ENPM686 Information Assurance

Secure IT Environment

Vinaykumar Yennam

Umi Hani Bacha

Dheepshika Raghunathan

Table of Contents

1. Problem Statement

Several computers in our company have recently been compromised. It was discovered that the company network had been under attack for several months. However, these attacks had not been previously detected. The attackers exploited both network and host vulnerabilities.

A rough estimate of the maximum cost of this task is: $500K for equipment and software and at least 1 full-time security administrator (first year salary only included in initial estimate).

The company has a network of Linux computers for scientific research and a network of Windows computers for administrative tasks.

Additionally, the company relies on its web server to advertise and sell some of its products, as well as providing a customer support portal.

2. Objective

The objective of this report is to report all the inadequacies in the security of the IT environment of the company and to redesign it while incorporating various security aspects. The IT environment should satisfy all the business requirements of the company. It should also implement various security measures to protect it from attacks. A security solution should be provided that ensures the best possible security for the organisation within the given budget.

3. Scope

In order to focus on the security aspects of the design, the scope will be limited to the below,

- The current state of the IT environment will be analysed and the possible issues that might occur in this infrastructure will be outlined
- The IT environment will be redesigned from the purpose of making it secure

- Make provisions to detect and possibly prevent any intrusion in the IT environment
- Secure connection and communication methods will be established between various computing devices
- The cost and resources required for the redesigning will be considered

Since the objective is to make the IT environment secure, any operations related costs that the company might incur will be out of the scope of this document. This might include the personnel and equipment cost for running the scientific research and the administrative departments. This might also include the expensed related to employing the customer support personnel.

4. Assets and their Significance

The company possesses many assets which are to be protected against external threats. These assets include

4.1. Scientific Research devices

The company contains a scientific research team that uses a network of Linux systems to conduct research and to store and share all relevant information. This is essential to preserve the working and the information stored in these computers because this is where new products are being researched. The company would then draw revenue using the results found in this research lab. If this data is stolen by an attacker, the research information might be leaked. This might result in the company incurring losses not only in the amount spent on research but also the market advantage they might have gained if the information was not leaked.

4.2. Administration Network

The Administrative team works on a network of Windows computers which are used by the company management to run the company business. The information on these computers would be business critical information such as costs, business plans, revenue information, etc. The leakage of

this information may disrupt the functioning of the company. This may lead to losses in the market share, product costs, procurement, etc. Even if the systems are down due to an attack, the company might incur losses in critical businesses.

4.3. Web Server

The company hosts a website which details the products, allows users to perform online transactions and provides a customer support portal. The web server must be protected to make sure that an attacker doesn't gain access to the internal network or to the customer information. The leakage of customer information may affect the confidentiality of the information that the customer shares with them.

4.4. Products sold by the company

Although not entirely within the scope of a secure IT environment, there must be some mechanisms to protect the products themselves. This is because the products are the major revenue generator for the company. The protections around the products may be mechanisms to protect product and customer information, production methodology and cost information, security cameras and monitoring for the products.

4.5. Company Database

The company database is where all of the company's data is stored. It is essential to protect this because the leakage of this would mean that all the information related to the company is revealed to outsiders. This would include critical data such as payroll information, customer information, product information, research information etc.

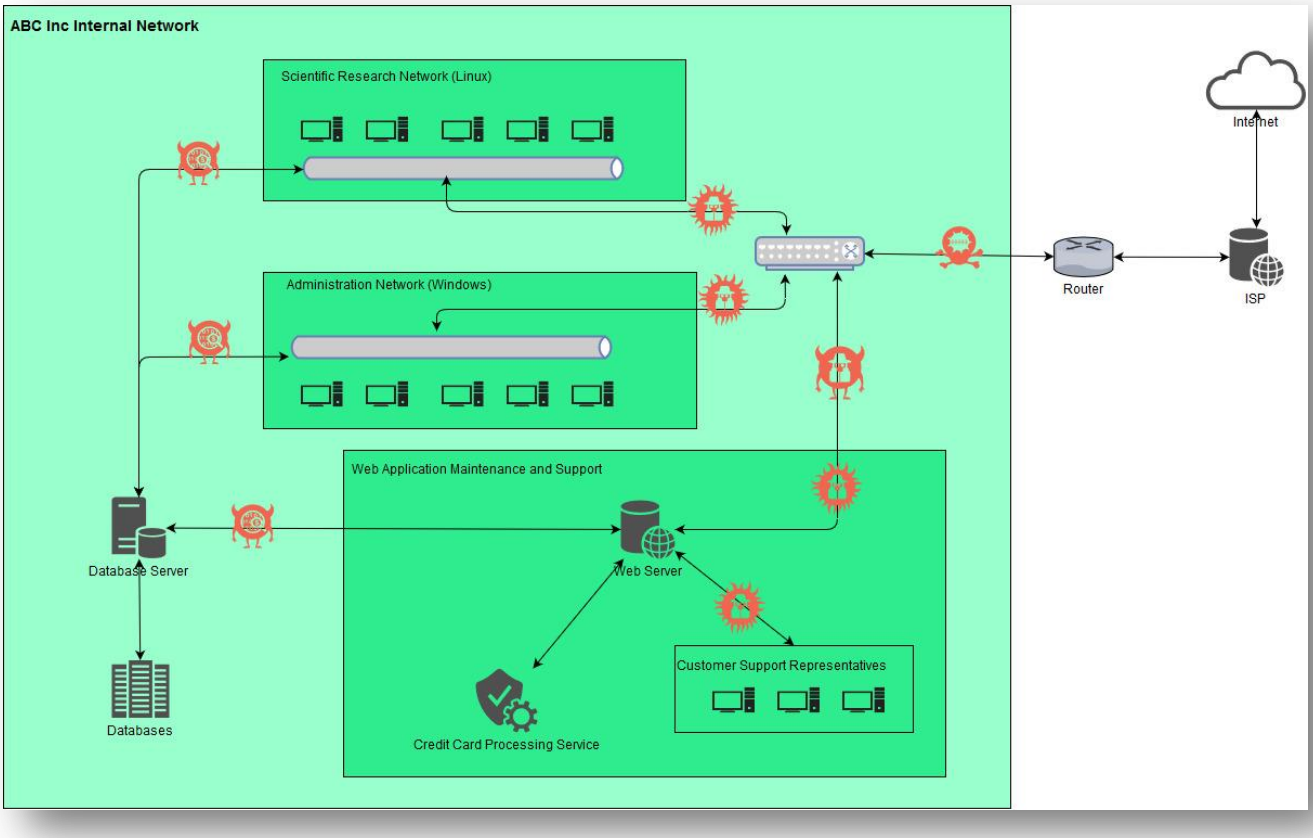
4.6. Source Code

The source code for the company website and the internal website is hosted from within the company. Any external alteration to this code could result in information leakage or malicious code

running in the company intranet. This could even reveal critical information such as user credentials and accesses in the system.

5. Current Infrastructure

The current IT infrastructure of the company is a basic one that consists of the required systems connected to the company intranet. This includes the web server, which is also connected to the ISP through which it is hosted in the internet. Currently, it does not employ any security measures such as Firewalls, IDS, IPS, etc.



In the current infrastructure, the Scientific Research Network, the Administrative network and the Web Application Maintenance and Support Network are all connected by a router that connects it to the ISP. These networks are also connected to the company database server that connects all the internal networks to the company database.

The systems within the various internal networks are connected on a common bus. The customer support representatives are also present within the intranet and hence have access to it.

6. Flaws in the Current Infrastructure

The current infrastructure of the IT environment of the company contains many flaws in design that might allow external entities access to the internal network. The flaws in the current infrastructure include,

6.1. No firewall configuration

In an organisational IT environment, a firewall is essential to block unnecessary traffic from entering the internal network. Lack of a firewall indicates that there is no filtering of the traffic that is entering the company's network. This could leave the network prone to malicious traffic entering the intranet.

6.2. No administrator to limit connectivity between resources

To ensure the security of an IT environment, it is essential that the traffic flow between various components in the intranet is strictly limited. That is any traffic must be allowed to flow in the intranet only when needed. This means that the connection between hosts and components and the access rights provided to various users must adhere to the company security policy and must be provided on a case by case basis. When there is no security administrator, there is no centralized control of the internal traffic of the company intranet.

6.3. No intrusion detection system

An intrusion detection system is essential to an organisation in order to detect any malicious traffic from entering into the intranet. When there is no intrusion detection system, there is no way to check the traffic that is entering the intranet.

6.3.1. No antivirus installed

An antivirus could be part of intrusion detection system that would detect any malicious code that is entering the company's network. When there is no antivirus present, viruses could easily infect the internal hosts. In case an antivirus is present, but it is not up to date, it would still be a risk as this would not protect the company's network from new viruses.

6.3.2. Improper logging of security events

All security events, irrespective of its severity, must be logged methodically and must be stored in such a way that it is readily accessible to the security team. This is essential, especially during a critical security incident. It might take the security admin or architects hours or even days to identify the cause of the security incident. Often, when logs are not properly maintained, the employees might have to spend hours even to identify the cause and solution to mitigate a recurring security issue. This would not only repeatedly affect the productivity of the employees, but would also leave the network prone to attack for hours.

6.4. No host protection mechanism

In many attacks to an organisation's network, the attacker would be interested in the contents of specific hosts, such as the CEO or the marketing head's system. If an attacker manages to gain access into the company intranet, he might gain access to the required host as well. When the data in the host is in plaintext, the data would be readily accessible to the attacker. A host protection mechanism, such as Bitlocker, could act as the last line of defence against attackers.

6.5. No layer separation

The separation of the internet and intranet layers is essential to identify and restrict traffic that is not required in the internal network. This would help prevent malicious users from gaining access to the internal resources of the company. This would also help the security admin in organising the accesses for the users to the company resources.

6.6. Weak Authentication

Good authentication is essential to make sure that malicious users don't gain access to the system by brute forcing passwords. The lack of this makes the system prone to dictionary attacks.

6.6.1. Improper password policies

Password policies specify the security measures that have to be taken to ensure proper authentication and to make sure that the passwords are not cracked easily. When the company lacks password policy, the passwords might not be protected efficiently. This may leave them vulnerable to exploits.

6.7. No organisation wide security policies

Organisation wide security policies are required to keep track of all security events and incidents. It is also essential to implement security practices in the all aspects of the company's working. It is the security policies that act as guidelines to implement the security in the day to day functioning of the company. The organisation wide security policies may also mandate the formation of a security team, whose sole function is to focus on the implementation, education and auditing of security policies in the organisation and to monitor and protect the company from security threats.

6.8. Weak data protection

The data that is stored in the database and the filesystem could contain confidential information. When data protection is not implemented, it makes it easy for the attackers to access this

information. It is hence essential to encrypt the data at rest to ensure confidentiality even when the host is compromised.

6.9. No proper backup system

A backup system protects the company's data against situations where the data requires to be recovered after some loss. The loss need not be complete. It could be so that some error was made which resulted in the loss of some data. A backup system is required to protect against such situations. It also has a security aspect where the error may open up vulnerabilities in the environment which might allow attackers to exploit it. So in such times, it might become essential to revert back to the previous protected state to stop attacks, before the errors could be fixed.

In some cases, such as a logic bomb attack, the loss might be complete as well. The backup system should be secure such that all the data could be recovered.

6.9.1. Disaster recovery

This is a special case where many hosts and parts of the data base were affected by a malware. Now once the security team gets rid of the malware, the data that was lost is to be recovered. When there is no backup system, this data could not be recovered and would constitute for the total loss of that data.

6.10. No secure communication between hosts

Even within the company intranet, malicious users may try to tap onto the flowing traffic and intercept it. The attacker may then try to retrieve interesting information from the traffic. During a man-in-the-middle attack like this, when the traffic is not secure and is in plain text, the confidentiality of the data that is being communicated is compromised. The integrity may also be compromised when the attacker tried to manipulate the packets and send modified data.

When the data in transit is encrypted, it becomes very difficult for the attacker to retrieve or manipulate the packets flowing in the intranet.

6.11. Issues with web application

The web application vulnerabilities might not just be exploitable but might also act as a way to enter into the internal company network.

6.11.1. Outdated software

Sometimes outdated software might be used in developing the web application. The software might have updated versions that might include security aspects. When the software is not updated, it might still contain the vulnerabilities in the legacy versions.

6.11.2. Improper protection against common web application vulnerabilities

Common web application vulnerabilities contain many exploits which are available in the public forum. Even a rookie attacker may be able to attack the company network if the code does not include mechanisms to protect against such attacks.

7. Possible Threats

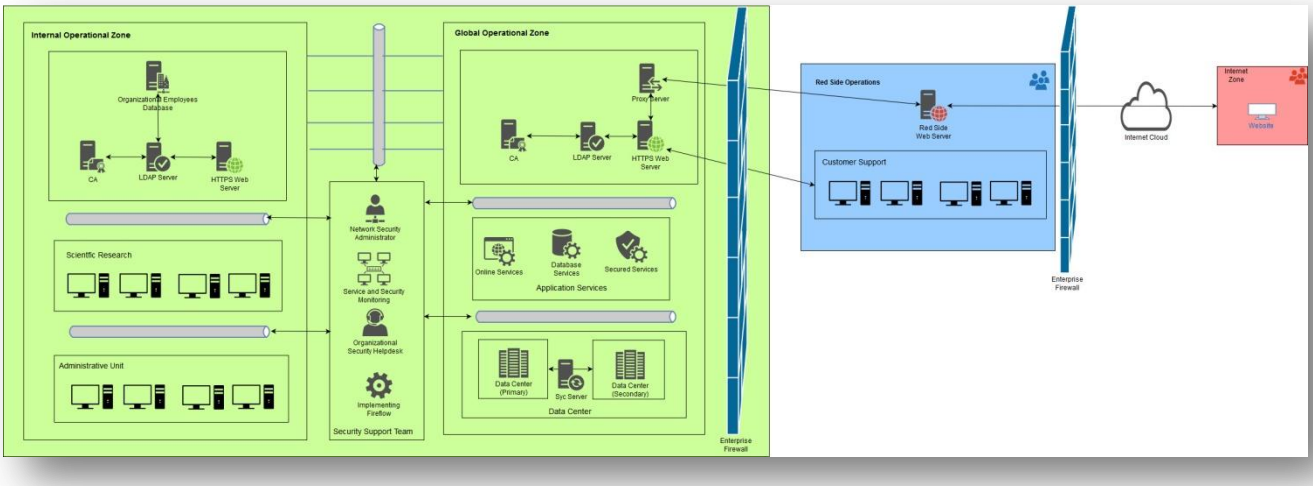
The above represent the threats that might occur in the current company intranet due to external attacks. These attacks might include,

1. ARP Poisoning at switch
2. SQL Injection (database)
3. Sniffing on wired media
4. Cross Site Scripting
5. Cross Site Request Forgery

6. POS malware
7. DDOS
8. Switch misassociation attacks
9. Man in the Middle attack
10. Routing table poisoning

8. Proposed Design

The IT environment could be redesigned to include various security aspects. This redesigned environment would satisfy all the requirements of the organisation and would include all required security aspects.



The IT environment could be segmented into zones

1. Internal zone or the green side
2. Enterprise zone or the red side operations zone
3. Internet zone or the red side

Two enterprise firewalls could be implemented to protect the environment from external threats.

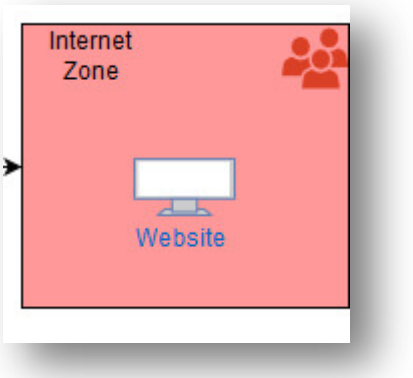
The Enterprise zone may contain both the red side web server and the network of hosts used by the customer support agents.

The internal zone could be further segmented into

1. Global Operational Zone
2. Internal Operational Zone
3. Security Support Team

9. Internet Zone

This zone represents the client side of the operations. This is where the customers would access the company website and could make online purchases.



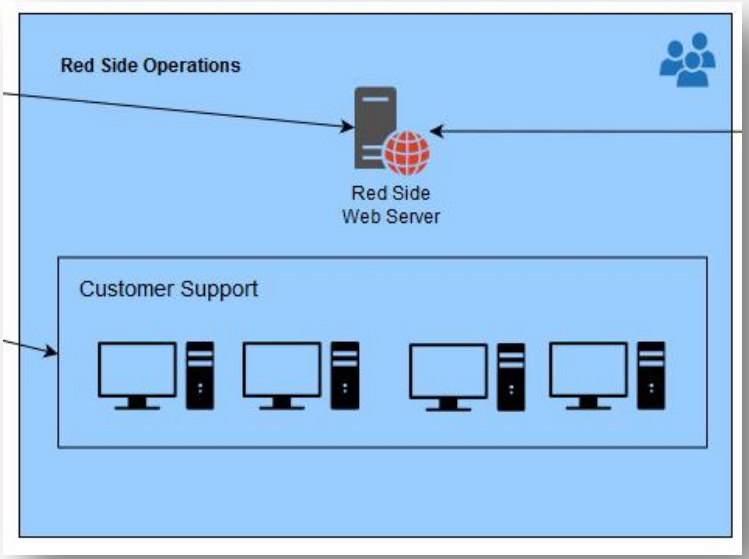
To ensure security, the website would require,

- User registration
- User Authentication
- Input Cleansing
- Access Control and Authentication

The applications in this zone will communicate Red Side Web Server in the Enterprise Zone.

10. Red Side Operations Zone

The red side operations zone contains components that are related to business communication with the customers who are on the external network.



The components in the zone would include

1. Red Side Web Server
2. Customer Support

10.1. Red Side Web Server

This is a dummy web server for the company's web application. This server will simply accept web requests from the client side applications and will relay them to the proxy server in the green side network.

This server sits in between the green side and the red site in order to hide the internal company network from client side applications and to reduce the risk of attacks from the client side.

The client side application communicates only with this server and will assume that this is the main server.

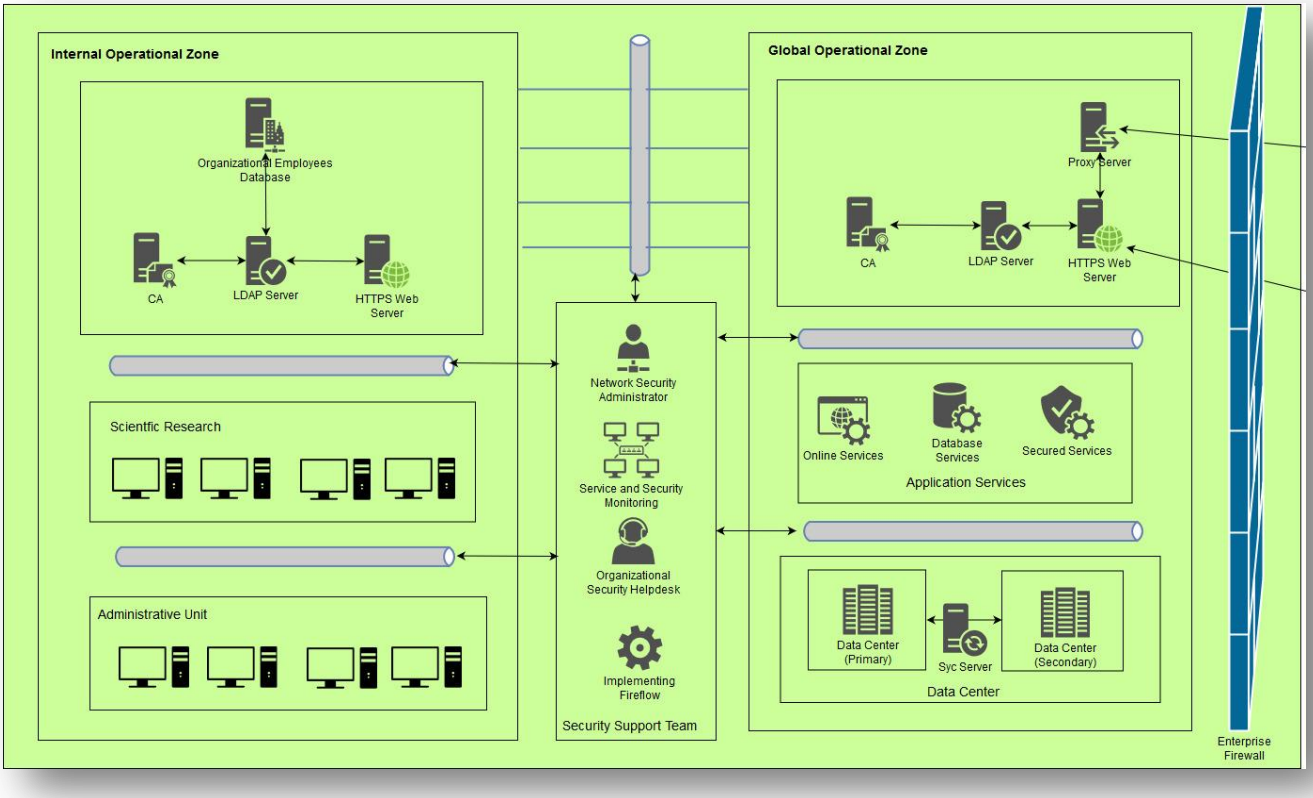
10.2. Customer Support

The customer support network provides online support for customers that access the support portal in the company website. The customers connect to the customer support representatives through a page in the website that starts a secure chat between a customer and a representative.

The representatives sit in the enterprise zone where they can access the chat through a custom portal. The customer support hosts do not have access to any other services or websites. These hosts are directly connected to the green side web server through a wired connection.

11. Company Green Side

The company green side consists of the company intranet. This consists of the major components in the company's internal network.



This zone provides the major functionalities of the business such as

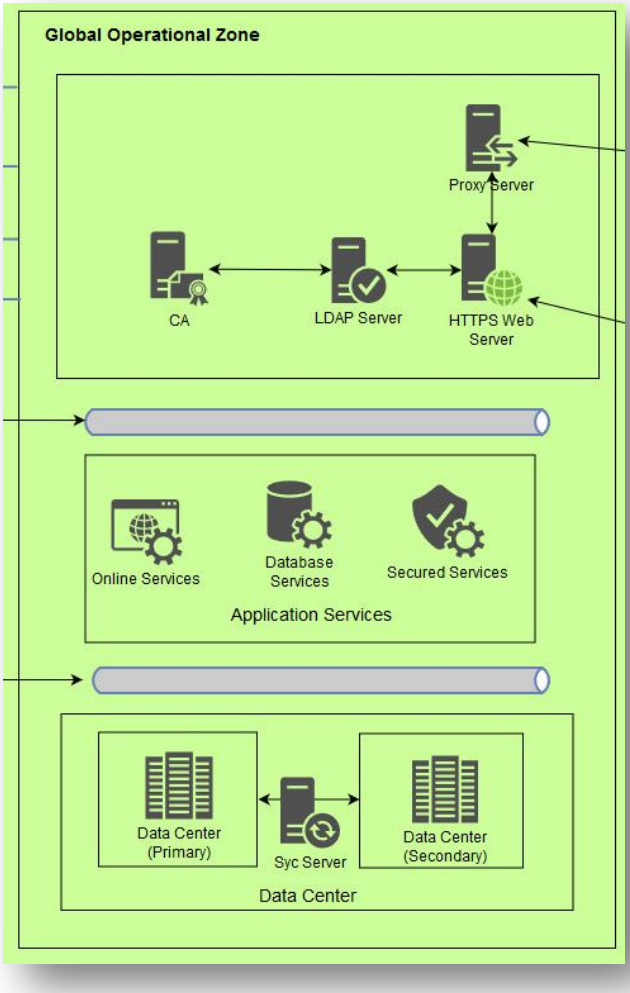
- Application server to host the website
- Online ordering capability
- Customer Support
- Database access
- Backup

- Service and Security Monitoring
- Scientific Research Network
- Administrative Network

All the internal components are layered as in the diagram. The connection traverses between the components in each layer via wired connections. The layers are connected by a wired bus mechanism and can communicate directly only with devices on the same layer, or with those devices for which they have access rights.

11.1. Global Operational Zone

The global operational zone is where the company's internal common components sit. These components are common to all the other zones in the company. The other zones can communicate with the resources in this zone via wired bus connections when they are given access to it.

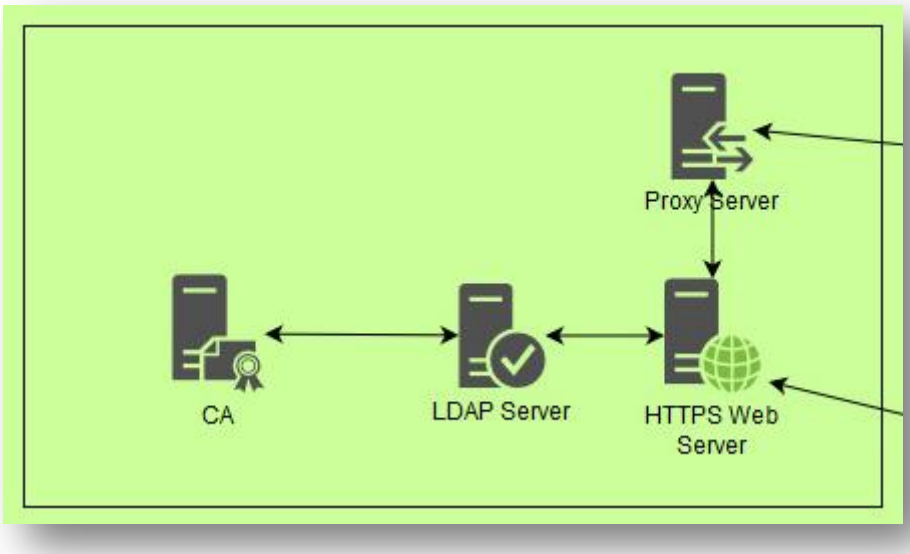


This zone mainly consists of the below layers

1. Web Application Maintenance and Support
2. Application Services
3. Data Centre

11.1.1. Web Application Maintenance and Support

This zone consists of the components required to maintain and support the company website.



11.1.1.1. Proxy Server

The proxy server is an intermediary server that accepts requests from the outside layers and transfers them to the internal web server. It also gets the responses from the internal web server and sends them to the red side web server.

The proxy server in the green side acts as a single point of entry to the green side network. It transfers only the web requests and does not perform any business critical activities.

Essentially, the proxy server hides the internal green side network from the outside world while acting as a doorway to it.

11.1.1.2. HTTPS Web Server

This is the main web server for the company's IT environment. This server services all the internal requests for the company's internal network. It also processes the requests coming from the external networks through the proxy server or through the customer support portal.

The web server performs authentication for all incoming connections using the adjacent LDAP server. Once authenticated, it forwards the requests to the application server. The web server could also host internal applications for monitoring such as Splunk to perform internal log and security monitoring. It could also host other internal business oriented applications that could be accessed only by the administrative users. The web server could also host an alert mechanism to alert the management users of any security incidents.

11.1.1.3. LDAP Server

The LDAP server performs the core authentication and authorization services for the company intranet. This server stores all the relevant user credentials. When an authentication request comes from the web server, the LDAP server authenticates the user and also verifies the accesses available to this user. The LDAP server uses the CA server to verify the certificates in the requests.

11.1.1.4. CA Server

The CA Server acts as a certifying agent for the organisation's applications. This server holds the relevant public and private keys. It checks the certificates for incoming connections and validates them. It also issues certificates when required and ensures end to end encryption.

11.1.2. Application Services

The application services layer consists of the core business services that are essential to host the company websites. It contains various components that perform various business critical operations. It includes,

1. Online Services
2. Database Services

3. Secured Services

11.1.2.1. Online Services

This is the core web service that communicates with the online clients to perform the required business operations. This also connects to the database server to send queries and receive responses from the database. This server also performs session management and session authentication for the company's websites. It could implement authentication tokens to authenticate the session. It may also perform access control in sharing application content in the company's website. This would ensure that a malicious user cannot gain unauthorised access to the application.

11.1.2.2. Database Services

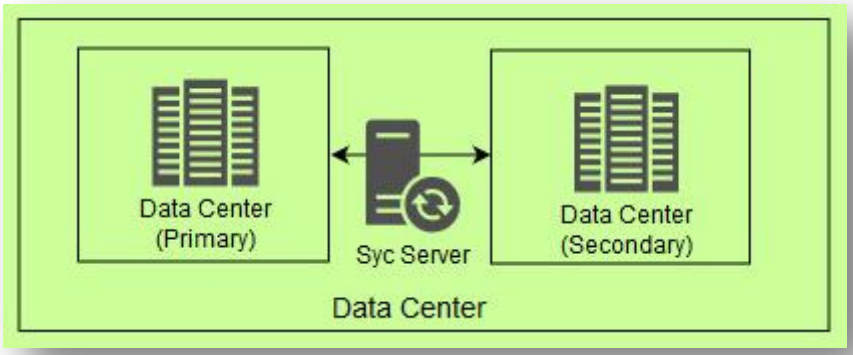
This service provides connectivity to the database. It implements data protection using a network traffic encryption mechanism such as SQL *net. This ensures that the requests sent and received from the database are encrypted. It also performs parameter binding to form the database queries to avoid SQL injection attacks.

11.1.2.3. Secured Services

This service implements third party secure credit card processing services. It connects the company's website to the third party credit card processing services and performs the relevant billing and transaction operations for the company application. This service ensures that the connection between the company application and the third party credit card service is reliable and ensures encrypted communications.

11.1.3. Enterprise Data Centre

The company data centre is where all the company data is stored. This is accessed by all the layers in the enterprise zones.



11.1.3.1. Sync Server

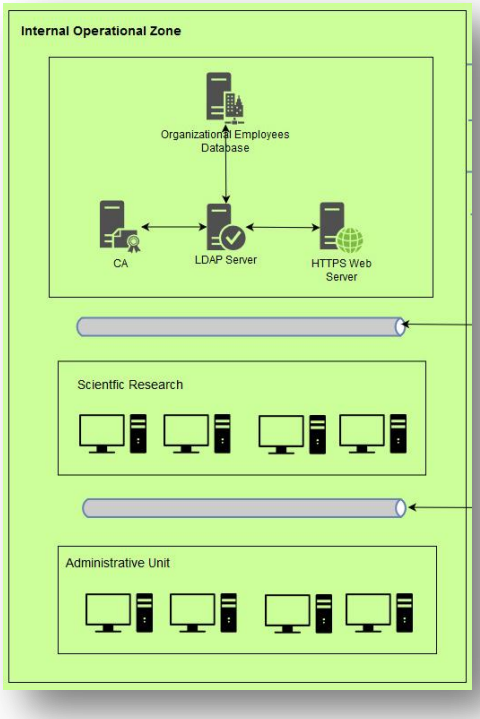
The sync server provides backup facility to the company network. The main function of the sync server is to act as a bridge between the primary and secondary data centres. The sync server ensures that the data in the secondary databases match that in the primary at all times. In case of failure, the sync server will up the secondary server while alerting the monitoring service regarding the failure.

11.1.3.2. Data Centres (Primary and Secondary)

The data centre is where the all the company's data is stored. All the above layers implement their queries on the primary data centre. The secondary data centre stores the same data as the primary data centre. Whenever the data in the primary data centre is updated, the sync server promptly copies the same in the secondary data centre. This way the secondary data centre is always an exact replica of the primary data centre. In case of failure in the primary data centre, the secondary is elevated to temporarily act as the primary data centre. This provides business continuity in the case of an attack on the primary data centre.

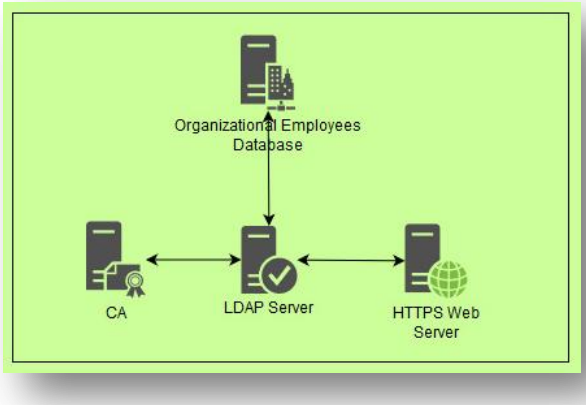
11.2. Internal Operational Zone

The internal operational zone consists of the confidential internal components of the company intranet. These components can connect to the global operations zone, but the components in the global operations zone cannot access components in this layer. This layer hosts the company's internal website, the scientific research network and the administrative network.



11.2.1. Internal Web Application Maintenance and Support

This layer contains similar components as the public website maintenance and support layer. The extra component this layer has is the Organisation Employees Database.



11.2.1.1. Organisational Employees Database

This database stores the authentication and authorization information for the internal users. This could include the employee usernames, password hashes, access control lists, etc. This information would be used in authenticating the users of the company's internal website.

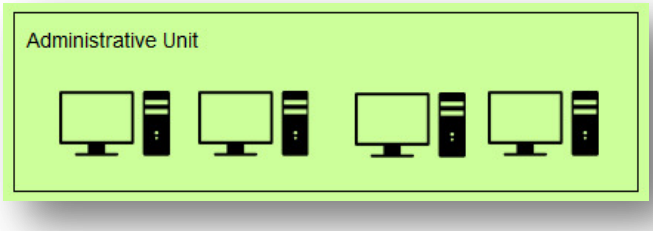
11.2.2. Scientific Research Network

This is a network of Linux computers that is used for scientific research.

These computers are used for scientific research in the company. These computers are connected by a wired connection are connect to other components through buses when access is granted to them.

11.2.3. Administrative Unit

This is a network of administrative computers that are used for the business critical and management tasks in the company.



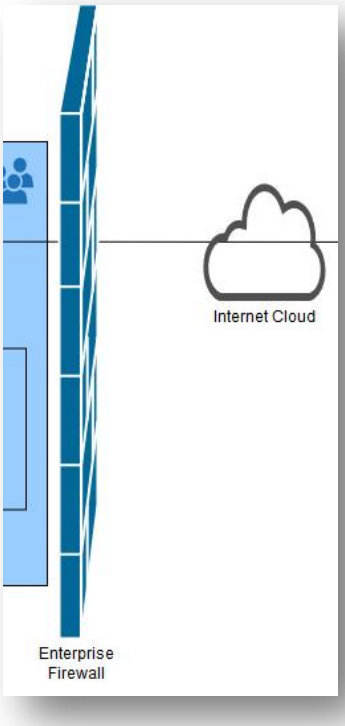
This is a network of windows computers that are connected through a wired connection in the company office. They are connected to other layers through wired buses and to components to which they have been given access.

12. Network Level Protection

Firewalls and IDS/IPS are used at the network level to provide security to the company's IT environment. Setting up all the network devices without logging defeats the purpose of deploying network protection devices. Hence, logging the activities and constantly monitoring will help achieve the goal of network devices

12.1. Red Side Firewall

The red side firewall makes sure that only the required traffic enters the company's red side. This firewall would essentially block any unwanted external traffic. This firewall establishes a barrier of trust between the external network and the intranet.



A traffic monitor could also be placed in this firewall to protect against denial of service attacks. Firewalls can also be used to rate limit the connections. This will help in mitigating Denial of Service.

Intrusion Detection system is used to detect any exploit code from external threat actors.

Intrusion Prevention system is a network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits.

12.2. Green Side Firewall

The enterprise firewall sits between the Internal Network Zone and the Enterprise Zone of the company's IT environment. This firewall performs 2 major operations,

1. Allows only HTTPS requests and responses to pass through on port 443.
2. Allows the above requests only between
    a. Red Side Web Server and Proxy Server
    b. Customer support hosts and HTTPS Web Server

This firewall will block all other traffic from passing through. This will reduce the risk of the company network being attacked at other ports.

The firewall can be configured to block incoming connection going to individual hosts. It is always the host that initiates a connection to the external untrusted network and not vice-versa.

The Green Side firewall also consists of an IDS/IPS component that monitors the company intranet for attacks from the company intranet and the enterprise operations zone. This is placed here to protect the company's network from insider attacks such as, ARP spoofing, poisoning switch tables, etc.

13. Component level protection

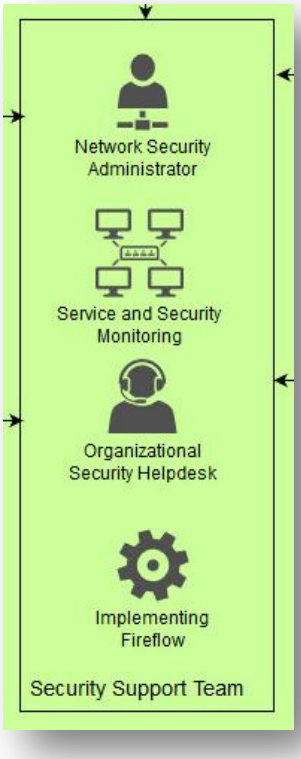
- Bitlocker is used to encrypt data at rest.
- To ensure data confidentiality full volume encryption is used and the cryptographic keys are stored in Trusted platform module (TPM).
- IP360 Toolset is used for periodic scanning of the network.
- For high availability, all the data of the nodes and the servers is backed up in the cloud.

14. Application level protection:

- Web application firewall is an application firewall for HTTP application. It has rules to cover common attacks such as cross-site scripting(XSS) and SQL injection.
- Secure communication protocols like SSH, SSL/TLS, HTTPS, SFTP is used. Sniffing/Eavesdropping will not help in gleaning information.
- All application development is done with secure coding practices and all user input is sanitized.

15. Global Security Support Team

The security support team performs the core of the security operations in the company's IT environment. This team will take care of the security policies, processes and monitoring of the company's network.



This team will include a Security Administrator and three security support employees.

15.1. Security Team Operations

The security team is involved in certain regular security operations such as security monitoring etc.

15.1.1. Service and Security Monitoring

This is the core management and log server. This server holds the logs for all activities occurring in the company's IT environment. This server connects to the Application Server and the Database server to monitor the operations and to detect unusual behaviour. This server may also monitor network traffic in the company network. The traffic coming to the Service and Security Monitoring from the Application Server and the Database service could be one way, such that this server cannot send data to either of these servers.

This server may run the Splunk Forwarder to pump log data to the Splunk instance running in the company web server. This server may also run incidence response mechanisms to react when unusual behaviour is detected.

This server will also implement a data retention policy that will ensure that after a certain period of time, the log data is purged. This would avoid any unnecessary leakage of critical information.

15.1.2. Organisational Security Helpdesk

The Security team also runs an organisational security helpdesk where they provide support to all employees who might require support related to security incidents or practices. All the items discussed in the helpdesk will be recorded and could be accessed when required.

15.2. Security Administrator Tasks

The security administrator plays a pivotal role in the security of the company's IT environment. The admin is connected to all the components and operates between them. Some of the tasks of the Security Administrator include,

15.2.1. Implementing Fireflow (Intranet Connectivity)

Initially all the ports in all the components are closed. The security administrator alone is authorized to enable the ports to establish connection between various components in the internal network. Based on the business requirements, the security admin will only enable those ports required for specific type of communication between two components.

This ensures that no unnecessary ports are open in the intranet and hence can avoid attacks on these ports.

15.2.2. Authentication

The security administrator authenticates all the employees of the company. When an employee joins the organisation, a user profile is created for the employee. The security administrator is the one who creates this user profile and stores all the relevant user authentication information. The security administrator also holds the rights to block user profiles from the company intranet in case a malicious incident is recorded.

15.2.3. Authorization and Access Control

The security administrator provides user profiles authorization to access various company resources. The authorization is given based on the requirements and the security administrator alone has the right to grant or revoke access. This avoids an attack where the user may elevate his privilege if the user can change authorization themselves.

The security admin alone creates and maintains the access control lists for the company's resources. The access control lists are periodically reviewed and updated.

15.3. Security Team Tasks

The security team deals with all the periodic security tasks that are to be performed in the organisation. Their purpose is to monitor the organisation intranet and all individual components for security violations or incidents. In case of a security incident, the security team acts as the first

responder and performs emergency tasks to protect the company network. Once the attack has been stopped and the issues are patched, the security team will work on recovery. Other tasks for the security team includes,

15.3.1. Creating Standard Security Policies

The security team is commissioned with creating standard security policies for the organisation. These security policies may include items for all levels, such as at the network level, component level, host level, employee level, secure coding practices, etc. The employee level policies could include avoiding tail gating, secure storage of sensitive information, document labelling, and document destruction policies. At the application level, the policies might include secure coding practices and data purge policies.

15.3.2. Support and Guidelines

The security team maintains the security policies and guidelines for the organisation. All the security policies are reviewed once a year and are updated when required. The security team creates security guidelines for the employees to follow. The guidelines are prepared based on the security policy. The security policies are updated to keep up with the market trends.

15.3.3. Auditing

The security team will perform annual or biannual security audits. The security audits may include penetration testing to make sure that there are no vulnerabilities in the system. The non compliances are recorded and corrections are enforced.

The security team may even recommend decommissioning components that have been unused for a specific duration. For example, if a component, such as a host, port, etc, has not been used for 6 months, the security team may recommend decommissioning it.

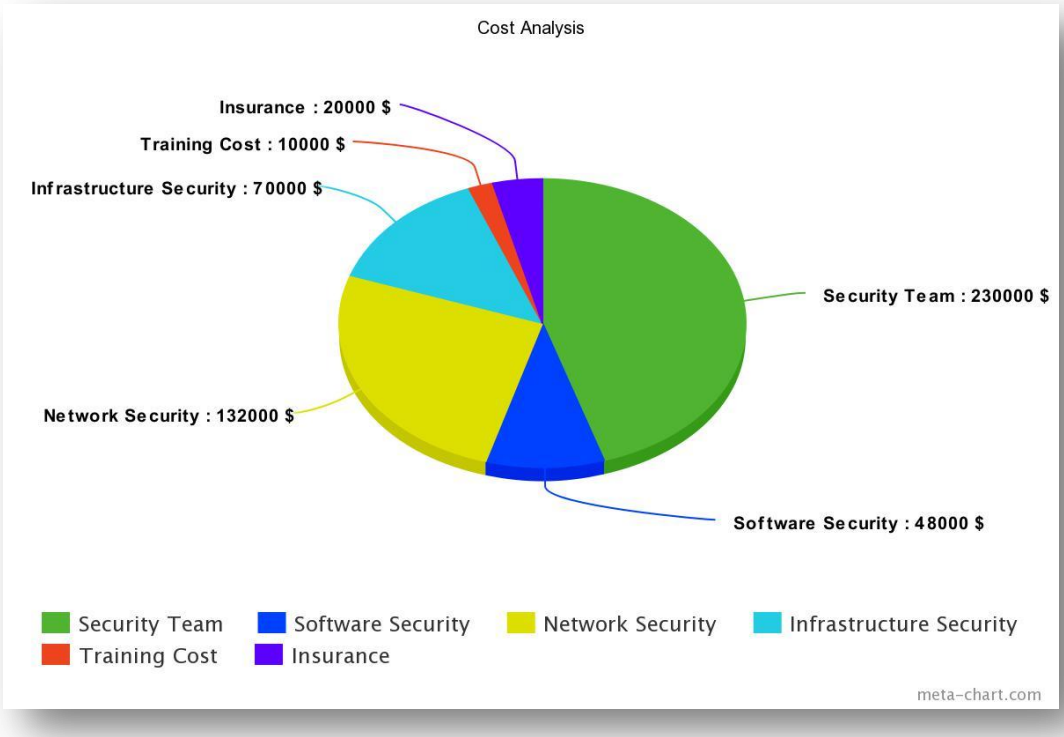
15.3.4. Monitoring Honeypots

The security team maintains and monitors honeypots for the company. Honeypots are replicas of the company's infrastructure but does not contain any business data. The security team leaves

these honeypots open to attacks and monitors the traffic flowing through it and the incidents that occur. This gives the security team insights into the vulnerabilities in the company's intranet. When such incidents occur, the security team logs the incidents and enforces fixes for these incidents.

16. Cost Analysis

The expenditure for the can be split as below,



COMPONENTS	ITEM	COST	QUANTITY	TOTAL COST
Security Team	Security Administrator	100,000	1	100,000
	Security Support Team	43,333	3	130,000
Software Security	ESET Enterprise Anti-Virus.	40	200	8,000
	Windows 10 + Bitlocker	200	200	40,000

Network Security	Intrusion Prevention System	20,000	1	20,000
	Intrusion Detection System	15,000	3	45,000
	Proxy Server	5,000	2	10,000
	Switches	500	4	2,000
	Routers	1,000	1	1,000
	Firewalls	2,000	2	4,000
	Backup per year per 1TB	100	500	50,000
Infrastructure Security	Security Cameras	300	100	30,000
	Database Migration and Sync servers	40,000	1	40,000
Training Cost				10,000
Insurance		20,000	1 per year	20,000

16.1. Trade Offs

- Although we could have used a Next Generation firewall, we chose to stick to a normal firewall because we have implemented both intrusion detection and prevention systems separately.
- The secondary database is also configured on cloud. Although having a dedicated backup server might have helped in higher availability, the costs of set up and maintenance would not justify the necessity of having a dedicated backup server and secondary databases
- Although 4k ultra resolution security cameras are available, it was beyond the budget.

17. Conclusion

The proposed design would reduce the attack surface, and thus reduces the chances of attack to the IT environment. It also ensures security at rest and in transit in the company intranet. The costs involved in setting up the environment was analysed and the best suited components were selected and listed. Trade offs were made in procuring components to keep the costs within budget.

Security is not a Product, it is a Process

Although an in depth analysis of all the security requirements for the IT environment was done and best components were selected, there might still be vulnerabilities in the infrastructure. As long as there are security measures to protect the environment, there will be attackers who will find novel ways to compromise it.