Capstone Final Paper

Tony Benjamin Khawaja-Lopez

Instructor: Eric Keith

Date: 11/06/2022

Executive Summary

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.

Findings

Marvin the Martian SOC was employed to investigate the large data breach which occurred late into this year. Investigations started at assessing ACME's current security posture, including internal policies and procedures, documentation, external and internal applications, and network security. Claims by the Cyber Stooges in released pressed statements attribute the breach to zero-day exploits, contrary to this evidence shows it was in fact due to gross negligence. OSINT investigations show that the official company website was being used as an internal security bulletin, showing organizational network and software assets.\

FIgure 1

Hardware Assets:

Cisco Identity Services Engine
Cisco Firepower
Cisco ASA 5500
Ubiquity Wireless and Network Equipment

Software Assets:

What's Up GOLD
Splunk Enterprise
Active Directory
Windows Print Server
Adobe Connect Server

Cloud Assets
OKTA IdP
Zoho Password Management Suite
Microsoft Teams
One Drive
Office365

Contact information for the CISO with organizational domain was on display, as well as all known critical security flaws were exposed in the clear on open web. Whether this was due to incompetence, automation failures posting to the website, or malicious intent, will need to be investigated further. Logs from the switch, firewall, and IDS were provided by the CISO for review to help determine the extent and origin of the attack.

Switch logs proved not to be helpful in determining anything about the attack, SOC recommends immediately configuring the switch to log network traffic to help with future incidents. Firewall findings show a much clearer picture, with attacks beginning on 12/12 and ending on 12/29, beginning at our web-facing assets our Apache web servers were attacked.

Eventually bad actors, potentially Chinese competitors, managed a buffer-overflow exploit on a MicroSoft server extension and taking over an employee's workstation. SSL certificates can be presumed as stolen, after successful heartbleed attacks on the servers, the exploited workstation was then used to traverse the network, takeover another host, elevate privileges, compromise internal databases and breach Exchange email servers.

IDS logs show that sustained brute force attacks beginning 12/17/2017 at 10AM and ending at 12/18/2017 at 10AM were successful in enumerating ACME domains, web and mail servers. Recon was being aggressively performed on ACME after bad actors realized there were no safeguards in place. After successfully breaching our defenses, the attacker moved across our network and created reverse shells on a handful of our servers, allowing them to steal data from the network. We may fairly conclude that malware was set up on several unused and unprotected UDP ports to facilitate quick data transmission. Multiple unused UDP ports demonstrate spyware activity. Attackers were able to intercept inbound email to ACME thanks to a vulnerability of IMAP servers.

This is all to paint a picture of complete lack of security practice, with many of these vulnerabilities being easily remediated with proper configurations, logging policies, and routine patching of software. Lack of access control and data owners/managers make investigation more difficult, as non-repudiation is nonexistent in the current environment.

Recommendations

Immediate patching of all ACME software is to be done, particularly to the Apache Server OpenSSL software, to patch the critical Heartbleed vulnerability. The first step in

preventing a recurrence of this event is to implement the security plan and security policies developed for ACME as soon as possible. Vulnerability patching, hardware upgrades, and cyber awareness training would also be helpful. To prevent phishing attempts and keep the ACME workforce up to date on security procedures, the SOC is asking for $45,816 for hardware and $17 per worker for KnowBe4 Cyber Security awareness training.

Hardware expenses are broken into the following:

1. C1000-48T-4G-L Cisco Switch $1,600USD
2. FPR2110-NGFW-K9 Cisco NGFW $6,621USD
3. ASA-IPS-10-INC-K9 Cisco IPS $35,000USD
4. AIR-SRVR-300GB-HD Cisco Server $2595USD

Proposed Network changes involve:

1. Network segmentation, separating Windows and Linux machines
2. A DMZ for business-critical servers and the vulnerability scanner
3. A NGFW placed after the honeypot to prevent further network traversal
4. IPS out-of-line to help prevent network breach
5. A Web proxy to log and prevent basic web server attacks

Proposed Network Diagram