GUARDIAN

greenlight-is.com/guardian

CASE STUDY

Guardian, Greenlight's Managed Cybersecurity Service, Thwarts TWO Separate Cyber Attacks for a Single Client in the SAME DAY!

CLIENT PROFILE

INDUSTRY	Life Insurance Planning
OFFICE LOCATIONS	California & New York
ESTABLISHED	1996

OVERVIEW

The Guardian client experienced two independent cyberattacks in the same day. The attacks were unsuccessful due to Guardian's comprehensive cybersecurity measures.

CYBERATTACK #1 – ACCOUNT TAKEOVER

A user at the client company was using the same password for multiple systems, including systems not monitored by Guardian. Her password was compromised, and with this information, the attacker attempted to log into the user's Microsoft 365 account. The user received a multi-factor authentication (MFA) request to approve the login and rejected it. The attacker used a technique called MFA bombing to repeatedly send requests for approval until the user accepted the request in order to make the notifications stop. The attacker was now authenticated and in the client's system.

GUARDIAN PROACTIVE RESPONSE

The Guardian Security Operations Center (SOC), which monitors activity 24x7, noticed that 1) the account had multiple denies on MFA prompts 2) the login was from an unknown device 3) the login was from a different location than normal. An investigation was triggered, and the SOC blocked the account and revoked all actively logged-in sessions, including the threat actor's session. This all occurred in a matter of minutes.

RESULT – DATA BREACH PREVENTED

It was determined that there had been no activity on the account since the account takeover. The threat actor simply did not have enough time to cause any harm. Without Guardian the company could have suffered a major data breach, downtime, and possible litigation.

Greenlight
INFORMATION SERVICES

GUARDIAN

greenlight-is.com/guardian

CYBERATTACK #2 – BUSINESS EMAIL COMPROMISE

A user at the client company received an email containing an invoice for $50,000 to be paid by one of the client's customers. The email appeared to be from a known vendor. The user attempted to forward the invoice to the client's customer for payment. The email and invoice were, in fact, from a cyber-criminal attempting to commit wire fraud.

GUARDIAN PROACTIVE RESPONSE

The Guardian email security filter detected that the initial email was suspicious and blocked the email. The user released the email from the filter without investigating. A second Guardian email filter detected that the email was from an impersonated domain and blocked the email a second time. The user released the email again and attempted to forward the email to the client's customer for payment. The Guardian email filter scanned the outbound email and blocked the email from sending.

RESULT – WIRE FRAUD PREVENTED

Upon investigation, it was clear the email was a fraud. Without Guardian email security in place, with its multiple filters and safeguards, the client's customer would have received the fraudulent request, may have assumed the email was legitimate, and sent $50,000 to cyber criminals..

SUMMARY

Cybercriminals are tirelessly working to circumvent security measures, so a comprehensive cybersecurity strategy is required, including proactive management, in order to detect and mitigate threats.

GUARDIAN

Contact Greenlight today to learn more about how we can protect your business.

guardianinfo@greenlight-is.com

Greenlight
INFORMATION SERVICES