Peer-graded Assignment: Creating a Company Culture for Security

A small fictional organization has a growing employee base with 50 employees in one office. The company is an online retailer of high quality artisanal, hand-crafted widgets. Since this company handles user payment data, the organization is extra cautious about privacy.

Add security measures to the following systems.

1.) An external website permitting users to browse and purchase widgets

For the authentication system we're going to set up a OTP security policy that requires non-dictionary words, an 8 character length specification, uses special characters, and enforces password rotation at least every 6 months. This will provide protection against brute force attempts and potential phishing.

For our external website security we will enable HTTPS in our domain so that data transfered over the website stays private. This can be done through enabling SSL/TLS after aquiring an online certificate. Most file hosting companies offer this service for free in the control panel. TLS, or Transport Layer Security, is the most up to date version of the original SSL, or Secure Socket Layer, security protocol and supports the most up to date cipher suites and encryption algorithms.

2.) An internal intranet website for employees to use

Getting started we would want to set up an Active Directory server for our internal infrastrucure configurations. We'll then want an OTP-based multifactor for employees secure login along with clear policies on company security and security training requirements. Employees will use the same password requirements as on the external website.

Now, in order to secure internal network security we will have to set up Antimalware protection and third party vulnerability scanners. These both use a progressive database to ensure any known threats and vulnerabilities can be automatically resolved by the security system if detected.

We will need to set up intrusion detection and prevention for systems containing customer data. The IDS/IPS will have to be configured in line with traffic being monitored as well as their alerts to any atypical internal network behavior. Similarly, IPS firewall rules will need to be configured to terminate bad traffic on the network.

Finally, customer data management must meet the requirements of the PCI DSS or Payment Card Industry Data Security Standards. PCI DSS has six objectives: build and maintain a secure network/systems, encrypt the transmission of customer data across open public networks, maintain a vulnerability management program, implement strong access control, monitor and test networks, and maintain an information security policy.

3.) Secure remote access for engineering employees

In order so that employees will have access to company resources anywhere, we will set up either a VPN or a reverse proxy as a remote access solution. We can configure its Access Control Lists (ACLs) to grant authorization for who needs.

We'll also want to segregate our VLAN's per their specific utility for Engineering, Sales, Infrastructure, and Guests. The VPN clients network should be separate through VLAN configurations or subnetting.

Separating our VLAN's like this gives us further control and accountability of important data.

4.) Reasonable, basic firewall rules

We'll need host-based firewall rules in order to mitigate attack surfaces and prevent access to anything on the network that's not necessary. Firewall configuration should begin using the concept of Implicit Deny allowing access to only these necessary services. This prevents a connection with any specific networks or IP ranges.

5.) Wireless coverage in the office

For the wireless security we'll implement 802.1X or WPA2 wireless encryption in order to securely authenticate users to the network. This can be done easily with setting up a RADIUS server for wireless authentication

Maintain security recommendations that ensure company policies promote a security culture. Educating employees regularly through security training is one of the most effective ways to ensure basic security procedures.

It's also vital to have privacy policy recommendations that will establish a company policy on accessing and storing critical user information. This policy usually includes a method for accessing customer data and stipulations on how it can be used, when, and for what duration. It should also define the classification of customer data types into tier'd security categories in order to document proper procedures for how those types of data are stored and accessed.

6.) Reasonably secure configurations for laptops

The laptop security policy will require company laptops and mobile devices to use Full Drive Encryption (FDE) in case of being lost or stolen. An example of this is Veracrypt Full Drive Encryption which fully protects the drive's data without the key. Also, devices must maintain Antivirus with current updates and security patches.

Some application policy recommendations are to implement a possible binary whitelist solution to prevent any additional attack surfaces. This would allow only applications deemed necessary to company production to be used. It is also required for regular software updates when available to counter any discovered security vulnerabilities.