MAKING SENSE OF

The security threat to Office 365

Office 365 is ubiquitous throughout the digital landscape. With email being one of the most common forms of attack, the need for vigilance has never been greater.

Most attacks come from a huge array of re-invented phishing attacks, where most emails usually appear to come from a known source. It only takes an attacker to discover a single password within the whole network to gain access. The concept is so simple; the consequences can be disastrous.

Email also introduces a web browser vector for the downloading of malware. This very commonly manifests itself as crypto ransomware, by supplying the recipient a link in the email body redirecting the user to a website hosting the malicious payload.

Office 365 (O365) is a cloud-based business system used for email, productivity, and collaboration. This platform and its data are a popular breach target for key threat actors who wish to extract data, elevate their privileges, abuse resources, or delete data. There is also an insider risk whereby so called 'trusted employees' take steps to exfiltrate/spill or delete sensitive data or obtain persistent access by building in backdoor accounts.

Weak passwords

When it comes to attacks on O365, one of the main issues is weak credentials. Password re-use is a good example of poor security practice. By using the same password across several different platforms, such as email, social media or network sign-ins only increases the chances of hackers gaining access.

Using weak passwords, or password re-use is a recipe for serious disruption. Unless you specifically set your accounts for Multi Factor Authentication (MFA), O365 will use the standard username and password option, which these days is not adequate enough.

MFA is an available option, although it is not provided as a default. With the sophistication and skilled application of threat actors increasing by the day, MFA is absolutely necessary to keep your email secure.

Electing not to use MFA is considered unacceptable for any form of remote access including hosted email.

Once access is obtained

The issue doesn't lie in gaining access, the issue lies within what the attacker does once they are in. The following points outline the damage an attacker can cause once they gain access to your network:

1. Scour compromised in-box for confidential data, personal data, any transactional data that they can abuse.
2. Email all your contacts and try and abuse your position of trust.
3. Begin monitoring your email communications looking for something they can abuse.
4. Once they have figured out how you receive money & pay money, they will usually send an email from you to one of those parties asking them to update the banking details they have on file to one the attacker controls, and the next transaction will be paid into the wrong account.
5. Use Skype and other O365 services to steal further data or increase credibility with real-time chat.
6. Attack multiple users from the same company.
7. The attacker can sit idle for extended periods and wait for the perfect moment to pounce.

Moving forward

Traditional attachments in email (zip files, macro enabled documents, etc.) remain as attack vectors and should ideally be mitigated through advanced malware detection including sandbox scanning where the attachments is executed, scanned and analysed before passing onto the recipient.

Some points to keep in mind are:

- Always use MFA for all remote access including email access from all types of devices.
- Add in additional layers of protection such as Adaptive Access Controls including Geo Blocking (knowing where your legitimate users are) and User Heuristics (device, browser, usage patterns).
- Use gateway services independent of the O365 platform that provides an immutable archive.
- Use advanced gateway security controls to be less susceptible to downloading malware. This includes URL Re-Writing (so the user doesn't connect directly to the internet site) and sandbox scanning.
- Implement DNS Security controls to prevent spoofing and sign emails (SPF, DKIM, DMARC)
- Harden your O365 implementation. The out of the box settings are not adequate for security or forensics.

Contact us to discuss how our security solutions can help protect your most vital assets

☎ 1300 922 923
+61 (2) 9290 4444

✉ info@senseofsecurity.com.au

senseofsecurity.com.au