Final Project

Bo Nappie

Cybersecurity

Section 1: Executive Summary

Abstract:

This report is on a case study of a startup company. The report has been curated from the perspective of a consultant who has been sought out by the startup company for advice and recommendations about securing the confidentiality, integrity, and availability of data and their application.

The startup company is developing a *subscription-based application for time management* where users are able to define TODO items and then track time that is spent on completing them. The company currently employs 25 individuals who work from home. The company also has a small corporate office with a data center.

This report consists of details, models, and analysis regarding recommended authentication systems, access controls, threat models, and the complete architecture of the system recommended for this startup company. The system and recommendations were designed to fit within the startup's annual budget of $325,000.

Given a budget of $325,000 per year, choose from the controls listed below. **Explain why** you chose each control, **what its function is**, and **what the overall application's architecture looks like once you have implemented all of your recommendations.**

Control	Cost per year
Chief information security officer	$200,000
Information security engineer	$125,000
Information security analyst	$100,000
Virtual Private Network	$10,000
Firewall (each)	$25,000
Phishing Awareness Training	$20,000
Antivirus/Endpoint Protection	$20,000
Patch management platform	$20,000
Vulnerability scanning service	$10,000
Whole disk encryption (per device)	$1,000
TLS encryption (per server)	$1,500
Penetration test (per engagement)	$30,000
Threat Intelligence Subscription	$30,000
Cloud Security Platform	$40,000
Multi factor Authentication Service	$25,000
Additional Security Consultancy	$20,000

Section 2: Environment

Description of the environment

The startup is developing a subscription-based application for time management where *users are able to define TODO items and then track time they spent on completing them.*

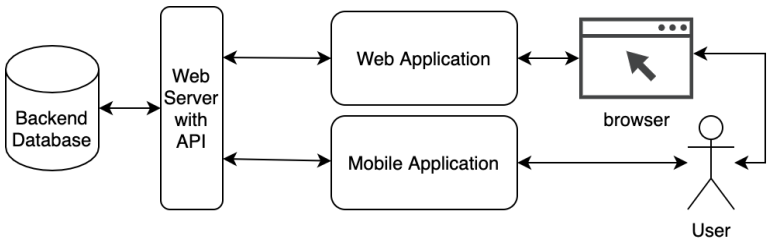
Prior to a user having access to utilize the application, the user must first register on the application by providing basic information, including their name, email address, phone number, and credit card details, in addition to creating login credentials such as a username and a form of authentication such as a password & face ID. Users can then begin to interact with the application through either a mobile app, or through a browser via a website.

Users of the app will be able to create a title, a description, a deadline, and an estimate of how much time it is expected to take for each TODO item. Users will also have the ability to assign TODO items to other users of the platform, given they are granted access to do so.

Data, including information regarding users' names, email addresses, and credit card details are stored in the backend database and is accessed via an API (Application Programmer's Interface). The architecture is visually displayed in the diagram below.

It is expected that the organization needs an infrastructure of approximately 15 servers during its startup stage.

The startup is run by 25 employees who work from home. Every employee is provided with a computer and a cell phone. The startup also houses a small corporate office with a data center.



Visual of the general architecture of the application

Section3: Authentication Subsystem Description

Cost for authentication subsystem:

$25,0000 – Multifactor authentication

Description:

Authentication is a primary line of defense to protecting data. **Multifactor authentication** is strongly recommended when users and employees are attempting to prove their identity in order to utilize the application.

Means of verifying a user's identity can be achieved through utilizing a password, a token, or a biometric. Each of these on its own are generally much weaker and more susceptible to being hacked, resulting in a breach of data.

When requiring two separate factors of verification to authenticate a user/employee, it becomes exponentially more difficult for a successful authentication attack to occur. This investment alone will mitigate the potential for an attack that occurs all too often on many other platforms that do not utilize multifactor authentication.

It is recommended in this case, that both users and employees are required to create a password that is *at least* 8 characters long, that includes *at least* one uppercase letter, number, and special character.

As a second form of authentication, it is recommended to utilize a biometric device for a facial scan. Given that all employees are provided with a cell phone and computer, and that many phones already have a biometric device, this factor should not be difficult to implement.

In the event that the user does not have a biometric device available, after the user provides the correct password, they will be given an option to send a token based code to the registered email or phone number that is linked to the account; once the user decides where to send the token based code to, a time limit will be enabled, and the user must obtain the code and enter it on the application within that time frame for the code to be valid.

Section 4: Access Control Model Description

Costs for access control:

$125,000- Information Security Engineer
$100,000- Information Security Analyst
total: $225,000

Description:

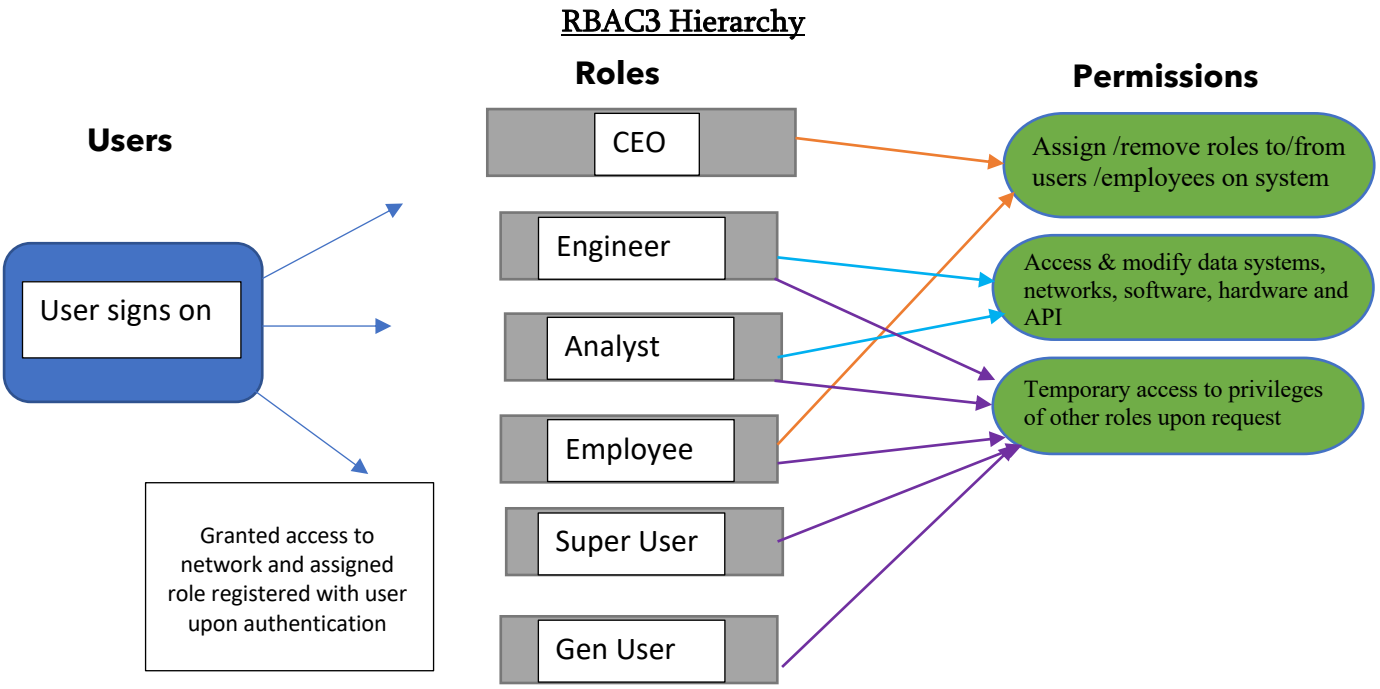
Access control systems work to prevent any unauthorized use of a resource, including using a resource in an unauthorized manner. Authorization is the process in which permissions are granted, access control is the process of which permissions are enforced. A role represents the job function and a description of the authority and responsibility of that role

It is suggested that the design for this application follow a the RBAC3 model, which implements both hierarchies and constraints in its design. Role Based Access Control Systems follow a principal of least privilege, in other words, users will be given the minimal set of access rights. It is also suggested that privileges are granted in sessions, where users and employees are given temporary permissions to perform a task.

Roles and Permissions:

- *Information Security Engineer-*
    - Permission to design, modify, and implement security strategies relating to data and networks
    - Permission to monitor traffic flows, strategize, and respond to intrusions
    - Permission to test hardware and software
    - Permission to review analyst's work, with obligation to report suspicion of unethical, unauthorized work.
    - Permission to temporarily inherit employee/user privilege's upon request.
- *Information Security Analyst-*
    - Permission to monitor network and systems to prevent, detect, and investigate breaches
    - Permission to modify and monitor software protection data resources
    - Permission to assist employees with technology processes and products
    - Permission to review engineers work, with obligation to report suspicion of unethical, unauthorized work.
    - Permission to temporarily inherit employee/user privilege's upon request.
- *CEO-*
    - Permission to oversee entirety of the startup
    - Permission to terminate an individual's access to *any* role
- *Employee-*
    - **Prerequisite:** must have been provided with a computer and a cellphone by the startup company.

    - Permission to assign users different roles. i.e. Super User
    - Permission to revoke access from users upon failure to pay the subscription fee.
    - Permission to utilize work computer/cellphone for work related activities *only.*
- *Super User-*
    - **Prerequisite:** task assigner/task doer will send request to other user(s). Eligibility for this role must first be approved from the other user(s) involved. From then, an employee will assign the appropriate user this role, which is specified in the request.
    - Permission to assign tasks to other users, including creating a title, a description, a deadline, and an estimate of how much time it is expected to take for that user.
        - *Constraint:* this role is to be assigned in sessions. Duration of a session will be specified within the request from user, i.e. Super User for one task, several tasks, one week, month, etc.
    - Inherits the permissions of a general user.
- *General User-*
    - **Prerequisite:** users can only be assigned this role upon successful registration on the application.
    - Permission to define TODO items and track time spent completing them.
    - Permission to add a title, a description, a deadline, and an estimate of how much time it is expected to take
        - *Constraint:* this role only has permission to assign tasks to themselves, not other users



Section 5: Threat Model

Threat modeling is technique used to enhance security across the network. This includes identifying and analyzing vulnerabilities, assets, and developing countermeasures to mitigate potential cyberattacks.

Popular methods for threat modeling include following the acronyms, STRIDE or DREAD, developing an attack tree, or utilizing the Common Vulnerability Scoring System (CVSS).

Developing a threat model and with recommending what controls must be implemented to secure this application.

Costs:

$20,000-Patch management platform
$10,000-Vulnerability scanning service
$10,000-Virtual Private Network
$25,000-Firewall (each)
Total: $65,000

Threat Model:

STRIDE:

Spoofing an identity of another user-

- Implement *multifactor authentication*

Tampering with data-

- Role based access control
- Session keys; automatically logged out after a period of inactivity

Repudiation-

-Maintaining access and audit logs, recording whose accessed the system, whose modified data, whose accessed the office.

Information disclosure-

- Modularity of information and resources

- Firewalls, VPN, vulnerability scanning service, patch management system

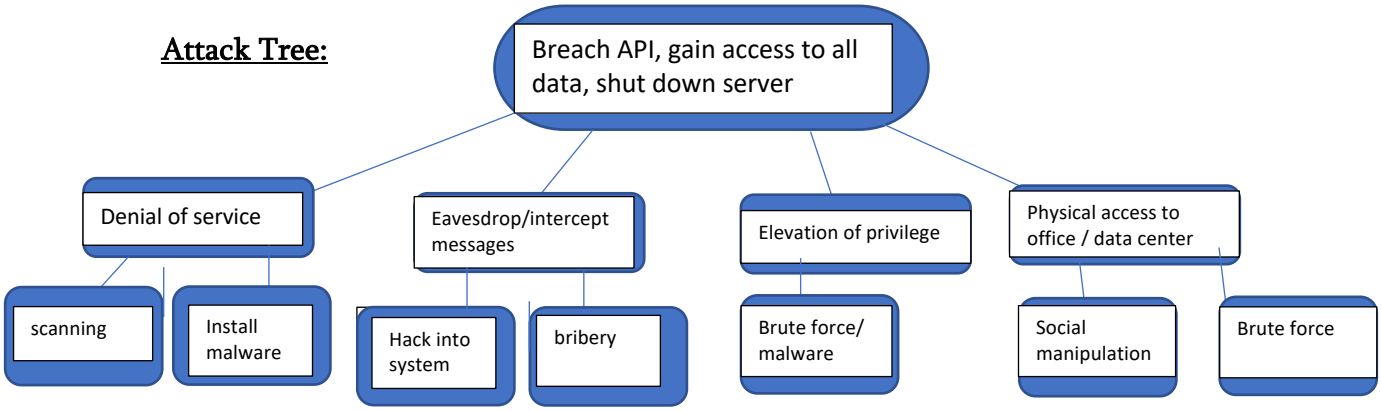
Denial of Service-

- Modularity/isolation of resources
- Separation of duty

Elevation of privilege-

- Role based access control
- Follow a system of least privilege

Attack Tree:



Section 6: List of Recommended Controls

Total cost: $315,000

-Multifactor Authentication:

Will aid in mitigating the potential for a user to spoof an identity by requiring two credentials. Multifactor authentication would be present as soon as the user/employee accesses the web or mobile application.

*Information Security Engineer:

Crucial for maintaining a secure system due to their vast knowledge and skill. Responsible for overseeing software and hardware and working to maintain data integrity. Obligation to make trips to the physical office and data center to monitor hardware.

*Information Security Analyst:

Shares many of the responsibilities of the security engineer in addition to helping employees and users. It is *highly recommended* that the startup hires *both* an analyst and engineer. Having two highly knowledgeable and skilled workers with isolation/separation of duty, will aid in mitigating the potential for an internal security breach to occur. In theory, if one suspects the other is performing unauthorized or suspicious activity, there is an obligation to report it. Less skilled/knowledgeable individuals may not be able to detect suspicious activity, as they wouldn't know what to look for.

-Patch Management Platform:

Highly valuable. Patch management works to apply necessary updates and bug fixes to operating systems, applications, software, and hardware. These updates and bug fixes are crucial for preventing an attack that could be performed if the weaknesses are not patched.

-Vulnerability Scanning Service:

A software tool that examines networks to find weaknesses such as weak network settings, out of date software, denial of service vulnerabilities and so forth, seeking out internal and external weaknesses in the network. This is a valuable tool to use, as some hackers may utilize the same tool to exploit weaknesses on networks; thus, it would be beneficial to invest in this service.

-Virtual Private Network:

Effective software that will protect valuable data and information by masking your devices IP address and identity, in addition to encrypting data securely, even when using public Wi-Fi, which would be highly valuable for this startup, where most employees are working out of office, and having users access the application from their smart phones or computers. A VPN will also protect financial transactions by keeping them anonymous and encrypted. This is valuable considering the startup will be requiring a subscription for the application.

-Firewall:

Software located between a network and the internet. Assess incoming data traffic to determine if there is any malware or threatening activity. The firewall will detect and block harmful activity from accessing the network. Additionally, a firewall can log the types of data traffic flowing and monitor the activity of employees.

The remaining $10,000 can be used on TLS encryption on servers. TLS encrypts data sent over the internet. This will prevent eavesdroppers and hackers from intercepting sensitive data, including credit card information, login information, emails and other sensitive information.

Section 7: Final Architecture