XL Insurance

Cyber

Surviving the storm: Defending against cloud misconfigurations, vulnerabilities, and insider threats

By Milad Aslaner, Head of Technology Group at SentinelOne and Gwenn Cujdik, Head of AXA XL Cyber Incident Response Team, North America

Over the last decade, Microsoft has expanded its product portfolio from an operating system provider to a company providing various solutions spanning productivity, collaboration, and cloud capabilities. Some organizations today choose Microsoft 365 and Microsoft Azure to consolidate their vendor portfolio while often compromising on best-in-class capabilities. This approach has introduced significant risks to organizations as they become overly dependent on a single vendor.

Today, all Microsoft services are dependent on Azure Active Directory as its primary Identity and Access Management (IAM) solution. With that, the weakest link in a Microsoft environment has become the user identity. When a threat actor can compromise a user identity with elevated privileges like the security administrator role, they can evade all the defense measurements and security tools of Microsoft. In this article, we will look into how to identify and defend against some common cloud vulnerabilities, insider threats, and dangerous cloud misconfigurations.

Continued ➲

Cloud vulnerabilities

Cloud services offer significant advantages in scale and operational cost for organizations. Therefore, it is no surprise that 89% of organizations use multi-cloud services for their operations. However, with the rising adoption of cloud services, threat actors are shifting their attacks to target the cloud services directly that an organization is utilizing.

This risk presents a challenge for enterprises as they try to combat the already large attack surface of the Windows operating system; they now also have to handle the exponential increase of vulnerabilities in cloud and security services.

For example, security researchers at Proofpoint discovered that threat actors could initiate direct attacks against Microsoft Office 365 due to a design flaw that could allow attackers to encrypt files stored on SharePoint and OneDrive. In this example, the threat actor creates a malicious OAuth web application and lures a legitimate user to grant the threat actor the permissions for an account takeover.

SentinelLabs disclosed a privilege escalation vulnerability in Windows Defender in 2021 that had remained undiscovered for 12 years. In 2022, the same researchers also showed how Azure Defender for IoT contained multiple flaws affecting cloud and on-premise customers that allowed for remote code execution by unauthenticated attackers.

Meanwhile, numerous variants of NTLM relay attacks have been discovered, with Microsoft even stating that some had the status of 'won't fix'.

Due to often limited visibility into cloud environments, many organizations struggle to secure their crown jewels effectively or assume the responsibility of securing their cloud instances with the Cloud Service Provider (CSP).

According to the IBM Data Breach report, more than 33 billion records were exposed in 2018 and 2019 alone due to cloud misconfigurations.

Insider threat

The 2022 Insider Threat Report from Cybersecurity Insiders identified that insider incidents have become more frequent over the last 12 months. Let's look into insider threats more closely and then explore the relationship in the context of Microsoft environments.

Type of Insider Threats

- **Incautious Insiders:** Incautious insiders are individuals with access to the corporate environment who make an innocent or careless mistake resulting in a cyber attack. These could be individuals that aren't cyber aware and, for example, fall for a targeted social engineering trap.

- **Malicious Insiders:** Malicious insiders are individuals who have access to the corporate environment and agree to help threat actors, often for monetary gain. A recent prominent example would be a former Canadian government employee who pleaded guilty to working for a ransomware group responsible for hacking hospitals during the pandemic.

Cloud misconfiguration

As organizations accelerate their adoption of cloud services to enable their digital transformation journey, security has often become an afterthought. The assumption that securing cloud instances is the sole responsibility of Cloud Service Providers (CSP) is dangerous. In a recent example, a VPN service provider had discovered a cloud misconfiguration that can result in attackers accessing sensitive data stored on Microsoft Azure Blob accounts. The 2022 Cloud Security Report from Check Point confirms that 27% of organizations experienced a security incident in their public cloud infrastructure, while 23% of those were caused due to cloud misconfigurations.

89%

of organizations use multi-cloud services for their operations

27%

of organizations experienced a security incident in their public cloud infrastructure

2022 Cloud Security Report from Check Point

With the rising adoption of cloud services, threat actors are shifting their attacks to target the cloud services directly that an organization is utilizing.

Counter measurements provided by Microsoft

When examining the majority of attacks that target Microsoft environments, it's clear that the top three reasons for these are cloud vulnerabilities, insider threats, and cloud misconfigurations. Across all, what most have in common are weak security policies and implementations on the identity front. It is no surprise that Microsoft advocates that 99.9 % of account compromises can be prevented with Multi-Factor-Authentication (MFA). The challenge is that only 22% of enterprise customers utilize MFA, and even then, the basic implementation is often insufficient. For example, a cybersecurity researcher recently discovered how to leverage a built-in functionality of WebView 2 to extract cookies that allow the attacker to bypass MFA authentication.

Continued ➲

As many organizations moved their user identity from on-premise Active Directory to hybrid or cloud-native identity with Azure Active Directory (Azure AD), new risks are rising. To better understand the security risk, we first need to understand the different roles in Azure AD and its relationship to Microsoft services. Today, all Microsoft services leverage Azure AD to manage Access controls. To help manage access controls, Microsoft offers several built-in roles that allow a user to manage Microsoft resources once assigned.

The highest privilege is given to the 'Global Administrator' role that gets full access to all aspects of Microsoft services. Generally, this built-in role is highly guarded; however, Microsoft offers more roles such as 'Security Administrator', which grants full access to all Microsoft security services including Microsoft 365 Defender, Microsoft Defender for Endpoint, and Microsoft Sentinel or 'Security Reader' that grants read-only access to the Microsoft security products. These roles are commonly given to security personnel within an organization. Be aware that, even if an organization utilizes Role-Base-Access-Control (RBAC) in Microsoft 365 Defender or Microsoft Defender for Endpoint any compromised user identity with the Security Administrator or Global Administrator privilege will be able to overwrite access controls and access the management consoles. Microsoft is aware that these roles can be influential and that there is a risk when these are compromised. Therefore, Microsoft advocates for using capabilities like Just-In-Time-Access and broader Privileged Identity Management (PIM) services. However, similarly to MFA, only a tiny subset of enterprise organizations are utilizing these services due to their complex implementation. For those that do not, once a threat actor can compromise a user identity with, say, security administrator privileges, they now have access to the majority of Microsoft services, allowing them to evade the built-in security capabilities Microsoft offers.

Attack simulations

Let's examine a few possible threat models for an enterprise environment that leverages Microsoft.

Identity-based attack

For this exercise, the example enterprise has no Multi-Factor-Authentication (MFA), and has a Hybrid Azure AD model, and utilizes Microsoft Defender for Endpoint. In this case, the threat actor compromises a user identity from security staff, confirms that the user account has security administrator privileges, and enumerates through the Microsoft 365 portal the enabled security controls and products. The threat actor then chooses whether they want to disable those or simply avoid them as they progress to reach their end goal.

Due to the nature of the attack, Microsoft Defender for Endpoint is ineffective as it's missing the context of the user identity.

Initial Access
Compromise of security staff user account.

Account Takeover
Confirmed 'Security Administrator' role assigned to compromised user account.

Tool Enumeration
Attacker remotely enumerate through Microsoft 365 portal enabled products in the environment.

Defense Evasion
Attacker can either disable security controls or simply avoid the traps of the enabled security controls.

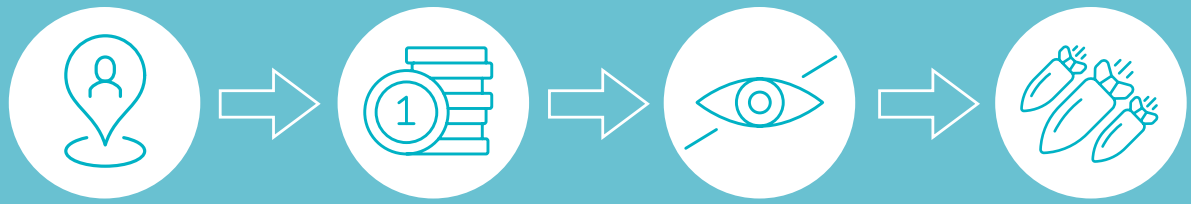
Impact
Attacker is able to perform their cyber attack completely in the shadow.

Continued ➲

Cloud-based attack

For this exercise the example enterprise has Multi-Factor-Authentication (MFA) and Privileged Identity Management (PIM), and Microsoft Defender for Cloud Apps. In this case the threat actor identifies one or multiple employees in the IT or Security team and offers monetary gain if they were to perform certain actions inside the corporate network.

As a result, given the user is within the IT or security division, the enabled security controls will most likely not raise immediate alerts for the suspicious activity but rather after the fact.



Reconnaissance
Threat actor identifies through social media unsatisfied IT or Security staff member.

Initial Access
Attacker pays employee to perform tasks inside the network on behalf of them.

Defense Evasion
Security controls will be initially blind as the activity is likely to look legitimate.

Impact
Attacker is able to perform their cyber attack in the shadow.

People, processes, and technology

The fundamental question becomes how organizations can reduce the risk of cloud misconfigurations, vulnerabilities in Microsoft products, and insider threats. When looking at this issue, it's essential to understand the requirements across people, processes, and technology.

People

According to research by Mimecast, 90% of security breaches are caused by human error. As such, it starts and ends with driving an effective security awareness program to reduce the risk of innocent or careless mistakes resulting in a cyber attack. It's important to acknowledge that nobody is immune from making mistakes and neither from falling for a targeted social engineering attack. Therefore, the way we drive the internal cyber awareness culture is paramount. Employees need to understand their privilege levels, how they can contribute to securing the enterprise, and report suspicious activities.

Processes

Consistent processes are critical and need to be tested. For example, the employee device usage policy should not leave room for interpretation. It should be clear what employees can or cannot do and outline the relevant security controls that need to be in place.

Furthermore, it should be clear how employees can report possible security incidents effectively. When defining these processes, it's essential that beyond just defining these, they are getting tested to ensure the security team can identify blind spots ahead of time.

Technology

According to the Verizon 2022 Data Breach Investigations Report, 61% of all breaches involved user identities. When looking at many enterprise organizations today, the IT and Security team needs to support various operating systems, cloud services, and endpoint types. These environments are often a combination of legacy and modern systems.

With that, it's no surprise that many organizations today have between 25 and 49 independent tools from 10 or more vendors to detect, triage, investigate or hunt for threats. However, as organizations are looking into vendor consolidation, they are looking for platform vendors that can help them across their digital estate rather than focusing on individual silos.

Continued ➲

As such, enterprises need to consider the integration of security capabilities that can detect, protect and respond to threats across the entire estate, leveraging the complementary nature of XDR and ITDR.

PROTECT	DETECT & RESPOND	PLATFORM
Priveleged Identity Management allows control, management, and monitoring of access priveleges within an organization.		**Extended Detection Response (XDR)** takes the approach of Endpoint Detection Response (EDR) and spans its capabilities across different surfaces including identity, email, SASE, etc. With XDR, organizations get a modern security platform to ingest and analyze data at scale and provide coordinated response actions.
Multi Factor Authentication provides proof of a user's identity from two or more authentication categories.		
Conditional Access ensures that only trusted and healthy identities and/or endpoints can access corporate resources and services.	**ITDR solutions** can detect and respond to identity-based cyber attacks through real-time infrastructure defense for Active Directory and Azure AD.	
Attack Surface Management provides ongoing assurance of security controls aagainst industry best practices.	**Network-based threat deception** helps lure in-network and insider threats into traps that enable security teams to uncover the adversary.	

It's no surprise that many organizations today have between 25 and 49 independent tools from 10 or more vendors to detect, triage, investigate or hunt for threats.

Conclusion

As organizations utilize cloud services, it is essential to understand the new threat models and be aware that securing cloud services isn't the sole responsibility of the CSP. Importantly, as security teams start to pivot, focusing on securing the cloud, it is important to look at the bigger picture for the enterprise environment and understand the risks across different surfaces–identity, email, endpoint, network–and identify means to protect, detect, respond, and recover from cyber threats across the entire digital estate.

Milad Aslaner *is Head of Technology Group at SentinelOne, a leader in cybersecurity. To learn more about how SentinelOne helps protect organizations from the issues discussed above, visit Singularity Identity.*

Gwenn Cujdik *is head of AXA XL's North America Cyber Incident Response Team in the US. She can be reached at gwenn.cujdick@axaxl.com.*

7123_09/2022