KN University Network Design

COIT13236 – Cyber Security Project

Document Title	Network Security Plan
Document Type	Technical Artefact
Document Status	Completed
Document Version	V_2.01
Group No	02
File name	group02-network-security-plan.docx
Created By	Narayan Parajuli (12144248)
Create Date	04/08/2024
Reviewed By	Krishan Himesh Abeyrathne (12217274)
Reviewed Date	14/08/2024

Table of Contents

Network Security Plan 3

Objectives 3

Diagram and Explanation 4

Key Components 5

1. Firewalls 5
2. Intrusion Detection and Prevention System (IDPS) 5
3. Virtual Private Network 5
4. Access Control 6
5. Security Information and Event Management (SIEM) 6
6. Patch Management 7
7. Policies and Procedures 7
8. Risk Management 8

Network Security Plan

Network Security Plan:

A Network Security Plan guarantees the university's network is safeguarded against dangers, keeps up with data integrity, and gives secure access to assets. The following is a consolidated arrangement that covers key components of network security.

Objectives

- **Confidentiality:** Ensuring the secrecy of sensitive data incorporates a comprehensive technique that integrates data characterization, access control frameworks, encryption, secure data storage, access methodologies, checking and inspecting, client preparing, and a vigorous incident reaction plan.
- **Integrity:** Ensuring data integrity incorporates executing measures that safeguard information from unapproved change and debasement, guaranteeing its precision and consistency all through its lifecycle. This consolidates cycles, advancements, and systems planned to detect and prevent information modifying, as well as components to really look at data precision.
- **Availability:** Guaranteeing the accessibility of network assets is critical for staying aware of nonstop access to information and services for students, Labor force, and staff. This incorporates completing measures to forestall downtime, promptly recover from interferences, and stay aware of ideal execution.
- **Compliance:** Consistence with genuine and regulatory requirements is principal for staying aware of the uprightness, privacy, and availability of organization assets while ensuring the school complies with material guidelines, rules, and standards.

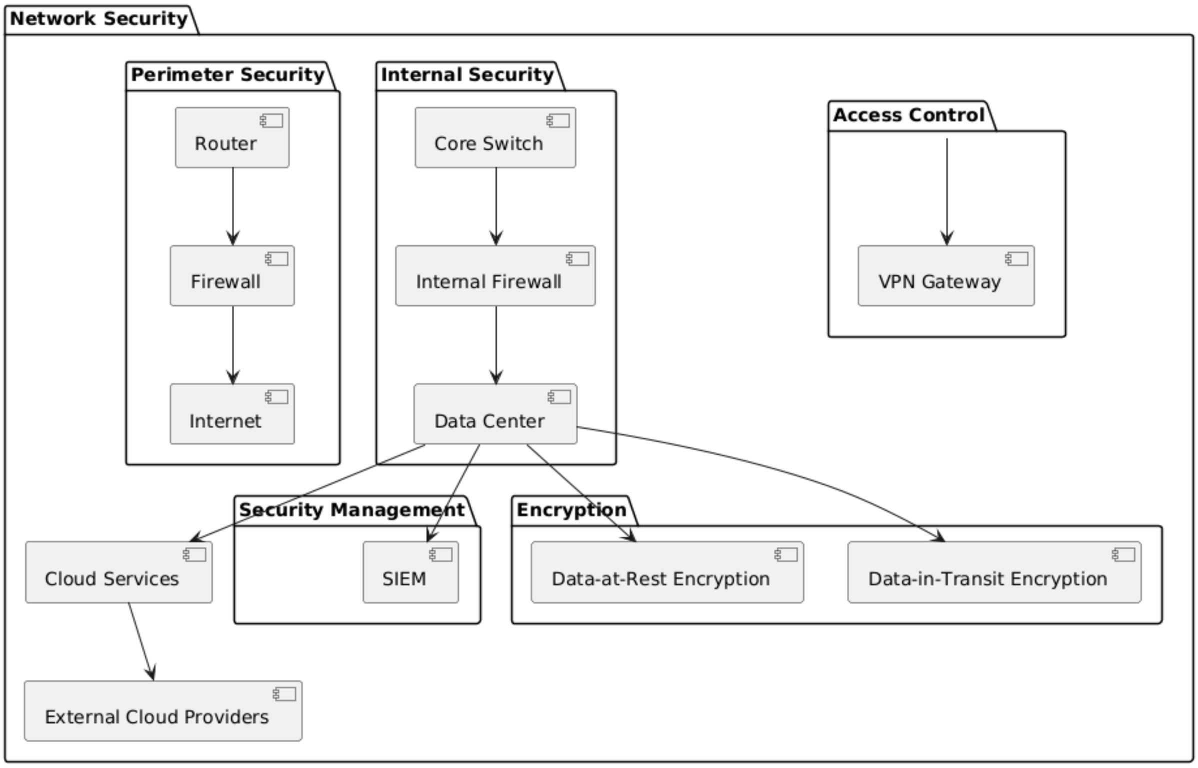

Fig: Network Security Plan

The KN University network security design is displayed in the above diagram. The network's first line of protection is perimeter security. The router that connects the college's network to the web is one of its parts. By filtering and managing all information entering and leaving the network, the firewall fills in as a security barrier. By restricting admittance to the network to simply protect and support traffic, this setup prepares for outside dangers coming from the Web. The network of the university is protected from inside by inward security. Inside the network, information flow is controlled and coordinated by the Core Switch. An interior firewall safeguards basic assets by watching out for and overseeing inward interchanges. This adds an additional layer of protection. The university stores and keeps up with its essential information in the Data Centre, which fills in as the hub of the network's data frameworks.

By utilizing a VPN Gateway, Access Control ensures that main approved clients can interface with the college network, even from distant areas. Using a SIEM framework to follow and inspect security action is known as security management. This recognizes and address potential dangers. To improve and keep up with its advanced administrations, the organization additionally utilizes cloud administrations, which lay out associations with outside cloud suppliers. The method involved with defending delicate data is called encryption. Data-at-Rest encryption safeguards protects information by ensuring that, regardless of whether somebody accesses it, they can't peruse it without the essential authorisation. Data-in-Transit Encryption shields information while it goes over the organization, forestalling block attempt or control while it is being sent starting with one area then onto the next.

The figure shows how the different components of network security are associated with one another and add to the general security of the KN University network.

Key Components:

1. Firewalls

Purpose: Their fundamental intention is to make an obstruction between a trusted interior network, and untrusted outside networks, like the web. In this way, firewalls help to protect against unapproved access, digital dangers, and information breaks. Model: Norton 360 Suite

- **Types:**
    - **Perimeter Firewalls:** Their basic role is to make a barrier between a trusted internal network, and untrusted external networks, like the web.
    - **Internal Firewalls:** Inner firewalls, generally called segmenting firewalls, are sent inside an internal network to make different security zones. Internal firewalls can isolate fundamental or fragile regions like finance, HR, or imaginative work from the rest of the network.

2. Intrusion Detection and Prevention Systems (IDPS)

Purpose: Intrusion Detection and Prevention Systems (IDPS) are planned to recognize and prevent malicious activities inside a network or structure. They have a huge impact in online protection by perceiving anticipated risks, cautioning administrators, and taking mechanized actions to mitigate risks.

- **Types:**
    - **Network-based IDPS:** Network-Based IDPS (NIDPS) are conveyed to monitor and take apart network traffic for signs of malevolent movement. They are regularly arranged at central issues inside a network, like gateways, switches, and routers, to give broad oversight of the information flowing through the network.
    - **Host-based IDPS:** Host Based IDPS (HIDPS) are presented straightforwardly on individual gadgets or hosts, like servers, workstations, or endpoints. They focus on observing and examining activities well defined for each host to distinguish and prevent dangers.

3. Virtual Private Network (VPN)

Purpose: A Virtual Private Network (VPN) is an innovation that gives secure distant induction to a network over the web. VPNs use strong encryption shows to shield data on the way, ensuring that any caught data is ambiguous without the encryption keys.

- **Types:**
    - **Site-to-Site VPN:** A Site-to-Site VPN is a strategy used to interface no less than at least two networks, regularly corporate or various levelled LANs, over the web securely. The primary job of a Site-to-Site VPN is to securely interface geologically dissipated campuses, allowing them to share resources and data securely over a public network like the web.

  - **Client-to-Site VPN:** A Client-to-Site VPN, generally called Remote Access VPN, licenses individual clients to connect with a confidential network from distant regions. The fundamental job of a client-to-Site VPN is to give distant clients secure and encoded admittance to an association inside network. This ensures that sensitive data and communications stay secured, regardless, when gotten to over conceivably temperamental public networks like home Wi-Fi or public hotspots.
- **Encryption:** Encryption is a security cycle that changes data into an encoded plan, making it indiscernible to unapproved clients. Solid encryption algorithms, for instance, AES-256, give major areas of strength for an against digital dangers, guaranteeing the secrecy and security of information sent over conceivably unreliable networks.

4. Access Control

- **Purpose:** Access control is a safety measure that manages who or what can view or involve assets in a computing environment. The fundamental role of access control is to limit access to fragile data and critical systems considering client roles and consents.
- **Mechanisms:**
  - **Role-Based Access Control (RBAC):** RBAC is a strategy for managing access to resources considering the jobs of individual clients inside an association. The principal job of RBAC is to rearrange and streamline the administration of client permissions by assigning jobs rather than individual authorizations to each client. This approach ensures that clients have fitting access in view of their work abilities and commitments.
  - **Multi-Factor Authentication (MFA):** MFA is a security mechanism that anticipates that clients should give something like at least two verification factors to gain access to a resource. The fundamental job of MFA is to decrease the risk of unapproved access by ensuring that whether one approval factor is compromised, other factors are expected to gain access.

5. Security Information and Event Management (SIEM)

Purpose: Security Information and Event Management (SIEM) is a far-reaching way to deal with cyber security that solidifies Security Information Management (SIM) and Security Event Management (SEM) to give ongoing examination, checking, and response to security occasions inside an association. The principal job of SIEM is to further develop a network security present by giving integrated detectable quality into network activities, recognizing potential security risks, and enabling speedy response to incidents.

- **Features:**
  - **Log Management:** Log management alludes to the process of gathering, storing, and dissecting log data made by various devices, applications, and structures inside a network. SIEM structures assemble log data from many sources, including network

devices (switches, routers), security machines (firewalls, IDS/IPS), servers, applications, and endpoint gadgets.

- **Event Correlation:** Event correlation is the technique associated with analysing and comparing log data from different sources to recognize patterns and distinguish potential security risks. SIEM systems use predefined rules, heuristics, and advanced assessment to correlate events and make critical security alerts.
- **Incident Response:** Incident Response alludes to the activities started by a university to recognize, inspect, and answer security events. SIEM frameworks have a basic impact in working with and mechanizing the incident reaction process.

6. Patch Management

Purpose: The purpose of patch management is to guarantee that product and frameworks are up to date with the latest patches and updates. This is urgent for keeping up with the security, stability, and performance of systems.

- **Process:**
  - **Inventory Management:** Inventory management includes maintaining a comprehensive list of all products, applications, and frameworks inside an organization.
  - **Patch Deployment:** Patch deployment is the process of applying patches to programming and frameworks to address weaknesses, fix bugs, or improve functionality.
  - **Testing:** Testing includes approving that patches and updates are applied accurately and don't present new issues or conflicts.

7. Policies and Procedures

At KN University, the Policies and Methods segment frames fundamental principles and rules that govern network security, data protection, and client conduct to guarantee a solid, consistent, and well-working IT infrastructure. Here is a breakdown of key components:

Network Security Policy: The Network Security Policy lays out rules for shielding the university's network from unapproved access, data breaches, and other security dangers. This guarantees that main approved people with explicit jobs and obligations approach the organization assets they need to play out their duties.

Access Control: Clients (students, staff, or any clients) are allowed admittance to just the network assets essential for their jobs. For example, staff individuals could approach student records, while students just access individual academic data.

Incident Response Plan:
This plan frames the steps the university will take to answer security incidents, for example, network breaks, data breach, or cyberattacks. The objective is to rapidly distinguish and relieve dangers while limiting harm and interruption to the university's activities.

Steps for incident response:
Detection: Identifying the presence of a potential security incident.
Investigation: Assessing the nature and effect of the incident.
Containment: Making quick moves to restrict the spread of the danger.
Eradication: Eliminating the reason for the incident (e.g., malware, unapproved access).
Recuperation: Reestablishing ordinary tasks and securing systems against future incidents.
Illustrations Learned: Post-incident audit to comprehend what turned out badly, report upgrades, and improve future response procedures.

Data Protection Policy:
This arrangement establishes the legitimate administration, characterization, and handling of data inside KN College, guaranteeing consistence with nearby and worldwide guidelines like GDPR. Information security measures are basic in forestalling unapproved admittance to delicate data, for example, student records, research information, or financial transactions.
Key Parts:
Data Arrangement: Characterizing classifications of data in view of awareness (e.g., public, interior, confidential).
Taking care of Methodology: Rules for storing, communicating, and sharing information safely, including encryption and access controls.

User Training:
KN University focuses on teaching clients about normal security dangers and best practices. Normal instructional meetings are led for the two students and staff, covering fundamental subjects to assist them with remaining educated and cautious.

Training Subjects:
Phishing Awareness: Recognizing and avoiding email and electronic phishing endeavors that look to take individual data.
Password Management: Best practices for creating strong passwords, utilizing password managers, and shielding login certifications.
Safe Web Use: Rules for safe perusing, perceiving malevolent sites, and keeping away from dangerous internet-based conduct.

These approaches and strategies intend to defend KN University's IT frameworks, safeguard information, and engage clients to act dependably inside the network. They contribute to a safe environment helpful for scholarly and administrative functions.

8. Risk Management

Purpose: Risk assessment is a fundamental part of risk management. Its principal job is to identify, evaluate, and focus on dangers to an affiliation's assets, assignments, and objectives. By understanding these risks, affiliations can foster methodologies to mitigate or manage them effectively, ensuring the continuity and strength of their activities.

- **Risk Mitigation**
  Risk mitigation implies implementing methodologies and exercises to diminish the probability and impact of recognized risks. The goal is to restrict likely risks and shortcomings, subsequently shielding a network assets, errands, and objectives. Convey firewalls to control and screen network traffic, forestalling unapproved access and mitigating external risks. Sporadically survey and update security approaches and strategies to ensure they stay significant and fruitful in watching out for current risks. Provide training on broad security works on, including perceiving phishing endeavours, safe web use, and genuine treatment of sensitive information.

- **Risk Analysis**
  Risk analysis at KN University implies distinguishing, surveying, and mitigating expected dangers to its IT framework, data, and activities. Key dangers incorporate cybersecurity threats (e.g., data breaks), functional interruptions, information security concerns, and physical hazards. Risks are assessed in view of probability and effect, with high-priority dangers, for example, data breaches or system blackouts getting the most consideration. Mitigating procedures incorporate cybersecurity measures, regular data backups, disaster recuperation plans, and client training. Nonstop observing, reviews, and clear communication guarantee that the risk management interaction adjusts to new difficulties, helping shield the university's systems and data.

- **Continuous Monitoring:** Constant checking incorporates the consistent impression of a college's IT environment to recognize and answer security risks and execution issues dynamically. Network observing gadgets track the exhibition, availability, and security of network system. They give pieces of information into network traffic, device status, and potential issues that could influence network performance or security.

References

International Organization for Standardization (ISO) (2024) ISO 31000:2018 Risk Management Guidelines. Available at: https://www.iso.org/iso-31000-risk-management.html (Accessed: 3 August 2024).

SANS Institute (2024) Network Security Policy. Available at: https://www.sans.org/security-resources/policies/network-security-policy (Accessed: 3 August 2024).

Cybersecurity & Infrastructure Security Agency (CISA) (2024) Multi-Factor Authentication. Available at: https://www.cisa.gov/multi-factor-authentication (Accessed: 3 August 2024).

Microsoft (2024) Encrypting Data Using AES-256. Available at: https://docs.microsoft.com/en-us/windows/win32/seccrypto/encrypting-data-using-aes (Accessed: 3 August 2024).