Cyber Security Defense Best Practices

Defense Against Digital Dark Arts

Sialkot Chamber of Commerce & Industry

Prepared By: Muhammad Farzad Ali
5-31-2021

Table of Contents

How to Defend Against Cyber Attacks

Security Goals

Good security defenses aren't just technical in nature. They are also procedural and policy-based.

If your company handles credit card payments, then you have to follow the Payment Card Industry Data Security Standard depending on local laws. It is broken into six broad objectives, each with some requirements. The objective is the end goal or what we'd like to achieve and the requirements are the actions that can help achieve that goal.

- The first objective is to **build and maintain a secure network and systems**. This includes the requirements to install and maintain a firewall configuration to protect cardholder data and to not use vendor supply default for system passwords and other security parameters.
- The second objective category is to **protect cardholder data**. In this objective, the first requirement is to protect stored cardholder data. The second is to encrypt the transmission of cardholder data across open public networks.
- The third objective is to maintain a **vulnerability management program**. The first requirement is to protect all systems against malware and regularly update antivirus software or programs. The second is to develop and maintain secure systems and applications.
- The fourth objective is to **implement strong access control measures**. This objective has three requirements. The first is to restrict access to cardholder data by business need-to-know to make sure that customer data isn't misused. The second is to identify and authenticate access to system components. And the third is to restrict physical access to cardholder data.
- The fifth objective is to **regularly monitor and test networks**. The first requirement is to track and monitor all access to network resources and cardholder data. This refers to things like setting up and configuring intrusion detection systems and conducting vulnerability scans of the network. The second is to regularly test security systems and processes. It's really helpful to test defense systems regularly to make sure that they provide the protection that you want. It also ensures that the alerting systems are functional.
- The sixth and final objective is to **maintain an information security policy**. It only has one requirement, to maintain a policy that addresses information security for all personnel. They help govern and regulate user behavior when it comes to information security aspects. It's important to call out that this requirement mentions that the policy should be for all personnel. The responsibility of information security isn't only on the security teams. Every member of an organization is responsible for information security.

Security is all about determining risks or exposure, understanding the likelihood of attacks; and designing defenses around these risks to minimize the impact of an attack.

Measuring and Assessing Risk

Security risk assessment starts with **threat modeling**. First, we identify likely threats to our systems, then we assign them priorities that correspond to severity and probability.

Another part of risk measurement is understanding what **vulnerabilities** are on your systems and network. One way to find these out is to perform regular vulnerabilities scanning.

Privacy Policy

Privacy policies oversee the **access and use of sensitive data**. They also define what appropriate and authorized use is, and what provisions or restrictions are in place when it comes to how the data is used.

Auditing data access logs is super important, it helps us ensure that sensitive data is only accessed by people who are authorized to access it, and that they use it for the right reasons. It's important for you to have an automated vulnerability scan conducted regularly.

You'll need to keep the vulnerability database up to date, to make sure new vulnerabilities are detected quickly. Conducting regular penetration tests is also really encouraged to test your defenses even more. The results of the penetration testing reports will also show you, where weak points or blind spots exist. These tests help improve defenses and guide future security projects.

Data handling policies should cover the details of how different data is classified. If something is considered sensitive or confidential, you probably have stipulations that this data shouldn't be stored on media that's easily lost or stolen, like USB sticks, portable hard drives, mobile phones and tablets.

Users

You can build the world's best security systems, but they won't protect you if the users are going to be practicing unsafe security. You should never upload confidential information onto a third-party service that hasn't been evaluated by your company.

Users don't like to memorize long complicated passwords, but this is super important to keeping your company safe. It's also important to have a password change system check against old passwords. A much greater risk in the workplace that users should be educated on is credential theft from phishing emails. If an email that seems authentic actually leads to a fake login page, users can blindly enter their credentials into the fake site and disclose their credentials to an attacker.

You can also combat phishing attacks with good spam filtering combined with good user education. You can help influence good user behavior by offering security training.

Third-Party Security

It's important to hire trustworthy and reputable vendors whenever you can. You also need to manage the engagements in a controlled way. This involves conducting a vendor risk review or security assessment. In typical vendor security assessments, you ask vendors to complete a questionnaire that covers different aspects of their security policies, procedures and defenses.

It's important to understand how well-protected your business partners are, before deciding to work with them. If they have poor security practices, your organization's security could be at risk. If you contract services from a company that will be handling data on your behalf, the security of your data is in the hands of this third party.

Security Training

It's impossible to have good security practices at your company if employees and users haven't received good training and resources. This will boost a healthy company culture and overall attitude toward security. Creating a culture that makes security a priority isn't easy. You have to reinforce and reward behaviors that boost the security of your organization.

Making employees retake the training every once a year or so, ensures that everyone's up-to-date on their training. You can also cover new concepts or updated policies when needed. This type of training should cover the most common attack types and how to avoid falling victim to them. This includes things like phishing emails and best practices around password use.

Incident Reporting and Analysis

Regardless of the nature of the incident, proper incident handling is important to understanding what exactly happened, and how it happened and how to avoid it from happening again.

The very first step of handling an incident is to detect it in the first place by intrusion detection systems, an employee may have noticed something suspicious and reported it to the security team for investigation.

The next step is to analyze it and determine the effects and scope of damage. Once the scope of the incident is determined, the next step is containment. You need to contain the breach to prevent further damage. Containment strategies will vary depending on the nature of the incident. If an account was compromised, change the password immediately. If the owner is unable to change the password right away, then lock the account. If it's a malware infection, can our anti-malware software quarantine? Or remove the infection? If not, the infected machine needs to be removed from the network as soon as possible to prevent lateral movement around the network.

Attackers will usually try to cover their tracks by modifying logs and deleting files, especially when they suspect they've been caught. They'll take measures to make sure they keep their access to compromised systems. This could involve installing a backdoor or some kind of remote access malware. With effective logging configurations and systems in place, these activities would show up in audit logs. So this type of access should be detected during an incident investigation.

Another part of incident analysis is determining severity, impact, and recoverability of the incident. It might not be possible to recover from the damage at all. In some cases, depending on backup systems and configurations, some data may be lost forever and can't be restored. Backups won't contain any changes or new data that were made after the last backup run.

Incident Response and Recovery

Once a threat has been detected and contained, it has to be removed or remediated. When it comes to malware infection, this means removing the malware from affected systems. But in some cases, this may not be possible, so the affected systems have to be restored to a known good configuration. This can be done by rebuilding the machine or restoring from backup. Take care when removing malware from systems because some malware is designed to be very persistent, which means it's resistant to being removed.

When all traces of the attack have been removed and discovered and the known vulnerabilities have been closed, you can move on to the last step. That's when systems need to be thoroughly tested to make sure proper functionality has been restored. It's important to incorporate the lessons you've learned from any incident into your overall security defenses. Stay vigilant and prepared to protect your system from attacks.