Teneo®

Microsoft Cloud Exploit Review by DHS's Cyber Safety Review Board Reveals Urgent Need for Security Overhaul

May 2024

In May and June 2023, a China-linked cyber threat actor group, motivated by espionage, breached Microsoft's cloud services using authentication tokens that were signed by a key which Microsoft had created in 2016.

The breach resulted in the compromise of Microsoft Exchange Online mailboxes belonging to 22 organizations and over 500 individuals around the world, with a specific focus on U.S. government mailboxes. The threat actor, known as Storm-0558, compromised senior U.S. government representatives working on national security matters, among others, including the email accounts of Commerce Secretary Gina Raimondo, U.S. Ambassador to the People's Republic of China R. Nicholas Burns and Congressman Don Bacon.

The following article provides insight into the Chinese operation targeting Microsoft, the Cyber Safety Review Board's (CSRB) assessment of the intrusion and Microsoft's security culture, as well as considerations for executives and organizations amid these critical developments.

How it Started

China-backed cyber threat actor Storm-0558 compromised Microsoft Exchange Online mailboxes across a broad spectrum of victims, mainly in the U.S. and UK. The U.S. Department of State, U.S. Department of Commerce and U.S. House of Representatives were among the compromised entities. Over a six-week period, the threat actor successfully downloaded approximately 60,000 emails from the State Department. In August 2023, in response to the breach, the Department of Homeland Security (DHS) announced that that they were tasking the CSRB, an independent investigative agency under the Cybersecurity Infrastructure Security Agency (CISA) and responsible for examination of “significant” cyber events, to conduct a thorough investigation of the intrusion. The CSRB was also responsible for a broader review of issues relating to cloud-based identity and authentication infrastructure affecting applicable cloud service providers (CSP) and their customers.

Current State of Affairs

On April 2, 2024, the DHS released a report detailing the CSRB’s findings from the review, which stated that the intrusion by Storm-0568 was “preventable” and “never should have occurred.” Most notably, the CSRB concluded that “Microsoft’s security culture was inadequate and requires an overhaul, particularly in light of the company’s centrality in the technology ecosystem and level of trust customers place in the company to protect their data and operations.” The findings also attribute the "cascade of avoidable errors that allowed this intrusion to succeed" to Microsoft's misconfigurations, backend architectural flaws and failure to adhere to best practices.

Since the intrusion, Microsoft released a new Secure Future Initiative (SFI) and has addressed some identified vulnerabilities through bug fixes, though the company has yet to undertake a comprehensive re-evaluation and enhancement of the security posture of its cloud environment – at least not publicly. It also seems that Microsoft is not certain how a key was stolen that enabled the hackers to access highly sensitive email inboxes in the 2023 intrusion, indicating significant shortcomings in their cloud computing cybersecurity that should be addressed urgently. Additionally, in January 2024, Microsoft disclosed a separate incident in which a Russian state-sponsored actor, which Microsoft calls Midnight Blizzard, accessed highly sensitive Microsoft corporate email accounts. Two months later, Microsoft claimed that Midnight Blizzard also gained unauthorized access to some of Microsoft’s source code repositories and internal systems.

Microsoft’s Critical Role in Corporate Infrastructure: A Double-Edged Sword

Cloud computing has become an indispensable resource to many companies that rely on this infrastructure to run operations and provide essential services to customers and partners. Driven by productivity and efficiency, adoption of these services continues to grow and they are becoming an indispensable function for most corporate entities. As a result, cloud service providers (CSPs) increasingly hold significant degrees of data, making cloud services a high-value target for a range of adversaries, including threat actors tied to nation-states.

Notably, Microsoft has a quasi-monopoly of operating systems and productivity suites. Its efforts in transitioning towards the cloud are further solidifying its dominance in the market. Their productivity and corporate tools render them virtually a default choice for organizations of all types and sizes. As such, although dependency on Microsoft to manage productivity tools, data, digital infrastructure, user authentication and security is convenient and streamlined, it has the added effect of creating a potential single point of failure. In turn, data management, encryption keys, device management, protection, user access and behavior analysis by the same platform poses a uniquely high level of risk if that service provider/vendor, such as Microsoft, is compromised.

Considerations for Executives

Companies must invest in and prioritize security consistent with a “new normal” in which cloud computing is an increasingly attractive target to a range of malicious actors. The breach targeting Microsoft’s cloud services by a China-based threat group actor underscores critical considerations for executives navigating the increasingly complex landscape of cybersecurity and cloud infrastructure. First and foremost, this incident highlights the necessity for executives to adopt a proactive approach to cybersecurity, recognizing that vulnerabilities within core infrastructure can have far-reaching consequences. Executives must prioritize continuous evaluation of their organization’s digital ecosystem, ensuring that robust security measures are in place to mitigate potential threats.

Moreover, executives should carefully assess their sole reliance on major technology providers, particularly in light of their expanding presence in cloud computing. This incident serves as a stark reminder of the inherent risks associated with such dependencies. Executives must balance the benefits of leveraging industry-leading platforms with the imperative to diversify and fortify their digital infrastructure to avoid single points of failure.

In response to the findings from CSRB’s review, executives and their organizations must advocate for heightened transparency and accountability from technology vendors. This includes urging companies like Microsoft to prioritize security as a fundamental aspect of their offerings rather than an optional feature. Executives should engage in ongoing dialogue with these vendors, emphasizing the importance of robust security protocols and the need for timely detection and response mechanisms to counter emerging threats effectively.

Of note, the 2023 incident that occurred was not detected by Microsoft itself, but rather by one of its targeted victims who had invested in premium licenses. Regrettably, this illustrates that customers of large operating systems/productivity suites may sometimes have to incur additional costs to ensure they are adequately safeguarded against the shortcomings of their service provider.

Finally, due to the CSRB’s review of Microsoft, Teneo’s Risk Advisory team assesses that dependency on singular product offerings mandates the need for additional tools and processes to monitor and control the operating environment. In addition to the implementation of defensive processes, it is imperative to establish and test a comprehensive resiliency and business continuity plan to counter potential cyber breaches, including those targeting companies like Microsoft and other cloud services.

For more information, email: Resilience&Intelligence@teneo.com

Authors

Courtney Adante
President, Security Risk Advisory
Courtney.Adante@teneo.com

Liad Mansky
Associate
Risk Advisory
liad.mansky@teneo.com

Teneo

The Global CEO Advisory Firm

Teneo is the global CEO advisory firm.

We partner with our clients globally to do great things for a better future.

Drawing upon our global team and expansive network of senior advisors, we provide advisory services across our five business segments on a stand-alone or fully integrated basis to help our clients solve complex business challenges. Our clients include a significant number of the Fortune 100 and FTSE 100, as well as other corporations, financial institutions and organizations.

Our full range of advisory services includes strategic communications, investor relations, financial transactions and restructuring, management consulting, physical and cyber risk, organizational design, board and executive search, geopolitics and government affairs, corporate governance, ESG and DE&I.

The firm has more than 1,600 employees located in 40+ offices around the world.

teneo.com