Company Name: SecureTech Solutions

Document Type: Network Diagram Description

Overview:

SecureTech Solutions' network architecture consists of multiple segments, including public, private, and DMZ zones, designed to ensure strong security boundaries between internal and external systems. The following document provides a detailed explanation of the core components involved in the company's network.

1. Firewall:

A perimeter firewall (Cisco ASA) is in place at the edge of the network, enforcing strict traffic control policies between public internet access and internal systems. An additional internal firewall separates the corporate LAN from the DMZ.

2. VPN:

Remote employees access corporate resources through an IPsec VPN tunnel. Multifactor Authentication (MFA) is mandatory for all remote logins.

3. Intrusion Detection System (IDS):

The network is protected by an IDS (Snort) that monitors inbound and outbound traffic for anomalies and potential threats.

4. Servers:

Critical servers, including email, file sharing, and application servers, are housed in a secured segment of the network, shielded behind the internal firewall. Server access is restricted to authorized personnel using role-based access control.

5. Data Encryption:

Data-at-rest is encrypted using AES-256, while data-in-transit is protected using TLS 1.3.

6. Backup Systems:

Regular backups are performed daily, and the backup servers are located in a separate physical location for disaster recovery purposes.

Conclusion:

All critical components are continuously monitored and undergo regular security audits. Policies are in place to address potential risks such as unauthorized access or data breaches.

Company Name: SecureTech Solutions

Document Type: Security Policy Document

Overview:

This document outlines the security policies implemented at SecureTech Solutions to safeguard its digital assets, data, and network infrastructure. These policies apply to all employees, contractors, and third-party vendors.

1. Access Control:

Access to sensitive systems and data is granted based on the principle of least privilege. Role-based access control (RBAC) ensures that employees can only access the systems necessary for their job functions.

2. Data Protection:

All sensitive data, including personal identifiable information (PII) and financial records, must be encrypted at all times, whether at rest or in transit. The company uses AES-256 encryption for data-at-rest and TLS 1.3 for data-in-transit.

3. Multifactor Authentication (MFA):

MFA is required for access to all critical systems. This includes the use of one-time passwords (OTP) in addition to standard login credentials.

4. Incident Response Plan:

In case of a cybersecurity incident, the Incident Response (IR) team will initiate containment measures, collect forensic data, and notify affected stakeholders. The IR team will ensure systems are restored to normal operations following incidents.

5. Security Audits:

Regular security audits and vulnerability assessments are conducted quarterly to identify and address security gaps. Third-party penetration testing is carried out annually.

6. Employee Training:

Employees undergo mandatory cybersecurity awareness training every six months. Topics include phishing, password security, social engineering, and best practices for protecting sensitive information.

7. Data Retention Policy:

Sensitive data is retained for a maximum of seven years. Secure deletion methods are employed for any data scheduled for removal.

Conclusion:

This policy is designed to ensure compliance with regulations such as GDPR and HIPAA, as well as to protect the integrity and confidentiality of company assets.

```
! Cisco ASA Firewall Configuration

hostname Firewall_SecureTech
enable password ********
!
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 192.168.1.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.0.0.1 255.255.255.0
!
access-list outside_in extended permit tcp any host 192.168.1.100 eq 443
access-list outside_in extended permit tcp any host 192.168.1.101 eq 80
!
object network INTERNAL_NET
```

```
 subnet 10.0.0.0 255.255.255.0
!
object network VPN_CLIENTS
 subnet 192.168.2.0 255.255.255.0
 nat (outside,inside) dynamic interface
!
nat (inside,outside) source static INTERNAL_NET INTERNAL_NET destination static VPN_CLIENTS VPN_CLIENTS no-proxy-arp route-lookup
!
crypto ipsec ikev1 transform-set ESP-AES-SHA esp-aes esp-sha-hmac
crypto map outside_map 10 match address outside_in
crypto map outside_map 10 set peer 203.0.113.1
crypto map outside_map 10 set transform-set ESP-AES-SHA
crypto map outside_map interface outside
!
service-policy global_policy global
logging enable
logging trap warnings
logging host inside 10.0.0.10
!
```

Company Name: SecureTech Solutions

Document Type: Incident Report

Incident Title: Unauthorized Access Attempt

Incident Date: October 10, 2024

Incident Description:

On October 10, 2024, at approximately 14:35 UTC, an unauthorized access attempt was detected on the company's internal network. The attempt originated from IP address 192.168.5.15, which was flagged as suspicious by the Intrusion Detection System (IDS).

Incident Response Actions:

1. The IT security team immediately isolated the affected server from the network.

2. An investigation revealed that the unauthorized access attempt was made through a brute force attack on the SSH port (Port 22).

3. The offending IP address was blocked at the firewall, and all SSH access was temporarily disabled for further investigation.

4. Logs and forensic evidence were collected for analysis.

5. The company's VPN access was restricted to known IP addresses, and all users were required to reset their credentials and enable multifactor authentication.

Lessons Learned:

1. SSH access should be restricted to specific IP ranges.

2. Implement stronger password policies and use key-based authentication.

3. Enhance logging and monitoring of SSH traffic to detect anomalies faster.

Next Steps:

- Conduct a full audit of all remote access systems.

- Implement additional layers of access control for critical infrastructure.

- Schedule a follow-up meeting to discuss long-term mitigation strategies.