Activity File: Considering Security and Business Objectives

In this activity, you'll play the role of a security consultant hired to help a financial services firm called GeldCorp decide how risky its business plans are.

- GeldCorp has provided a list of business plans. They want you to explain the security implications of each one and advise which projects they should pursue and which they should cancel.
- In addition, they've included their security department's recommendations for making the organization more secure. They've asked that you review these and tell them which suggestions are good and which are too extreme.

Instructions

For each suggestion, consider the following:

- Whether it leads to improved or reduced security.
- Whether the improvement in security is worthwhile. (What are the advantages and why do they matter?)
- How much work will it take to implement.

Then, determine if the business should proceed with the project, and briefly explain your decision.

Business Plans

GeldCorp provided the following business plans and security suggestions below:

1. The business wants to give all developers access to all data.
    - This request was made by the director of engineering. They suggest that the free access will help their teams move faster and help managers cut costs by delegating work more efficiently.

2. The director of IT wants to make administration servers accessible from public IP addresses, instead of just from within the corporate subnets.
    - Typically corporate/company networks are not publicly accessible on the internet, and are instead put behind a gateway that opens only for those with access.
    - The director of IT argues that allowing anyone to access machines on the company's network will help their administrators, many of whom work remotely, to connect to the servers they need to manage. They expect this feature to improve retention and hope to gain an increase in number of hours worked by employees.
3. Your newest SOC analyst wants to merge all email servers into a single database, hosted on a single machine.

    Currently, your company saves emails to several different mail servers. (A mail server is a machine that stores emails: When you send someone an email, it doesn't go to their computer, it goes to the mail server, where it's stored in a database. Then, when you want to read your emails, you log into the mail server, and it gives you a list of every email sent to you.)
    - The analyst argues that this setup will improve efficiency by making it easier to monitor the database, and save money by reducing the number of machines on the network.

Security Recommendations

GeldCorp provided the following recommendations from its security department.

1. The director of security suggested implementing a private corporate VPN.
    - A VPN is a gateway that sits between the private corporate network and the Internet. Every time someone tries to access a site on the internal company network, the VPN "tests" the request to determine if it's coming from an employee. If it is, the request is approved.
    - Since the company has grown to over 300 employees, the director argues that it's increasingly critical to ensure confidential information remains hidden.
    - The VPN project would require significant changes to the company's networking infrastructure and onboarding all employees with the VPN. This would mean making sure that everyone has keys to prove they're an employee.
    - The advantage is that the business would have better control over communications to

and from its core networks.

2. The director of engineering suggested requiring all developers to use SSH keys instead of passwords to communicate with internal SSH servers. They plan to block password access in two weeks.

    - **Note:** We'll cover SSH in a later unit. For now, know that SSH is a way to log into a remote computer and run commands on it. You can log in using an SSH password, but because passwords can be cracked, it's preferable to use SSH cryptographic keys to log in via SSH.

3. In addition to merging mail servers, your SOC analyst suggested hardening the server in the following ways:

    a. Encrypting all stored emails.

    - Suppose an attacker breaks into the mail server and downloads every email on it. This would include sensitive information about projects and finances, which could lead to potentially catastrophic leaks.

    - But if the attacker breaks in and downloads encrypted emails, they will be unable to access the information inside, since the text will be illegible. In other words, encrypting the data ensures that attackers can't do anything with it, even if they steal it.

    b. Only allowing machines on the corporate network (or VPN) to download mail.