National Cyber Security Centre

Working Remotely: Securing Microsoft Azure and Office 365

New Zealand's National Cyber Security Centre is hosted within the Government Communications Security Bureau

April 2020

Staying Secure in the Cloud

Microsoft Azure and Office 365 (O365) are cloud services used by many organisations providing remote working solutions for staff. Some organisations already have a well-established O365 security posture, but for those who are required to stand it up in a hurry, this document provides straightforward starting guidance to securing the O365 environment. In the long term, however, a comprehensive cyber security programme will be required to ensure ongoing resilience.

Getting started

A good beginning point is the Centre for Internet Security (CIS) benchmarks[1] and Microsoft's own Secure Score tool[2]. These two resources provide suggested security settings that should be considered. It's important that you have a sound understanding of the advantages and drawbacks of each setting, and that you make a record of your decisions to enable them or not.

Email is still a significant vector for threat actors. Priority should be placed on reviewing email security and following Microsoft and CIS advice for securing O365 Outlook and Exchange Online. Some government agencies may require additional security settings to be applied, depending on the level of national security classification in use.

Sharing is a popular feature of cloud services, and managing this function is a critical security control. Understand the default sharing settings and adjust these as necessary, either globally or on a per-service basis (such as for OneDrive or SharePoint Online). Monitor the services in use to discover those that are available but may not have been configured. If a service is not strictly necessary, consider disabling it to reduce management overheads.

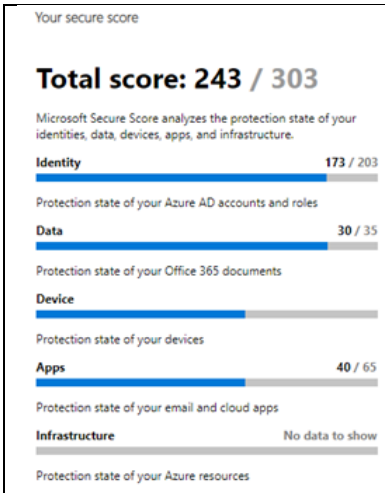
Set up a 'break glass' account to ensure access is retained during an emergency or major incident. This can be achieved by using the default [yourdomainhere].onmicrosoft.com assigned to an organisation by O365 at the time of initial setup. A member of your organisation's IT or security team should be required to read the messages in the message centre and develop reporting for the health and use of the organisation's Microsoft Azure or O365 tenancy. Check the billing section and ensure payments and payment methods are updated and active.

CIS benchmarks

The Centre for Internet Security offers a number of free downloadable documents that can be used to help secure both Microsoft Azure and O365. The Microsoft Office[3] and Azure[4] benchmark documents are particularly useful as they provide both recommended controls and the steps to implement them. These documents can be used as an excellent starting point to securing your O365 services, or to improve the security you already have in place.

O365 uses Azure Active Directory and other Azure services, so reading the Azure benchmark document in addition to the Microsoft Office document is recommended. Further information from Microsoft on the CIS benchmarks can be found here[5].

Microsoft Secure Score



The Microsoft Secure Score tool[2] is a useful way to gauge your current level of security in O365. Note that your secure score can take a day to update after any changes are made.

To begin with, focus on raising the identity score as high as is practically possible. As with most of the Microsoft tools and services, the specifics of the tool can change weekly, but we advise concentrating on identity to start with.

MFA (multi-factor authentication) should also be a priority. After implementing MFA, turn on the security settings you can easily and quickly activate.

Come back to the secure score tool on a regular basis and make continuous improvements to harden your O365 security.

Make efforts to raise your score and monitor for security decreases; cloud environments are dynamic, and security is rarely 'set and forget'.

Multi-factor authentication (MFA)

Enable multi-factor authentication (MFA) as a priority. The MFA option we advise for Microsoft Azure and Office 365 to use is the Microsoft Authenticator application, with notifications active. It is possible to use the Microsoft Authenticator app for an account on more than one phone, which has benefits for service desks and administration while still providing good security.

Requiring re-authentication after a defined time period also improves security. However, a balance needs to be struck between that period and other conditional access and identity protection controls. If you set the re-authentication time too low (for example to 24 hours), this may result in your users not realising they need to re-authenticate and could disrupt time-sensitive processes like responding to email.

Support for Office 365

An investment in reducing support requirements can free up time to help you focus on security. Something as simple as enabling self-service password resets will provide users with a better experience and help to release critical IT resources.

For organisations with an internal Active Directory (AD) that synchronises with an Azure Active Directory (AAD), enable password write-back (sync). If this has not been set, it is important to ensure that users reset their passwords before working remotely. If this is not completed and their password expires, it is not easy to reset and creates interruption to their work.

Azure Active Directory (AAD) P2/E5 licensing

Active Directory Premium 2 combined with E5 licensing has additional benefits and offers access to improved functionality. For organisations with a base of lower-grade licenses such as E3 or Business, it can be well worth investing in an upgraded E5 license for key staff, administrators, and data or security people, so they have access to the premium tools and services.

At higher licensing levels, enabling access to services and features such as Microsoft's Lockbox (an additional content access and approval control) is as simple as moving a slider bar. Additionally, Microsoft's Sentinel is a cloud-based SIEM that is subscription-based and provides monitoring for those without existing SIEM or centralised logging.

Links

1. https://www.cisecurity.org/cis-benchmarks/
2. https://securescore.microsoft.com/
3. https://www.cisecurity.org/benchmark/microsoft_office/
4. https://www.cisecurity.org/benchmark/azure/
5. https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-cis-benchmark?view=o365-worldwide