# Acme Company Mission Analysis

By: Christopher Bristol

# Team Introduction

- Christopher Bristol (Director of IT)

## *Agenda*

- We will be discussing and going over our findings within the ACME network infrastructure

- Going over different mitigations/recommendations in order to better secure the network

## Leadership’s intent and concept of operation

- Address different levels of vulnerabilities in the network infrastructure, in order to prevent threat actors from accessing the IT systems and applications

ACME COMPANY
suck less

- Configure different mitigation plans in order to prevent malicious activities/actors from infiltrating our network

- Implement Risk framework and security throughout ACME

## Problem Statement

- ACME  was recently breached
- Security has not been integrated into engineering, product design, innovation or distribution centers
  - Usually done as an afterthought.

ACME COMPANY
suck less

- No identified Risk framework
  - Security by Obscurity process to manage risks
  - Consequences:
    - Theft
    - Failure to thrive
    - Lack of transparency
    - Lawsuits

- More of ACME's partners and suppliers compromised in last 2 years
  - Brought awareness to C-Suites

# Mission Statement

- Focus on integrating security into different ACME divisions:
  - Engineering
  - Product design
  - Innovation
  - Distribution centers
- Implement a constructive and effective Risk framework
  - Address security policies into practices across the IT infrastructure and each division

ACME COMPANY
suck less

- Monitor and train employees to identify features of malicious activities
- Proper tracking of reports, logs, data storage
- Effectively generate and perform mitigation plans to alleviate current vulnerabilities and further flaws.

## Review Initial Guidance

- Ensure software is up to date throughout our network.

- Implement HTTPS and SSL certificate for the website to protect any information between the server and the browser while a user is engaging with our site.
- Record user access and administrative privileges.
- Backup all of our data
  - Even if we don't plan on our data being taken for ransom, we should still have backups just in case.

# Specifies, Implies, and Essential tasks

*Specified Tasks*

- Going into the network infrastructure, and determining vulnerabilities and their threat levels
- Coming up with mitigation plans to subdue these vulnerabilities

- Installing remote security scanning tools and scanning each server
- Find and report different asset findings

- Identify and implement an effective and beneficial security framework across the IT infrastructure and each division in ACME.
- Incorporate some sort of risk mitigation program/plan to reduce any current or future incidents from occurring

*Implied Tasks*

*Essential Tasks*

# Intelligence Preparation of the Environment

Environment:

- Network of 11 computers
  - Workstations x4
  - Vuln Scanner x1
  - Honey Pot x1
  - Testing x1
  - Ubuntu Box x2
  - LDAP Server x1
  - SpiceWorks x1

Effects:

- Weak and repeated passwords favors the adversaries.

- Lack of MFA favors the adversaries. No authentication if passwords are brute forced

Threat/Adversary:

- Competitors
- Cyber Criminals

Adversary Course of Action (COA)

1. Search for unsecured devices/ports
2. Obtain credentials from social engineering / brute force
3. Using stolen credentials/exploits to gain access to our database.
4. Steal information from our database
5. Hold said stolen data for ransom or sell stolen data

# Pertinent facts and assumptions

- No real Risk framework/security strategy across ACME
- Use Security by obscurity process to manage risk

- Assume that employees don't have general knowledge about company security policies/procedures

# Assets available and resource shortfalls

- ACME products are growing throughout Europe, Asia, Middle East, and Africa
  - APAC (Headquarters Hong Kong)
  - EMEA (Headquarters Cork & Ireland, Sub-office in Germany)
- Three start-up businesses
  - Nerdy Minds

- Wild Rock PR
- 10AK Technologies

➢ Little to no information/resources from previous security team

# Proposed CCIRs (Commander's Critical Information Requirements)

- ***Priority Intelligence Requirements (PIR)***
  - Multiple ransomware files found on system
  - Multiple successful admin users login without having to provide any credentials
- ***Internal Information Requirements (IIR)***
  - Honeypot server serves no purpose
  - New network map created with the addition of new systems
    - Assigned IP addresses

- ***Essential Internal Information (EII)***
  - User Credentials
    - Passwords
  - Personal Information
    - Financial Information
    - Employee information

# Initial collection plan

- Create ticketing system for our team to point out any issues
- Run vulnerability scans. (Nessus)

- Check for open ports and map out the network (Nmap)

## 2022 Q4

### Reconnaissance

- Identifying the current state of our system's ecosystem
- Audit the current systems for vulnerabilities
- Investigate the data breach
- Identifying desired end state.
- Meet with CISO and go over future course of action (recommendations and budgeting)

## 2023 Q1-Q2

### Implementation

- Purchase needed software and licenses (Windows, Splunk, Scanners, Cloud Storage, IDS, VPNs, etc)
- Utilize tools (performing audits and scans regularly), implementing our SIEM
- Offer training to employees to identify malicious behavior
- Set new standards for password strength
- Introduce VPNs into our system to ensure more security

## 2023 Q3

### Respond / Eradicate

- Rollout company wide ticketing system
- Ensure the data breach has been fully contained
- Deploy backups
- Create and apply response plan (Threat Intelligence)
- Discover most current threats and patch accordingly

## 2023 Q4

### Maintenance

- Maintain everything built so far
- Full penetration test
- Review reports
- Ensure future incidents do not occur
- Stay up to date on current exploits and vulnerabilities
- Share threat intelligence throughout the company
- Generate and perform mitigation tasks based on current events

# Conclusion

ACME has experienced some adversity recently with our previous CISO stepping down, losing the 3rd party security team, and the most recent data breach. It is now more important than ever, to recognize our mistakes and to improve from them. Now that we have discovered the risks within our ecosystem, it is now time to act. We now have an internal security team to make the difference. Company wide training will help our entire internal team make good decisions. Staying up to date

on our reports will bring any concerns to our attention. Keeping our software up to date will mitigate exploits due to outdated software. With these changes implemented, we can ensure a strong future for our brand and our reputation.

# References

Photos:

- https://cdn-www.comingsoon.net/assets/uploads/2018/08/Wile-E-Coyote.jpg
- https://www.questionpro.com/blog/wp-content/uploads/2018/08/data-collection.jpg

ACME COMPANY

Websites :

- http://acmecompany.us/
-

,