Solving Common Security Challenges with Microsoft 365

By Janine Griffiths

Today, most organizations use a hybrid cloud model and Software as a Service (SaaS) solutions to accelerate innovation and online collaboration with others. To keep up with this trend, the Center for Internet Security (CIS) published correlating security foundation benchmarks, including the CIS Microsoft 365 (M365) Security Foundation Benchmark. This benchmark includes guides and best practices to help organizations securely configure their M365 environment and its core services such as Exchange, SharePoint, OneDrive, and Intune with Azure AD.

Most Common Security Challenges with M365

Since NCC Group works day in and day out with clients to assess these best practices, we thought it might be helpful to share the most common security issues related to M365 environments, and correlating recommendations for mitigating these issues that can be found in the CIS benchmark.

Building a secure foundation in the cloud requires organizations to update their systems to meet their new ways of work (think: the shared responsibility model) now and in the future, as the cloud landscape – and attacks against their systems, integrations, and applications - continue to evolve.

Spamming, phishing, password attacks, malicious apps and data exfiltration are 5 of the most common ways NCC have seen Microsoft 365 tenants get compromised in real-world environments.

The CIS foundation benchmark recommends about 80 configurations in 7 categories (Account/Authentication, Application Permissions, Data Management, Email Security/Exchange Online, Auditing, Storage, Mobile Device Management) to mitigate and prevent against the most common attacks.

Enabling built-in protections, using additional multi-factor authentication and

regular monitoring and report reviews are necessary to keep up with the continuous stream of threats. These and many more recommendations are all in the benchmark with additional details about the impact and rationale. This shows the complexity of the M365 security and leaves space for assessing the more advanced security settings.

Find Solutions to these Challenges Today

While some businesses evaluate and benchmark their cloud security independently, many lean on the expertise of third-party consultants, like NCC Group, to help them assess these best practices, and rest assured that their data is secure.

NCC Group has a robust and thorough M365 Assessment service that can conduct a comprehensive review of your cloud platform. If you want to find gaps in your current cloud platform and come up with the solutions to fix these security challenges, our experts can help your business today.

Contact Us

While we hope you found our outline of the most common issues beneficial, it is also important to note that these – and the CIS benchmarks overall – only provide a foundational level of security. If you are looking for a partner to assist in assessing CIS benchmarks and beyond, including company-specific assessments and recommendations to cover attack paths and avoid data leaks, contact us today.

Learn More

Read about the specifics of each issue and our related recommendations in the full research article on Shaking The Foundation of An Online Collaboration Tool by examining M365 Top 5 Attacks vs the CIS M365 Foundation Benchmark

nccgroup

Call us on:

General Number:
+44 161 209 5200
24/7 Emergency Incident Response:
+44 161 209 5148

Latest from
@NCCGroupplc

There's been no recent tweets