofing. We recommend that you implement these security measures as they make it more difficult to perform e-mail spoofing.

Sender Policy Framework ('SPF')

SPF is an e-mail validation standard designed to prevent e-mail spoofing. SPF allows the company to specify which mail servers are allowed to send e-mails for the company's domain.

DomainKeys Identified Mail ('DKIM')

In short, DKIM is a method to verify that e-mails between a sender and a recipient are sent from the correct source. DKIM uses a digital signature that is added to the e-mail header by the mail server from which the e-mail is sent.

A DNS record is created in the company's external DNS server which contains the public key for the digital signature in the e-mail header.

Domain Message Authentication Reporting & Conformance ('DMARC')

DMARC checks if the sender uses both or one of the above measures, and based on the result, it is assessed what needs to be done if the e-mail cannot be verified.

Based on the result of the SPF and DKIM checks, DMARC determines if the email should be delivered, quarantined or deleted, as specified in the underlying rules.

Hvis e-mailen ikke kan verificeres gennem ovenstående, kigger mailsystemet på DMARC-manualen og afgør derfra, om mailen skal i karantæne, eller om den skal fjernes helt.

9) Improve awareness

We recommend that you improve your employees' awareness in respect of e.g. phishing e-mails. It may include links to be clicked, invoices to be paid and pages that request a username and password.

Also, your employees must be instructed not to approve MFA, unless they have requested it themselves. Learn more about awareness here (https://www.pwc.dk/cyberaware)

10) Procedures

We recommend that you make explicit agreements on the invoicing procedure. For example, e-mails forwarded by the managing director must always be followed by a phone call.

Invoices that seem different must always be controlled. For instance, VAT may be missing or incorrect, the invoice looks odd or the wording is incorrect (Google Translate).

Establish clear rules and procedures for the summer holidays, etc. In our experience, cyber criminals often take advantage of holidays when the persons who are usually involved in the payment of invoices are on holiday.

Contact

Mads Nørgaard Madsen
Partner
M. + 45 2811 1592
E. mads.norgaard.madsen@pwc.com

Thomas Grandjean
Director
M. + 45 2811 1792
E. thomas.grandjean@pwc.com