NETIZEN
CyberSecure Solutions

Netizen Case Study: 2024 KnowBe4 North Korean Insider Threat

Overview

KnowBe4, a cybersecurity firm based in Florida that specializes in providing phishing training simulations, recently faced a security incident involving an insider threat. The situation unfolded in mid-July when KnowBe4 hired an employee who was later discovered to have used a fake identity to gain access to their systems. This individual, initially hired as a Principal Software Engineer, had been posing as a legitimate candidate with the help of an AI-generated photo and a stolen U.S.-based identity.

On July 15, 2024, KnowBe4 sent the employee a Mac workstation. Upon receiving and starting up the workstation, it initiated the installation of malware, which triggered alerts from KnowBe4's endpoint detection and response software. The Security Operations Center (SOC) team observed suspicious activities originating from the employee's account at 9:55 p.m. EST. The SOC team contacted the new hire to investigate these anomalies. The individual initially attributed the issues to troubleshooting actions on their router; however, further scrutiny revealed attempts to alter session history files, transfer harmful files, and run unauthorized software. It was also discovered that the perpetrator utilized a Raspberry Pi device to facilitate the download of malware.

Initially cooperative with SOC inquiries, the new hire later stopped responding. By 10:20 p.m. EST, the SOC successfully secured the device and halted any further activities. Further investigations, conducted in cooperation with Mandiant and the FBI, revealed that the person involved was a North Korean agent who had assumed a false identity. The deployment of malware was deliberate and formed part of a broader plan that also included utilizing VPNs and gaining remote access from North Korea.

Impact

This incident raised significant concerns; however, it's worth noting that KnowBe4's systems remained secure, with no data compromised (or malware executed). Once the suspicious activity was detected, KnowBe4's SOC acted swiftly to contain the threat. The hacker had access only to basic communication tools—such as email, Slack, and Zoom—with no permissions to enter sensitive systems, customer data, or the company's internal networks. The workstation provided to the hacker was also highly restricted, containing no preloaded data and equipped solely with endpoint security and management tools. Quick detection and isolation prevented any unauthorized data access, or malware execution.

What the incident did do, however, was reveal weaknesses in KnowBe4's hiring and vetting processes, especially concerning remote employees. Consequently, the company has tightened these procedures; this includes implementing more stringent steps for shipping workstations and verifying the identities of new hires.

Although there were no direct financial losses or legal consequences, the company did incur various costs related to investigating the breach, reinforcing security, and updating hiring practices. These measures are essential for maintaining the organization's ongoing integrity and security.

The impact and overview provided here are based on public statements and FAQs from KnowBe4 regarding the incident. While Netizen did not directly assist KnowBe4 in this case, the tactics used in this attack are similar to those observed in other social engineering incidents handled by Netizen for various clients.

What Can Be Learned From This?

In addressing insider threats similar to the North Korean hacker case reported by KnowBe4, organizations can implement several preventive measures to enhance their security posture and through that mitigate the effects of such threats.

One of the most effective strategies for preventing insider threats is comprehensive end-user awareness and training. Insiders, whether malicious or inadvertently negligent, often contribute to security breaches through a lack of knowledge or improper behavior. Regular training sessions—ideally conducted on a quarterly basis—should focus on educating employees about the dangers of insider threats, recognizing suspicious activity, and adhering to best practices for data protection. Training should cover topics such as maintaining strong passwords, recognizing phishing attempts, and understanding the importance of reporting unusual behavior. For example, employees should be instructed on how to handle confidential information and the importance of verifying unusual requests or communications.

User and Entity Behavior Analytics (UEBA) tools are essential for identifying potential insider threats. UEBA tools analyze user behavior patterns to detect anomalies that may indicate malicious activity. A notable example is Splunk UBA, which helps establish baselines for normal user activities and flags deviations. Data loss prevention solutions also play an important role in monitoring and controlling the movement of sensitive data. Symantec Data Loss Prevention is a widely used DLP tool that can help organizations prevent unauthorized access and data transfers.

Multifactor Authentication (MFA) is another very important component of a layered security approach designed to ward off insider threats. While MFA is often associated with mitigating external threats, it is also proven effective in preventing unauthorized access by insiders. MFA requires users to provide multiple forms of verification before gaining access to critical systems or data, including verification methods like one-time passcodes, biometric verification, or hardware tokens. By implementing MFA, organizations add an additional layer of security—reducing the risk of unauthorized access, even if credentials are compromised.
Implementing network segmentation and strict access controls helps to contain and limit the potential impact of insider threats. By segmenting the network into distinct areas and applying access controls based on job roles and responsibilities, organizations can ensure that sensitive

data and systems are accessible only to authorized personnel. For instance, a finance department should have separate network segments from other departments, with restricted access controls in place. This approach not only prevents unauthorized access but also limits the spread of malicious activity within the network.

Effective monitoring and incident response are essential for managing insider threats. Continuous monitoring of user activities and network traffic can help identify unusual behavior that may indicate a potential threat. SIEM tools like Wazuh provide scalable and flexible log and event monitoring—enabling organizations to track user actions and detect anomalies. Coupled with a well-defined incident response plan, organizations can ensure that any suspicious activities are promptly investigated and addressed. This includes having clear procedures for handling and mitigating security incidents.

Policy and procedure documentation is vital for managing insider threats. Organizations should develop and maintain detailed policies that outline procedures for reporting suspicious behavior, handling data breaches, and conducting regular security audits. Clear documentation helps ensure that all employees are aware of their responsibilities and the steps to take if they suspect malicious activity. Well-defined policies and procedures contribute to a structured and effective response to insider threats—minimizing confusion and improving overall security posture.

By adopting these preventive measures, organizations can better safeguard against insider threats and reduce the impact of any potential incidents. Effective training, detection tools, access controls, and monitoring systems are key components of defense strategies—helping to protect sensitive information and maintain organizational security.

For more information,
visit our website at https://www.Netizen.net or call 1-844-NETIZEN