ACME Security Plan

Produced by: Marvin the Martian SOC

Commissioned by: WIley E. Coyote

Date: 11/05/2022

3 Months Change Passwords

Every 90 days (about 3 months) enforce a password change policy with a 8-12 character minimum, including special characters and numbers. Network, system and application passwords should be changed as well, and MFA is to be enforced on all systems. Password reuse policies should be set, so as not to allow the reuse of passwords in too short a span of time.

3-6 Months Simulated Phishing exercises

Simulated phishing exercises should be conducted on a routine basis to evaluate your entire organization's security posture, policy adherence, and tailor security training. Phishing is one of the fastest growing cyber-attacks and they are becoming more advanced, if you're not on top of this you will quickly fall victim to a phishing attack(s).

3-6 Months Remote Access Testing

Remote access for business continuity should be tested quarterly, including VPN access, web applications, etc. In the event of an unforeseen disaster, it is imperative to keep the business running and have essential members of the organization guarantee access.

6-12 Months Penetration Test

Vulnerability assessments are to be made at minimum once a year, ideally twice. With this information, we can remediate any potenital vulnerabilities in our networks, systems, and

training. Proactive approaches to security help to prevent breaches, loss in credibility, IPs, reduce fines for non-compliance and prevent class action lawsuits in the case of PII.

6-12 Months Tabletop Exercises For Mangement and IR

At least once a year, tabletop exercises should be held either virtually or in person to bring together senior management, incident response teams and the organization as whole. Run through playbooks, make sure everybody knows their parts, and help to develop better incident responses. Much like disaster recovery, if it is not routinely tested, there is no way to make sure that the organization moves as a whole.

12 Months Employee InfoSec Training

Once yearly, either virtually or in person, infosec training should be held organization wide. This should be comprised of common threats including phishing, and malware, best practices and a review of security policies.

12 Months Review and Update Internal Security Documentation

Security documentation should be updated yearly, as threats are always evolving, and business is always changing and growing. This includes BCP, Access Control Policies, Acceptable Use Policies, Incident Response Plans, and Disaster Recovery Plans. Not only does this serve to help the organization remain compliant but helps to keep us ahead of the curve and on the front lines in the constant battle for Cyber-Security.