Strategic Cyber Security Report- August 2022 Edition

A Monthly summary of Strategic Information for Cyber Security Leaders

This is a series spun from a need I identified when talking to CISOs — as explained on the kick-off article, this series follows the format of:

What's Top of mind in 3 domains: People, Processes, Technology for CISOs.

Contents

People

- **M365 Adoption Score to replace Productivity Score**

Adoption Score, a set of metrics and tools for Microsoft 365 admins and IT leaders to improve the everyday experiences of their workforce and to help organizations get the most out of their investment in Microsoft 365. Adoption Score will start rolling out today to replace the former Productivity Score dashboards and introduce new features, new controls, new guidelines, and new purpose.

The solution ensures user privacy:

no one in a customer's organization can use Adoption Score to access data about how an individual user is using apps and services *in Microsoft 365.*

One of the firsts features available is called Time Trends.

Read more about it here.

For more information on managing the Adoption Score experience: Microsoft Adoption Score — Microsoft 365 admin.

For more information about Adoption Score, check out the Adoption Score overview video.

- How to better protect Wireless Devices

The latest post of our Tech Community Voices blog series, Microsoft Senior Product Marketing Manager Brooke Lynn Weenig talks with Jennifer Minella, Founder and Principal Advisor, Network Security, of Viszen Security and the author of "Wireless Security Architecture: Designing and Maintaining Secure Wireless for Enterprise." The thoughts below reflect Jennifer's views, not the views of Jennifer's employer, and are not legal advice. In this blog post, Jennifer talks about wireless security.

Read all the interview here.

Processes

- **Azure Threat Research Matrix**

The ATRM is primarily focused on AzureAD and Azure Resource TTPs. Due to the nature of AzureAD being used by other products, such as M365, occasionally it is necessary to include techniques or technique details that also pertain to other products.

The intent of the ATRM is not to replace MITRE ATT&CK, but to rather be an alternative for pure Azure Resource & AzureAD TTPs.

Finally, ATMR is free and agnostic:

The Azure Threat Research Matrix is meant to be product-agnostic, meaning specific detection queries are for technologies within Azure by default and not an additional, paid solution.

Access the Azure Threat Research Matrix here: aka.ms/ATMR

Read more here.

- **Data Governance — 5 tips for holistic data protection**

Microsoft Purview is a Data governance platform included in Microsoft E5 and E5 compliance. Customers should make use of its Data labelling for information protection and allows for a unified data governance platform for all Enterprise needs.

The 5 tips are:

1. Create a data map of all your data assets
2. Build a decision and accountability framework
3. Monitor access and use policies
4. Track both structured and unstructured data
5. Delete data that's no longer needed

Read the full article with more details here.

- **NZ Cyber Resilience Framework by CERT**

What is the NZ Cyber Resilience Framework?

"It's a framework or an index that we're looking to develop that can be used by private, public and individuals. It's not a cybersecurity framework where you have a tick box, and you go, Oh, I need to do these steps to be a bit more," says Lopez.

The article explains further:

CERT NZ has been developing this framework for about a year, and in its initial research, it hasn't found anything similar in the international landscape. Only indexes or systems based on public information are currently available and there isn't anything that is as comprehensive as what the government agency wants to develop. Lopez says many of the things that exist out there are also quite technical. They don't necessarily think about the social impact a cyber attack can have on an individual and a community.

CERT NZ is looking for help — a good thing for professionals and organizations wanting to be part of the development of said framework:

For businesses and industries who see the framework as useful, Lopez is asking them to reach out to CERT NZ. She says the agency is currently in the phase of seeking to understand what the problem is and how it can put the framework or the index together. CERT NZ wants it to be usable for anybody, whether it be an individual or business, to understand if there's a particular weakness or strength in their industry.

More on the article by Securitybrief.

Technology

Some relevant information related to technology and threats are:

- **Newly discovered technique to maintain persistence in compromised environments is being used by Threat actors. Discovered by MSTIC, they named it "MagicWeb"**

Microsoft security researchers have discovered a post-compromise capability we're calling MagicWeb, which is used by a threat actor we track as NOBELIUM to maintain persistent access to compromised environments.

How MagicWeb works:

MagicWeb is a post-compromise malware that can only be deployed by a threat actor after gaining highly privileged access to an environment and moving laterally to an AD FS server. To achieve their goal of maintaining persistent access to an environment by validating authentication for any user account on the AD FS server, NOBELIUM created a backdoored DLL by copying the legitimate Microsoft.IdentityServer.Diagnostics.dll *file used in AD FS operations.*

How to mitigate:

It's critical to treat your AD FS servers as a Tier 0 asset, protecting them with the same protections you would apply to a domain controller or other critical security infrastructure. AD FS servers provide authentication to configured relying parties, so an attacker who gains administrative access to an AD FS server can achieve total control of authentication to configured relying parties (include Azure AD tenants configured to use the AD FS server). Practicing credential hygiene is critical for protecting and preventing the exposure of highly privileged administrator accounts. This especially applies on more easily compromised systems like workstations with controls like logon restrictions and preventing lateral movement to these systems with controls like the Windows Firewall.

Migration to Azure Active Directory (Azure AD) authentication is recommended to reduce the risk of on-premises compromises moving laterally to your authentication servers. Customers can use the following references on migration:

Use the activity report to move AD FS apps to Azure AD

Move application authentication to Azure AD

Read more on the official blog.

Hacks

- **DoorDash (Food delivery) hit by 3rd party compromise**

Just a reminder that Supply chain attacks can happen to anyone, a Zero-trust architecture and good Software/asset management with SBOM can mitigate some of these risks associated with these attacks.

DoorDash recently detected unusual and suspicious activity from a third-party vendor's computer network. In response, we swiftly disabled the vendor's access to our system and contained the incident.

Article here.

- **LastPass Security Incident**

Two weeks ago, we detected some unusual activity within portions of the LastPass development environment. After initiating an immediate investigation, we have seen no evidence that this incident involved any access to customer data or encrypted password vaults.

Lastpass provided more information around common questions on the incident on their official notice.

Full notice from Lastpass here.

Acknowledgements

Learn more about my Cloud and Security Projects: https://linktr.ee/acamillo

Consider subscribing to Medium (here) to access more content that will empower you!

Thank you for reading and leave your thoughts/comments!