Implementing a Cybersecurity Solution: Where to Start

For many overburdened IT teams, the most challenging part of creating an end-to-end cybersecurity posture is identifying where to start. We've created the following guide to get you over this initial hurdle.

In this guide, you'll get answers to common early-stage cybersecurity questions that help you take the right next steps based on your needs.

1

Can a hacker on the Internet break into my network?

If this question is top of mind for your organization, perform an external penetration test.

An external penetration test emulates an attacker trying to break into your network from the outside. The goal of an engineer performing this assessment is to breach the perimeter and prove that they can gain access to the internal network. This test includes:

- Open source reconnaissance against the organization
- Full port scan covering all TCP ports and the top 1,000 UDP ports of the targets in scope
- Full vulnerability scan of the targets
- Manual and automated exploit attempts
- Password attacks

2

Have any new vulnerabilities popped up since my last full assessment?

Identifying and prioritizing vulnerabilities is the first step in managing risk for your organization. An external vulnerability scan identifies network-level vulnerabilities on your systems and assets that are exposed to the Internet. Whereas penetration testing includes manual identification, review, and exploitation of vulnerabilities, a vulnerability scan tries to simply identify issues in an automated fashion.

- Four quarterly scans on all externally available assets to be completed within one year
- Individual vulnerabilities prioritized with issue description, remediation, and reference links
- Technical Findings Report provided following each quarter's scan
- Does not include Executive Report or Presentation of Findings

3

Once an attacker breaks into my network, what damage can they cause? Also, if an internal employee goes rogue, what can they access?

Protecting "east-west" traffic within the network is a major priority for organizations today, which is why many teams are concerned with understanding where they're vulnerable in the event of a breach.

An internal penetration test emulates an attacker on the inside of your network. This could be either an attacker who is successful in breaching the perimeter through another method or a malicious insider. The goal of an engineer in this module is to gain root and/or domain administrator level access on the network, and gain access to sensitive files. Activities include:

- Active and passive network reconnaissance including traffic sniffing, port scanning, LDAP
- Enumeration and SMB enumeration
- Vulnerability scan on all in-scope targets
- Spoofing attacks such as ARP cache poisoning and LLMNR/NBNS spoofing
- Manual and automated exploit attempts
- Shared resource enumeration
- Password attacks

4

Is my web application secure, and what could an attacker do to my organization's website?

If application or website security is a concern for your organization, we suggest performing an in-depth vulnerability assessment and penetration test on both the unauthenticated and authenticated portions of the target web application. An engineer will test for all of the OWASP top 10 critical security flaws, as well as a variety of other potential vulnerabilities based on security best practice. Activities include:

- Network-level penetration testing of host server
- Website mapping techniques such as spidering
- Directory enumeration
- Identifying logic flaws and authorization bypasses
- Automated and manual tests for injection flaws on all input fields
- Directory traversal testing
- Malicious file upload and remote code execution
- Password attacks and testing for vulnerabilities in the authentication mechanisms
- Session attacks, including hijacking, fixation and spoofing attempts
- Other tests depending on specific site content and languages

5

Will my employees click a link or provide information on a call that will jeopardize my network?

The "human element" presents an oft-overlooked but complex challenge to cybersecurity.

A social engineering assessment is designed to target and take advantage of the human element to gain access to your network. This is done using a variety of methods to get an employee to click on something they shouldn't, enter or provide their credentials to an unknown individual/website, or divulge information that may assist an attacker in breaching your network. The goal for the engineer performing this assessment is to gain information that may assist an attacker in future attacks, gather credentials or gain a foothold on the internal network. This assessment will include:

- Phone-based attacks
- Spear-phishing attacks
- Bulk phishing attacks

6

Can a hacker break into my network from the parking lot?

A wireless penetration test is a comprehensive evaluation of the wireless networks in your organization using automated and manual methods. Areas covered include:

- Password attacks
- WEP/WPA cracking
- Guest wireless segmentation checks
- Traffic sniffing attacks
- SSID spoofing
- Rogue access point discovery

7

Can an attacker physically break into my building?

A physical penetration test is an assessment of the physical security of your premises. Our engineers will attempt to gain access to your facility by identifying weaknesses and/or using social engineering. Once inside, our engineers will attempt to gather sensitive information, gain access to sensitive areas such as the data center and attempt to gain internal network access.

8

Does my company comply with PCI DSS 3.2? Can you help my organization fill out an SAQ or prepare for our upcoming ROC?

If PCI compliance is a mandate at your organization, we recommend a PCI gap analysis before implementing any new cybersecurity technology.

During a PCI gap analysis, you will be paired with a certified PCI Professional (PCIP) to evaluate your company's compliance. If your company is required to fill out a Self-Assessment Questionnaire (SAQ), we will assist you in selecting the appropriate SAQ, determining the scope of PCI within your network, evaluating your current state of compliance and filling out the SAQ. If you are preparing for a Report on Compliance (ROC) audit, we will provide you with a full gap-analysis, identifying where you might fall short and providing the steps you need to take to become compliant before your final audit.

9

Does my security program provide adequate security as required by HIPAA/HITECH?

HIPAA and HITECH regulations also present unique challenges for organizations to address.

In a HIPAA/HITECH assessment, a comprehensive audit is conducted on all the ways electronic protected health information (ePHI) is stored, processed or transmitted on your network. A HIPAA/HITECH Gap Analysis will be a complete audit of your organization's:

- Physical safeguards
- Administrative controls
- Technical controls
- Security policies and procedures
- Organizational requirements
- Breach notification and incident response

10

Does my organization comply with NIST 800-53 or DFARS requirements?

Gauging your NIST 800-53 or DFARS compliance requires an interview-driven process which comprehensively explores your current security policies, procedures and techniques. During this process, a third-party will find the gaps in your NIST/DFARS compliance and provide a roadmap for meeting your compliance objectives.

Some of the topics our interviews will cover include:

- Physical security
- Security assessments
- Systems and communications protections
- Access controls
- Audit and accountability

11

Is my security program in-line with industry best practice?

This is one of the most common questions we hear regarding cybersecurity posture. A good place to start is performing an interview-based review of your information security program, using the Center for Internet Security (CIS) Top 20 Critical Security Controls as a metric. Some of the areas covered include:

- Inventory and asset management
- System hardening
- Account management and principle of least privilege
- Disaster recovery and continuity of operations
- Incident response

12

Do my employees understand how to help enforce organizational cybersecurity protocols, and are they aware of the ramifications of a breach?

One of your greatest defenses against breaches and cyberthreats is your employees, which is why it's so important that they understand best-practice procedures and preventative measures. Training is a great place to start.

We recommend training led by experts who can incorporate experiential details and practical advice that demonstrate the ramifications of employee actions to both their privacy and the organization as a whole. Optimal security awareness training will educate your employees to:

- Identify common indicators of an attack
- Understand ways to protect themselves
- Recognize the bypass of security controls
- Report potential incidents

13

Is my firewall configured according to best practice?

A firewall audit is a manual inspection of your firewall using the Center for Internet Security (CIS) benchmark and device-specific best practices. In addition, an engineer will review the firewall rules, searching for overly specific rules, proper rule sequencing or other gaps in your security posture. Finally, the firewall audit will include network scanning to validate its effectiveness.

14

Is my device in-line with industry best practice?

A host compliance audit involves the manual inspection of a workstation, server or network device using the Center for Internet Security (CIS) benchmark and device-specific security best practices. This assessment will identify the security holes in your system and provide specific actions to take to harden the device.

15

Are my employees choosing strong passwords? If not, what trends do they follow?

During a password audit, an engineer will evaluate the strength of passwords currently in use in your organization. This should include taking a dump of your employees' hashed credentials and run them through a password cracker in order to identify weak passwords and common usage patterns. This audit can be used to justify stronger password policies, used in security awareness training to improve password choice among employees and used to improve the organization's overall resilience if an attacker is able to capture hashed credentials.

16

Can you provide an overall risk assessment that matches our controls to our threats?

A formal risk assessment evaluates the threats to your organization, the vulnerabilities of your network and the security controls you have in place to protect your network. A risk assessment correlates information from your security assessments and evaluates the overall risk to your organization to help drive strategic decisions.

17

Is our cloud presence configured in-line with industry best practice?

This assessment is an evaluation of your organization's cloud infrastructure for security vulnerabilities. Our engineers will assist you in evaluating the unique security responsibilities associated with cloud computing. Individual services can include cloud application assessments, cloud infrastructure penetration testing, host/OS configuration audits and cloud architecture reviews.

18

Is my IoT device vulnerable to attack?

Developing a secure IoT solution depends on a number of security considerations that should be addressed and prioritized proactively. If IoT security is a concern for your organization, we recommend engaging an expert third-party to perform a comprehensive IoT assessment.

An IoT assessment will evaluate your devices and its associated infrastructure against common attacks. It can include an evaluation of the edge device, the gateway, the cloud infrastructure and/or any mobile applications. Engineers will evaluate your IoT Device utilizing the OWASP IoT Framework Assessment methodology.

19

Is an attacker still on my network? How did they get in, and what did they take?

When you suspect you have been breached, knowing exactly how it happened and what was affected can be difficult to discern. Certified engineers can assist you with the incident response process, ensuring the malware is removed and normal business operations are restored. Moreover, root-cause analysis will attempt to determine how the breach was possible and steps to take to prevent it from happening again. Moreover, we will evaluate the malware including:

- Open-source intelligence – We will evaluate the hash and any unique strings in the malware to see if they match known-malware signatures.
- Reverse-Engineering – Where possible, we will recreate the incident with advanced process monitors and determine the exact malware behavior.
- Log Analysis – Using the information gathered, we analyze the logs of affected devices to determine if the breach spread to other machines.

Ready for an Assessment?

If any of the areas mentioned in this guide are a priority at your organization, we can help you take the next step to an assessment. Visit ConRes.com/AssessMyIT to sign up for an assessment that fits your needs.

ConRes
CONTINENTAL RESOURCES