RISK ASSESSMENT REPORT

ACME ANVILS
17 SEPTMEBER 2021

Scope

The scope of this risk assessment is focused on ACME system's use of resources and controls to mitigate vulnerabilities exploitable by threat agents (internal and external) identified during the RMF control selection process, based on the system's categorization.

This initial assessment will be a Tier 3 or "information system level" risk assessment. While not entirely comprehensive of all threats and vulnerabilities to the IS, this assessment will include any known risks related to the incomplete or inadequate implementation of the NIST SP 800-53 controls selected for this system. This document should be updated after certification testing to include any vulnerabilities or observations by an independent assessment team. Data collected during this assessment may be used to support higher level risk assessments at the mission/business or organization level.

Purpose

This initial risk assessment is to identify and document areas where the selection of risk management framework controls was compromised in a recent data breach and may have left residual risk. This will provide security control assessors, officers, and organizational leadership an upfront risk profile.

Risk Assessment Approach

This initial risk assessment was conducted using the guidelines outlined in the NIST SP 800-30, Guide for Conducting Risk Assessments. A Qualitative/Semi-Quantitative approach will be utilized for this assessment. Risk will be determined based on a threat event, the likelihood of that threat event occurring, known system vulnerabilities, mitigating factors, and consequences/impact to mission.

Table 1: Threat Sources

TYPE OF THREAT SOURCE	DESCRIPTION
ADVERSARIAL - Individual (outsider, insider, trusted, privileged) - Group (ad-hoc or established) - Organization (competitor, supplier, partner, customer) - Nation state	Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources (e.g., information in electronic form, information and communications, and the communications and information-handling capabilities provided by those technologies.

TYPE OF THREAT SOURCE	DESCRIPTION
ADVERSARIAL - Standard user - Privileged user/Administrator	Erroneous actions taken by individuals in the course of executing everyday responsibilities.
STRUCTURAL - IT Equipment (storage, processing, comm., display, sensor, controller) - Environmental conditions • Temperature/humidity controls • Power supply - Software • Operating system • Networking • General-purpose application • Mission-specific application	Failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances which exceed expected operating parameters.
ENVIRONMENTAL - Natural or man-made (fire, flood, earthquake, etc.) - Unusual natural event (e.g., sunspots) - Infrastructure failure/outage (electrical, telecom)	Natural disasters and failures of critical infrastructures on which the organization depends but is outside the control of the organization. Can be characterized in terms of severity and duration.

The following tables from the NIST SP 800-30 were used to assign values to likelihood, impact, and risk:

Table 2: Assessment Scale – Likelihood of Threat Event Initiation (Adversarial)

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Adversary is **almost certain** to initiate the threat event.
High	80-95	8	Adversary is **highly likely** to initiate the threat event.
Moderate	21-79	5	Adversary is **somewhat likely** to initiate the threat event.
Low	5-20	2	Adversary is **unlikely** to initiate the threat event.
Very Low	0-4	0	Adversary is **highly unlikely** to initiate the threat event

Note: We've rated this category as "Very High" given the vulnerabilities discovered and controls needing implementation (outlined in Overall Assessment).

Table 3: Assessment Scale – Likelihood of Threat Event Occurrence (Non-adversarial)

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Error, accident, or act of nature is **almost certain** to occur; or occurs **more than 100 times per year**.
High	80-95	8	Error, accident, or act of nature is **highly likely** to occur; or occurs **between 10-100 times per year**.
Moderate	21-79	5	Error, accident, or act of nature is **somewhat likely** to occur; or occurs **between 1-10 times per year**.
Low	5-20	2	Error, accident, or act of nature is **unlikely** to occur; or occurs **less than once a year,** but **more than once every 10 years**.
Very Low	0-4	0	Error, accident, or act of nature is **highly unlikely** to occur; or occurs **less than once every 10 years**.

Note: We've rated this category as "High" (outlined in Overall Assessment).

Table 4: Assessment Scale – Impact of Threat Events

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	The threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A severe or catastrophic adverse effect means that, for example, the threat event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

Qualitative Values	Semi-Quantitative Values		Description
Moderate	21-79	5	The threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A serious adverse effect means that, for example, the threat event might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.
Low	5-20	2	The threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A limited adverse effect means that, for example, the threat event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Very Low	0-4	0	The threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation.

Note: We've rated this category as "High" given the vulnerabilities discovered and controls needing implementation (outlined in Overall Assessment).

Table 5: Assessment Scale – Level of Risk

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	Threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

Qualitative Values	Semi-Quantitative Values		Description
Moderate	21-79	5	Threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Low	5-20	2	Threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Very Low	0-4	0	Threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

Table 6: Assessment Scale – Level of Risk (Combination of Likelihood and Impact)

Likelihood (That Occurrence Results in Adverse Impact)	**Level of Impact**				
	Very Low	Low	Moderate	High	Very High
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

Risk Assessment Results

Threat Event	Vulnerabilities / Predisposing Characteristics	Mitigating Factors	Likelihood (Tbl 2 or 3)	Impact (Table 4)	Risk (Tbls 5 & 6)
Perform perimeter network scanning	Open Ports	Close ports	Very High	Moderate	High
Phishing Attacks	Email Accounts	Staff Awareness Training/User Access Limits/Ahead of attack prevention tools	Very High	Very High	Very High

Threat Event	Vulnerabilities / Predisposing Characteristics	Mitigating Factors	Likelihood (Tbl 2 or 3)	Impact (Table 4)	Risk (Tbls 5 & 6)
Malware delivery to internal information systems.	Email/System Patching/Software applications/File sharing services	Update & configure legacy systems, software & File share services	Very High	Very High	Very High
Exploit vulnerabilities on internal information systems	File Sharing/Samba	Application upgrade/Close vulnerable ports	Very High	High	High
Compromise mission critical information	System Patching/Software applications/File sharing services	Update & configure legacy systems, software & File share services	Very High	Moderate	High
Conduct attacks using unauthorized ports, protocols, and services	Open ports/Vulnerable services	Close ports/Deploy new services	Very High	High	High
Conduct brute force login	Password integrity/management	Multi-factor authentication/Password reset protocols	High	High	High
Obtain sensitive information via exfiltration	Phishing/Malware/Open ports/Vulnerable hardware	Application upgrades, patches/Training/Close ports	Very High	Very High	Very High

* Likelihood / Impact / Risk = Very High, High, Moderate, Low, or Very Low

Risk Assessment Summary

Methodology & Evidence

Upon taking inventory and assessing of hardware and software applications on the ACME system and running vulnerability scans on the network, the following is the deduction of the assessment with recommendations/opportunities in accordance with NIST 800-53 and CIS Controls.

- Some machine hardware residing on the network that are non-essential and pose vulnerabilities.
    - Linux machine (open ports, not securely configured, should at minimum be segmented off from the network)
    - Spiceworks machine but application not in use or utilized.
    - LDAP machine not securely configured for use.
    - Multiple Ubuntu machines not updated to current OS.
- Firewall configuration and integrity unknown.
- Password management protocols are absent.
- Account Management & Access Control Management are not implemented (users with administrative privileges that are not required).
- File sharing application (Samba) not recommended for enterprise deployment.

In the time range approximately December 13-17th there were multiple DNS requests logged and attacks on two of the legacy Ubuntu machines (14 & 16-1) and traverse directories, compromise those directories and gain access to sensitive data with administrator access through Samba (TRiddle account). The Samba file sharing system was sharing access with the LDAP server as well as shared Samba ports with the Ubuntu 14 machine which is setup as a server with access to multiple machines on the network. This allowed for remote access and infiltration through SMB protocols and eventually exfiltration of data.

Recommendations

- Close ports – It was also discovered that port 139 (open) which is utilized by NetBIOS Session Service provides access to shared resources to anyone on the internet. Port 445 which was also discovered open, is used by Microsoft Directory Services for Active Directory and SMB protocol over TCP/IP. Port 8834, Nessus Web. Port 631, Internet Printing Protocol of UDP and port 3306 for MySQL. SSH ports were also open on both Spiceworks Server and LDAP machines.

- VPN - VPNs bolster your device's security and control. A VPN will ensure your data is kept secure, information is remotely accessible, personal data remains anonymous and that you have access to file sharing between groups.

- Proxy Server - You can configure your proxy server to encrypt your web requests to keep prying eyes from reading your transactions. You can also prevent known malware sites from any access through the proxy server.

- Smart Enterprise Firewall – Can protect the organization from malicious code. A smart firewall will look for and block viruses, worms, spam, and other unwanted Internet traffic. It will also log intrusion attempts as well as other violations to business policies. This enables you to examine unauthorized access attempts and other suspicious activity.

- As previously stated, segment or decommission hardware not applicable, relevant or in use for business objectives.

- Procurement and deployment of SIEM monitoring capabilities to flag and alert of abnormal events from baselines.

Employ & deploy the top five CIS Controls over the next 12 months:

1. Inventory and Control of Enterprise Assets
2. Inventory and Control of Software Assets
3. Data Protection
4. Secure Configuration of Enterprise Assets
5. Account/Access Control Management

Appendices

https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final