Case Study and Course Project

ABC Case Study and Course Project Requirements

Overview

- Data security is of vital importance to the continuation of any organization. But data is only as secure as the controlled access to that data is strong. Access control covers all three pillars of information security. Strong access control supports confidentiality as only people and devices with authorized permissions can access data. It supports integrity as data can be changed only by those with authorization to do so. And it supports availability, allowing people and devices needing access to data and assets to have it.
- Creating software that is free of vulnerabilities should be the goal of every software development company. Although this lofty goal may not be possible in practice, organizations can, through secure design, validation, testing, and auditing throughout the software development lifecycle and in the development environment, to come as close as possible.

The Course Project: This Security Report will be complete through the submission of individual parts each week throughout the course, with the final Security Report due at the end of Week 6.

-

You are tasked with writing a security report to the Chief Information Officer of a fictitious company, ABC Software Inc. Based on the organization's current situation and make-up, you will create a 12-15 page report in which you:

- Discuss at least 10 areas of ABC Software in which strong access control is needed, and why it is needed
- Using access control best practices, recommend at least 8 methods and techniques to identify and authorize **people** to control physical and logical access to data and assets
- Using access control best practices, recommend at least 3 methods and techniques to identify and authorize **devices** to control physical and logical access to data and assets
- Discuss at least 5 possible threats to a secure software development environment at ABC Software
- Recommend solutions to these threats
- Discuss possible at least 5 possible issues and threats to creating secure programs
- Recommend solutions for these threats for programmers and coders to be implemented throughout the Software Development Life Cycle (SDLC)

- Recommend at least 4 types of security tests and assessments to be applied to completed programs before general release.

Refer to the Final Assessment Template below for an exact description of your Security Report, and the Weeks in which various parts are due.

This Security Report will be completed through the submission of individual parts each week throughout the course, with the final Security Report due at the end of Week 6.

Items Required for Final Submission

- A 12-15 page security report that includes:
- Proper APA formatting of the report
- A minimum of ten (10) valid references and associated in-text citations

Case Study – ABC Inc.

You work for Security Consulting Associates (SCA). Recently, one of your clients, ABC Software (ABC), located in Tampa, FL, has called with a big problem. Some of their network servers were compromised, resulting in the possible loss of personal information and credit card numbers of purchasers of the software products produced by the company. It is not known at present whether this attack came from inside the company, or outside. ABC is currently dealing with this problem as best they can, but they need your company to help them to prevent this from happening in the future. Your manager has assigned this project to you, the new consultant. In researching ABC, you find that the company has the following setup:

1. A wired network of 300 users segmented into the following departments
    1. Executive Management
    2. Research and Development
    3. Human Resources
    4. Sales and Marketing
    5. Purchasing and Billing
    6. Warehousing and Order Fulfillment
    7. Information Technology and Security
    8. Facilities Management

2. A wireless network available to all internal users, with a separate segment available for use by visitors and non-registered users
3. A Website used for Advertising, and Marketing with a secure section for ordering and payments
4. Remote Access capabilities for users working from home or on the road
5. A system of routers and switches and firewalls that protect the network from outside intrusions, and segment the network into subnets for each department
6. A demilitarized zone (DMZ) in the network which includes the Web Server and Email Server

Your research has also yielded the following information about ABC:

1. The key business processes include the following:
    1. The development of new programs including applications for business and gaming
        1. This process is core to the company's success. It is extremely important that company secrets do not get out as the competition in the software and gaming industry is fierce. A short outage in this area would not prove critical, but downtime of more than a couple of days could postpone the release of new or improved products
    2. The marketing of their products to business and personal users
        1. This process is crucial to the company's success, but again, a short outage would not critically impact the company. But a lack of marketing lasting any more than a week could begin to adversely affect the bottom line.
    3. The online sales of their products to businesses and consumers
        1. It is of utmost importance that out online purchasing system is secure with a near 100% uptime rate. If there are security breaches, it will erode customer confidence in ordering online. If there are web outages lasting any longer than a few minutes, customers may move on to another site to purchase competing products.
    4. The direct sales of their products to distributors and retail outlets
        1. Again, It is of utmost importance that the direct sales purchasing system is secure with a near 100% uptime rate. If there are security breaches in the customer database, it will erode customer confidence in ordering from ABC. If there are database and/or ordering system outages lasting any longer than a few minutes, customers may lose confidence in the company in general, and salespeople in particular, when their orders cannot be placed
    5. The fulfillment of orders placed by businesses and consumers
        1. This system and database needs to be secure as well. Regarding uptime, the maximum tolerable outage is one day or less. Customers can understand a slight delay due to technical issues, but any longer than that may result in them not ordering from ABC in the future. Also, any downtime will result in fulfillment warehouse crews being paid for not working, which affects the bottom line.
    6. The billing of customers for purchase made via direct sales.
        1. Again, the maximum tolerable downtime for this system is one day or less. The longer it takes to bill customers, the longer it take to receive payment, and the less cash on hand for the business.

7. The payment of salaries and commissions to employees and salespeople.
    1. Employees and salespeople are paid twice each month – once on the 15th, and once on the last day of the month. Missing a pay date can be disastrous for a company with regard to employee satisfaction and morale. This system can never be down for more than one day, and never around the 15th or last day of the month. And since paystubs contain personal information such as social security numbers and year-to-date payroll information, data security is obviously a very high priority, as is data integrity.

A large amount of data that is stored on the network in the following manner:

1. File Server - General – Data that is available to most employees including:
    1. Meeting notes
    2. Company presentations
    3. Marketing materials
    4. Training modules
    5. Departmental reports
    6. Organizational Charts
    7. Budget Reports
2. Human Resources Server – Private employee data and information such as:
    1. Names and Addresses
    2. Social Security Numbers
    3. Payroll Information
    4. Years of Service
    5. Benefits Information
3. Business Server including data such as:
    1. Customer database and Billing Information
    2. Orders and Fulfillment Database
4. Application Server including:
    1. Programs developed in-house for sale to clients and customers
    2. New development projects
5. Backup Servers with tape backups on removable media.

A site survey of the facilities and site on which it sits has revealed the following:

1. Exterior
    1. The building is owned by ABC Software, is a free-standing building, and there are no other tenants
    2. The site on which the building sits in in an industrial park in Tampa, Fl. with no fencing or separators from other free-standing buildings.
    3. The employees of ABC park in an open lot next to the building. The lot has no apparent security mechanisms in place.
    4. Employees enter the building through a side entrance and are let in by swiping a card

5. The building itself is armed with a central station alarm system that is tied directly into the local police station.
6. Last year, a hurricane hit the Tampa area. Although ABC suffered no damage, some of the other buildings in the industrial park suffered various levels of damage from the storm.
7. There have been a small number of vandalism complaints in the past two years including graffiti painted of the exterior walls of two of the buildings in the industrial park, and employees' cars being vandalized at night in another.

2. Interior
    1. The building is one-story with all offices and departments located in the first floor.
    2. Three nights each week, the doors to the offices and departments are left unlocked so that the cleaning crew can clean these areas.
    3. Clients and others can enter the building though the main entrance, which is unlocked between the hours of 9:00 AM and 5:00 PM. The main entrance opens to an open reception area where a receptionist greets them. There is a locked door between the reception area and the rest of the building that the receptionist can open with a buzzer system.
    4. The building's electrical system was last updated 7 years ago, but has been functioning well except for two instances in the past year when the power went out. The first time was the result of a hurricane that hit the area and the power was out for three days. The second time was last summer when a heat wave caused an extreme usage of power in the area, and the power went out for eight hours. Because of these two events, ABC has been looking into installing a backup generator. They have not had one to this point.
    5. The building has a sprinkler system in case of a fire. The system is water-based, and because of this, has been de-activated in the server room and data center. To protect the servers and equipment there is an older dry fire suppression system installed in those rooms.

Additionally, ABC is concerned about the security of the software programs that their Research and Development Department produces and sells. As previously noted, the development of new programs including applications for business and gaming is the number one business process for ABC. This process is core to the company's success. They would like some recommendations regarding the security of these programs. Not only are they interested in keeping company secrets from getting out (as the competition in the software and gaming industry is fierce), but they want to be sure that the software they create is secure and as free from vulnerabilities as possible. After all, if they become known for releasing software that is full of vulnerabilities and holes, they won't be in business too long.

Final Assessment Template

1. Introduction (Week1)
    1. Overview of scenario and purpose of this report

2. Using information gleaned from the Case Study, textbook readings, assigned competency readings, and your own research, discuss all of the areas (**at least 10**) of ABC Inc. in which strong access control is needed, and why it is needed (Week 1).
    1. Include in your discussion networks, subnets, devices (servers, routers, switches, intranets, internets, etc.), and any other areas where strong access control is needed
3. Using information gleaned from the Case Study, textbook readings, assigned competency readings, and your own research, recommend the implementation of access control methods and techniques (**at least 8**) to identify and authorize **people** to control physical and logical access to data and assets (Week 2)
4. Using information gleaned from the Case Study, textbook readings, assigned competency readings, and your own research, recommend the implementation of access control methods and techniques (**at least 3**) to identify and authorize **devices** to control physical and logical access to data and assets (Week 2)
5. Using information gleaned from the Case Study, textbook readings, assigned competency readings, and your own research, recommend **at least 4** types of security tests and assessments to be applied to completed programs before general release to ensure the security of these programs and applications. (Week 3)
6. Using information gleaned from the Case Study, textbook readings, assigned competency readings, and your own research, discuss **at least 5** possible threats and attacks that could compromise software programs, and recommend solutions to these possible issues to be implemented to ensure secure application and program development (Week 4).
7. Using information gleaned from the Case Study, textbook readings, assigned competency readings, and your own research, discuss possible threats (**at least 5**) to a secure software development environment, and recommend solutions for these (Week 5).
8. Summary and Final Security Report (Week 6)
    1. Present a summary of your report, and the Final Submission of your Security Report for ABC Software, Inc.