DKBINNOVATIVE CASE STUDY

ENHANCING HEALTHCARE WITH CYBERSECURITY

Following a corporate acquisition, the implementation of our security monitoring tools quickly identified suspicious login activity in the acquired company's Microsoft 365 environment. Investigation revealed a long-standing account compromise that had been exploited to create unauthorized Azure infrastructure used for malicious phishing campaigns.

This unauthorized infrastructure had operated undetected for over a year, generating approximately $10,000 in illicit charges to the company's credit card.

SITUATION

A client recently completed the acquisition of a company with inadequate cloud security controls. As part of the post-acquisition integration process, our standard security tools were deployed across the acquired company's digital environment.

CHALLENGE

Within days of deployment, our security monitoring system detected suspicious login patterns for a Microsoft 365 account belonging to the acquired organization. Initial investigation indicated this wasn't a new security breach but rather an ongoing compromise that had remained undetected by the acquired company.

DKB innovative

INVESTIGATION FINDINGS

An investigation revealed that a compromised account had been accessed by unauthorized parties for over 12 months. During this time, the attackers used the account credentials to provision multiple Azure virtual machines and related infrastructure. This unauthorized setup was leveraged to conduct widespread phishing campaigns. As a result, all associated costs, which exceeded $10,000, were charged directly to the company's credit card linked to the account. The acquired company lacked monitoring systems to detect unusual account activity or unexpected cloud resource provisioning. Additionally, basic cloud security configurations were absent, which allowed the unauthorized access to persist undetected for an extended period.

BUSINESS IMPACT

The incident had a significant business impact, including a direct financial loss of over $10,000 due to fraudulent infrastructure charges. There was also a risk of reputational damage stemming from phishing campaigns launched through company-linked infrastructure. Additionally, the company faced security remediation costs and operational disruptions throughout the investigation. Compliance concerns were also raised due to the potential exposure of sensitive data.

PREVENTATIVE RECCOMENDATIONS

To prevent similar incidents in future acquisitions, several key security measures are recommended. Conducting thorough security assessments should be a standard part of the due diligence process before finalizing any acquisition. Upon acquisition completion, comprehensive monitoring tools should be deployed immediately to track potential threats. Enforcing multi-factor authentication across all cloud environments is crucial to enhance account security. Establishing alerts for unusual account activity, geographic access anomalies, and unexpected resource provisioning can provide early warning signs of suspicious behavior. Regular reviews of cloud billing can help identify unexpected charges or unauthorized resources. Implementing least-privilege access controls for all cloud services will limit exposure and reduce the risk of compromised accounts.

RESPONSE

Our team took immediate action to mitigate the situation. The compromised account was secured, and its access credentials were promptly reset. All unauthorized Azure infrastructure was identified and removed to prevent further misuse. A comprehensive review was conducted to confirm that no lateral movement had occurred into the parent company's environment.