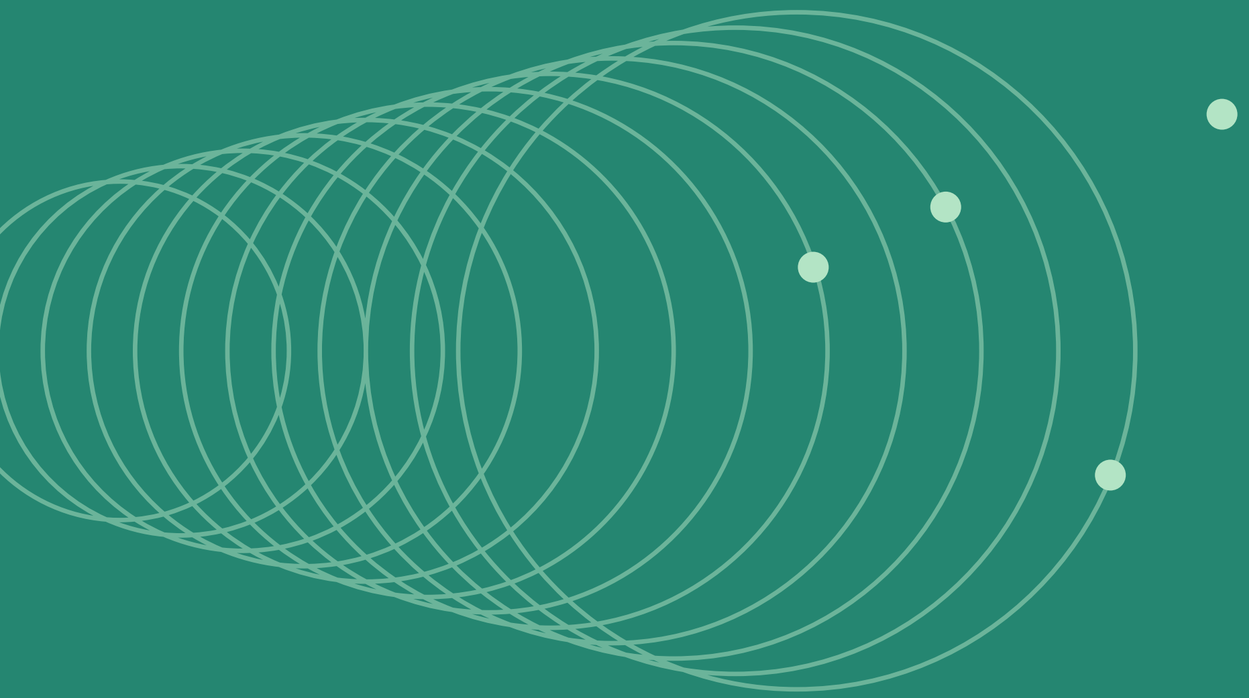
ACME

ACME Data Breach

Presented by: Marvin the Martian SOC

Key Findings



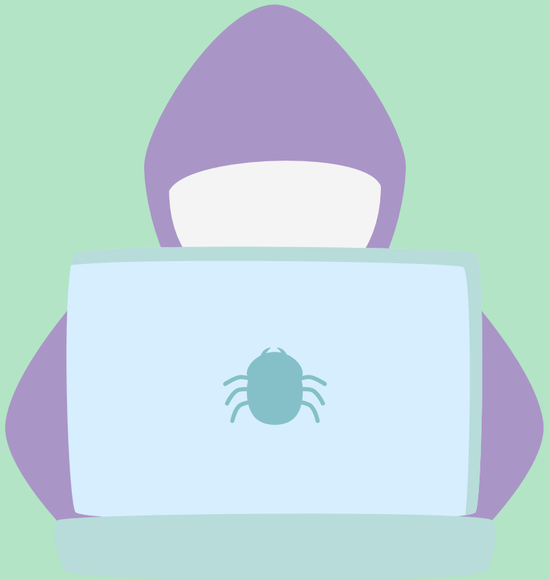
Marvin The Martian has concluded that the recent data breach experienced by ACME was due to direct negligence on the part of Cyber Stooges. Lack of ownership, basic security practices, accountability, and insufficient hardware. Bad actors whose origins have yet to be determined were able to successfully enter our network and leave with undetermined data, leaving behind ways to monitor our communications and activities. Currently, ACME has numerous critical security flaws, and exposed vulnerabilities

Monitoring Summary

The scope of the monitoring involved all ACME hardware and network assets, and web services, including switches, web servers, firewalls, Intrusion Detection Systems, hosts, and the company website. Logs were reviewed for all devices,

Incident Summary

Beginning 12/12/2017 and ending on 12/29/2017 ACME was subject to multiple Cyber-attacks. Web server attacks were launched on ACME until they were able to take over a workstation, then using that as a pivot point to maneuver around our network and eventually take another host. From here on, Exhange email servers were compromised, internal databases were modified, and malicious code was executed. Spyware was installed on ACME network assets allowing the bad actors an easy way in, and a way to monitor and intercept all ACME network traffic. ACME Mail servers were targeted for spyware, allowing bad actors to intercept all inbound and outbound traffic, and data was shown to have been stolen from ACME.



Threat Summary

Currently the biggest threat facing ACME is its lack of basic security practices when faced with a competitive market. ACME is a leader in Anvil covers and cellphone hardware, with its lead on the market being sought after by Chinese competitors. The lack of access management, vulnerability patching, and IT awareness training will not only lead to loss of IPs but conclude in potential class action lawsuits for loss of any PII, and heavy fines for failure to comply with PCI and GDPR regulations.

Recommendations

Implementation of the security plan and security polices created for ACME ASAP is at the top of the list, vulnerability patching, hardware refresh, and cyber awareness training would help to prevent this event from recurring. The SOC is requesting $45,816 for hardware, and $17/person for KnowBe4 Cyber Security awareness training to help avoid phishing attacks, and keep ACME staff up to date on security practices.

Proposed Network