Congratulations! You passed!
TO PASS 80% or higher

Keep Learning

GRADE
100%

Creating a Company Culture for Security - Design Document

LATEST SUBMISSION GRADE
100%

1. **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.

   1 / 1 point

   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 met 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 falling 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 rules 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

   External website security

   This is for external website to perform purchase activity by customers.

   To provide a secure e-commerce transaction, our security goals have to include the following:

   * Verifying the authenticity of a person to perform a secure transaction.
   * Making sure that unauthorized persons or systems are unable to access the information of users.
   * Protecting confidentiality of the customers data.
   * Making the data accessible and usable.
   * Logging the transactions for further reference and support activity.

   Internal website security

   This is for intranet website accessed by the company employees.

   The intranet website should only be accessed by the company employees.

   In order to do that, our security goal have to include the following:

   * Making sure that the access is only within their intranet by implementing a firewall mechanism.
   * Specifying the authentication mechanism to access the website by the company employees.
   * Supervising the activities and user management on the website by a company's system administrator.

   Remote access solution

   We need to perform a secure remote access control to some company's employees.

   We need to define the following:
   * What device requires the remote access?
   * What remote access is appropriate for the role given the device used?
   * Is the employee going to access from a public location, another company site, internal wireless, etc.?

   Does the need for strong authentication increase based on the device used, where it is used, and what it is allowed to access?

   Firewall and basic rules recommendations

   The Basic Firewall rules to be implemented are the following.

   Block by default: We have to block all incoming and outgoing connections.

   Allow specific traffi: We only have to allow specified IP addresses.

   Allow Inbound-only: We have to allow Intranet users

   Wireless security

   Wireless coverage in the company's office.

   We can configured a login based limited access to company Wi-Fi by the employees.

   The connection must be Password protected and could be metered.

   VLAN configuration recommendations

   We have to create security zones for the remote user.
   Should separate incoming traffic from internal resources.
   Could use dynamic VLAN assignments and ACLs.

   Laptop security configuration

   We have to secure the laptop that uses the company's employees.
   These laptops can be responsible for bringing in viruses and causing the organization to lose sensitive data.

   So we must:
   * Encrypt the disks on the laptops.
   * Ensure Antivirus are always up to date.
   * White listing the devices on the network.

   Application policy recommendations

   * Perform automated application security testing.
   * Compliance with industry standard data policies and protocols.
   * Integrate secure coding principles in all software components.

   Security and privacy policy recommendations

   * Contact Information: Make it easy for your customers to contact you or file a complaint.
   * How organization will Share Customer Information: Customers need to know that their data will only be used to complete the transaction and nothing more.
   * Cookie Policy: Explain your cookie practice.
   * Make sure new customers or users have easy access to your policy.

   Intrusion detection or prevention for systems containing customer data

   We have to implement security methodologies up to date for the growing e-commerce market.
   This is an difficult task to do, but it can be achieved through some practices such as reverse engineering and/or penetration testing.

   Correct

   Thank you for your submission!

   A great submission should include:

   - Two authentication system requirements, like Security Key-based multifactor or OTP-based multifactor, and some kind of centralized authentication system (e.g., LDAP or Active Directory).
   - A description of HTTPS.
   - Recommendation for both a VPN service and a reverse proxy solution.
   - A description of two or more types of firewall services (e.g., implicit deny rule, remote access, websites).
   - Requirement for 802.1X.
   - A description of four VLAN requirements, including Engineering VLAN, Sales VLAN, Infrastructure VLAN, and Guest VLAN.
   - Three laptop security requirements, including FDE recommendations, antivirus recommendation, and a binary whitelisting recommendation.
   - Requirement for a software update requirement policy and a requirement for restrictions on the types of applications permitted.
   - Recommendations for rules protecting access to user data and for rules protecting the storage of user data.
   - A description of four of the following security policy recommendations: passwords requiring a minimum of 8 characters; passwords requiring special characters; requiring periodic password changes > 6 months; and some form of mandatory security training for users.
   - A requirement for a NIPS/NIDS on the network for customer data and a requirement for HIPS/HIDS on systems containing customer data.