Final Project - Sample Submission

Authentication

Authentication will be handled centrally by an LDAP server and will incorporate One-Time Password generators as a 2nd factor for authentication.

External Website

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

Internal Website

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 and only with an authenticated account.

Remote Access

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 VPN. Both of these would rely on the LDAP server that was previously mentioned for authentication and authorization.

Firewall

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

Wireless

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 VPN, reverse proxy, and internal website authentication. 802.1X is more secure and more easily managed as the company grows, making it a better choice than WPA2.

VLANs

Incorporating VLANs into the network structure is recommended as a form of network segmentation; it will make controlling access to various services easier to manage. VLANs can be created for broad roles or functions for devices and services. An engineering VLAN can be used to place all engineering workstations and engineering services on. 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 Guest VLAN would be useful for other devices that don't fit the other VLAN assignments.

Laptop Security

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 a 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.

Application Policy

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.

User Data Privacy Policy

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 made for specific pieces of data, rather than overly broad, exploratory requests. 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.

Security Policy

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 or punctuation
- Password must be changed once every 12 months

In addition to these password requirements, a mandatory security training must be completed by every employee once every 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.

Intrusion Detection or Prevention Systems

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.