FOCUS TECHNOLOGY | cisco Partner

Cybersecurity Program Gap Checklist

Identifying gaps in your cybersecurity is essential for safeguarding your organization against potential threats, ensuring compliance with regulations, protecting sensitive information, and maintaining trust and confidence among stakeholders. Review this cybersecurity program gap checklist to compare your current cybersecurity posture against industry standards and best practices and determine fresh steps to take to further protect your digital assets, data, and systems from potential threats.

Account Protection

Poor password hygiene remains one of the most common ways bad actors get control of an account. Protect passwords to protect accounts. Do you have the following?

- **Active directory policies to require password complexity**
- **User lock out after a number of incorrect attempts to combat brute force attacks**
- **Screen timeouts to protect confidential data and prevent unauthorized use Multi-factor authentication (like Cisco Duo) to require users to provide multiple layers of verification**

Network Security

Implement and enforce proper network and wireless security to safeguard the organization's data, systems, and infrastructure. The key components include

- **A guest wireless network to limit non-employee access**
- **Network segmentation to limit what is accessible in the event of a breach Wireless security protocols to establish secure communications**
- **Virtual Private Network (VPN) connectivity to avoid users relying on open ports to remote in to desktops and server.**
- **Next-Generation Firewalls (such as Cisco Firepower), including features like application firewalling, intrusion detection, and packet inspection, to help control traffic based on predetermined security rules**
- **Cisco Umbrella to secure internet traffic and protects users at the Domain Name Server (DNS) layer with asset discovery, vulnerability protection and behavioral monitoring in one tool**

Endpoint Protection

Virus and malware protection are still needed, but no longer enough. The number of endpoints has expanded. In addition to laptops, tablets, and other mobile devices, you may have handheld scanners, robots, printers, and Internet of Things devices. All these devices need regular monitoring and threat detection to identify active threats and remediate attacks. Best practices for protection and detection include:

- **Patch management to keep devices to address known vulnerabilities in software and operating systems**
- **Endpoint encryption to secure data on all devices (such as with Cisco Secure Endpoint)**
- **Network access control to manage user and device access to your network**
- **Data classification to isolate your most valuable and vulnerable data**
- **Web filtering to block potentially malicious sites**
- **Data Loss Prevention (DLP) to safeguard your data against unauthorized removal Secure email gateways to prevent access to suspicious links or files**

Cloud perimeter security creating a cloud firewall around people and devices and adding cloud-based web filtering

Security Operations

Many organizations lack the proper tools and staffing levels to keep up with cybersecurity responsibilities. In other cases, too many tools and alerts causes real alerts to be missed. The best tools offer comprehensive capabilities:

- **Security Information and Event Management (SIEM) such as Cisco SecureX provides visibility into the entire network**
- **Extended detection and response (XDR) automates data collection and correlation across multiple security layers for faster detection and improved response times**
- **Reduce your attack surface by identifying gaps and taking action to strengthen your cybersecurity posture.**

Backup and Disaster Recovery

Backup, and Business Continuity / Disaster Recovery protects from issues ranging from viruses, application corruption, mechanical failure, human error, site outages and ransomware. Preserve optimal flexibility and network redundancy with one of these traditional models for environment replication:

A geographically separate alternative or secondary data center A hosted, secure, environmentally-controlled data center facility A cloud-based data center (public or private)

Focus Technology has maintained a five-star standard of excellence in IT for over 25 years. We have the hands-on experience and practical know-how to protect your organization from new and emerging cyber threats. Contact us today.

617.303.0480

https://www.focustsi.com/

10 Post Office Square
Suite 1005 Boston, MA 02109