Google IT Support Certificate: Course 5: IT Security - Defense Against the Digital Dark Arts

Week 6: Creating a Company Culture for Security

Creating a Company Culture for Security - Design Document

Overview: Now that you're super knowledgeable about security, let's put your newfound know-how to the test. You may find yourself in a tech role someday, where you need to design and influence a culture of security within an organization. This project is your opportunity to practice these important skillsets.

Assignment: In this project, you'll create a security infrastructure design document for a fictional organization. The security services and tools you describe in the document must be able to meet the needs of the organization. Your work will be evaluated according to how well you meet the organization's requirements.

About the organization: This fictional organization has a small but growing employee base, with 50 employees in one small office. The company is an online retailer of the world's finest artisanal, hand-crafted widgets. They've hired you on as a security consultant to help bring their operations into better shape.

Organization requirements: As the security consultant, the company needs you to add security measures to the following systems:

- An external website permitting users to browse and purchase widgets
- An internal intranet website for employees to use
- Secure remote access for engineering employees
- Reasonable, basic firewall rules
- Wireless coverage in the office
- Reasonably secure configurations for laptops

Since this is a retail company that will be handling customer payment data, the organization would like to be extra cautious about privacy. They don't want customer information to fall into the hands of an attacker due to malware infections or lost devices.

Engineers will require access to internal websites along with remote, command-line access to their workstations.

Grading: This is a required assignment for the module.

What you'll do: You'll create a security infrastructure design document for a fictional organization. Your plan needs to meet the organization's requirements, and the following elements should be incorporated into your plan:

- Authentication system
- External website security
- Internal website security
- Remote access solution
- Firewall and basic rule recommendations
- Wireless security
- VLAN configuration recommendations
- Laptop security configuration
- Application policy recommendations
- Security and privacy policy recommendations
- Intrusion detection or prevention for systems containing customer data

My Response:

1. Authentication system:

Authentication will be handled centrally by an LDAP server and will incorporate One-Time Password generators as a second factor for authentication.

2. External Website Security:

The customer-facing website will be served via HTTPS since it will be serving an e-commerce site that permits visitors to browse and purchase products, as well as create and log into accounts. This website would be publicly accessible.

3. Internal Website Security:

The internal employee website will also be served over HTTPS, as it will require authentication for employees to access. It will also only be accessible from the internal company network with an authenticated account.

4. Remote access solution:

Since engineers require remote access to internal websites, as well as remote command line access to workstations, a network-level VPN solution will be needed, like OpenVPN. To make internal website access easier, a reverse proxy is recommended in addition to a VPN. Both of these would rely on the LDAP server that was previously mentioned for authentication and authorization.

5. Firewall and basic rule recommendations:

A network-based firewall appliance would be required. It would include rules to permit traffic for various services, starting with an impact deny rule and then selectively opening ports. Rules will also be needed to allow public access to the internal website and to permit traffic to the reverse proxy server and the VPN server.

6. Wireless security:

For wireless security, 802.1X with EAP-TLS should be used. This would require the use of client certificates, which can also be used to authenticate other services like VPNs, reverse proxy servers, and internal website authentication. 802.1X is more secure and easier to manage as the company grows, making it a better choice than WPA2.

7. VLAN configuration recommendations:

Incorporating VLANs into the network structure is recommended as a form of network segmentation. It will make managing access to various services easier. VLANs can be created for broad roles or functions for devices and services. An engineering VLAN can be used to place all workstations and engineering services

on it. An infrastructure VLAN can be used for all infrastructure devices, like wireless APs, network devices, and critical servers like authentication. A Sales VLAN can be used for non-engineering machines, and a Guess VLAN would be useful for other devices that don't fit the other VLAN assignments.

8. Laptop security configurations:

As the company handles payment information and user data, privacy is a big concern. Laptops should have full disk encryption (FDE) as a requirement to protect against unauthorized data access if the device is lost or stolen. Antivirus software is also strongly advised to avoid infections from common malware. To protect against more uncommon attacks and unknown threats, binary whitelisting software is recommended in addition to antivirus software.

9. Application policy recommendations:

To further enhance the security of client machines, an application policy should be in place to restrict the installation of third-party software to only applications that are related to work functions Specifically, risky and legally questionable application categories should be explicitly banned. This would include things like pirated software, license key generators, and cracked software. In addition to policies that restrict some forms of software, a policy should also be included to require the timely installation of software patches. "Timely" in this case will be defined as 30 days from the wide availability of the patch.

10. Security and privacy policy recommendations:

As the company takes user privacy very seriously, some strong policies around accessing user data are a critical requirement. User data must only be accessed for specific work purposes related to a particular task or project. Requests must be reviewed and approved before access is granted. Only after review and approval will an individual be granted access to the specific user data requested. Access requests to user data should also have an end date. In addition to accessing user data, policies regarding the handling and storage of user data are also important to have defined. These will help prevent user data from being lost and falling into the

wrong hands. User data should not be permitted on portable storage devices like USB keys or external hard drives. If an exception is necessary, an encrypted portable hard drive should be used to transport user data. User data at rest should always be contained on encrypted media to protect it from unauthorized access. To ensure that strong and secure passwords are used, the password policy below should be enforced:

- Password must have a minimum length of 8 characters.
- Password must include a minimum of one special character of punctuation.
- The password must be changed once every 12 months.

In addition to these password requirements, mandatory security training must be completed by every employee once a year. This should cover common security-related scenarios, like how to avoid falling victim to phishing attacks, good practices for keeping your laptop safe, and new threats that have emerged since the last time the course was taken.

11. Intrusion detection or prevention for systems containing customer data:

A Network Intrusion Detection System is recommended to watch network activity for signs of an attack or malware infection. This would allow for good monitoring capabilities without inconveniencing users of the network. A Network Intrusion Prevention System (NIPS) is recommended for the network where the servers containing user data are located. It contains much more valuable data, which is more likely to be targeted in an attack. In addition to Network Intrusion Prevention, Host-based Intrusion Detection (HIDS) software is also recommended to be installed on these servers to enhance monitoring of these important systems.