Security Architecture for Tech Solutions Inc.

Osamudiamen Eweka

CYB-653-Z1 Securing and Defending Networks

Dr. Donnie Wendt

Utica University

Table of Contents

Executive Summary

Tech Solutions Inc., a mid-sized company providing online products and services, handles sensitive data, including personally identifiable information (PII). To enhance its security posture, the company is transitioning to a zero-trust model while supporting legacy on-premises applications with a defense-in-depth strategy. This comprehensive security architecture addresses the diverse needs of Tech Solutions Inc. by implementing tailored security measures for legacy on-premises applications, cloud-based applications, SaaS products, and on-premises email services.

Legacy on-premises applications will be protected using network segmentation, firewalls, and intrusion detection/prevention systems (IDPS), ensuring isolation and monitoring of critical applications. For cloud-based applications, the zero-trust approach involves robust identity and access management (IAM), multi-factor authentication (MFA), encryption, and micro-segmentation, with continuous monitoring for real-time threat detection.

SaaS applications for internal business functions will be accessed securely through virtual private networks (VPNs) or secure access service edge (SASE), with conditional access policies and endpoint security measures. On-premises email services will utilize advanced email filtering, encryption, and regular security awareness training for employees.

By implementing these measures, Tech Solutions Inc. can ensure robust protection of its sensitive data and secure access to its products and services, maintaining its reputation and trust among customers and stakeholders.

Introduction

Tech Solutions Inc. provides online products and services, involving the handling of personally identifiable information (PII) and other sensitive data. The company's infrastructure includes a mix of legacy on-premises applications and cloud-based applications, supported by a major cloud service provider. Additionally, the company leverages software-as-a-service (SaaS) products for internal business processes such as HR and finance. Employees work in a hybrid environment, requiring secure access both from home and the office. This document outlines the security architecture needed to address these diverse needs, with a focus on implementing a zero-trust architecture (ZTA) for cloud-based and SaaS applications, while maintaining a defense-in-depth strategy for legacy systems.

Legacy On-Premises Applications:

Overview

Legacy on-premises applications at Tech Solutions Inc. are critical for providing products and services to customers. These applications are hosted in the company's data center and require a traditional defense-in-depth strategy due to their inability to fully transition to a zero-trust architecture (ZTA).

Security Measures

1. **Network Segmentation:** Implement network segmentation to isolate different parts of the network and limit lateral movement. Critical applications should be placed in a demilitarized zone (DMZ) to protect them from external threats while allowing necessary external access (Dhiman et al., 2024). Network segmentation helps in containing potential breaches and reducing the attack surface by isolating sensitive data and applications.

2. **Firewalls and Intrusion Detection/Prevention Systems (IDPS):** Deploy firewalls and IDPS to monitor and block malicious traffic. This includes using both network-based and host-based intrusion detection systems (Rose et al., 2020). Firewalls act as the first line of defense by controlling incoming and outgoing network traffic based on predetermined security rules. IDPS helps in identifying and mitigating threats in real-time by analyzing network traffic for signs of malicious activity.
3. **Access Control:** Utilize role-based access control (RBAC) to ensure that only authorized personnel can access sensitive applications. Implement multi-factor authentication (MFA) for an additional layer of security (Rukhsara et al., 2016). RBAC ensures that users are granted access based on their roles within the organization, minimizing the risk of unauthorized access. MFA adds an extra layer of security by requiring users to provide two or more verification factors to gain access.
4. **Regular Audits and Monitoring:** Conduct regular security audits and continuous monitoring to detect and respond to potential threats promptly (Bhardwaj & Goundar, 2017). Regular audits help in identifying vulnerabilities and ensuring compliance with security policies. Continuous monitoring provides real-time insights into the security posture of the network, enabling quick response to threats.

Cloud-Based Applications:

Overview

Cloud-based applications at Tech Solutions Inc. are used for delivering customer-facing products and services. These applications are hosted on a major cloud service provider, which requires a zero-trust approach to ensure secure access and data protection.

Security Measures

1. **Identity and Access Management (IAM):** Implement a robust IAM system that includes MFA and strict access controls. Use principles of least privilege and continuous authentication to verify user identities (Rose et al., 2020). IAM systems manage user identities and access permissions, ensuring that only authorized users have access to critical systems and data.
2. **Encryption:** Ensure all data in transit and at rest is encrypted using strong encryption algorithms. Employ end-to-end encryption for sensitive data (FORCE, 2013). Encryption protects data from being intercepted or accessed by unauthorized parties, ensuring the confidentiality and integrity of sensitive information.
3. **Micro-Segmentation:** Apply micro-segmentation to create isolated segments within the cloud environment, reducing the attack surface and containing potential breaches (Dhiman et al., 2024). Micro-segmentation involves dividing the network into smaller, isolated segments, each with its own security controls, to prevent lateral movement of attackers within the network.
4. **Continuous Monitoring:** Utilize cloud-native security tools for continuous monitoring and threat detection. Implement automated responses to mitigate identified threats (FORCE, 2013). Continuous monitoring tools provide real-time visibility into the security posture of cloud environments, enabling quick detection and response to threats.

SaaS Applications:

Overview

Tech Solutions Inc. uses SaaS applications for internal business functions such as HR and finance. Employees need to access these applications securely from both remote and office locations.

Security Measures

1. **Secure Access:** Employ secure access solutions such as virtual private networks (VPNs) or secure access service edge (SASE) to protect data during transmission from remote locations (Dhiman et al., 2024). VPNs create a secure tunnel for data transmission, protecting it from interception. SASE integrates network security functions with WAN capabilities to provide secure access to applications from anywhere.
2. **Conditional Access Policies:** Implement conditional access policies to ensure that access to SaaS applications is granted based on the security posture of the device and user context (Rukhsara et al., 2016). Conditional access policies evaluate the security posture of devices and user context (such as location and behavior) before granting access to applications, ensuring that only trusted devices and users can access critical resources.
3. **Endpoint Security:** Ensure that endpoints accessing SaaS applications are secured with antivirus, anti-malware, and regular patching (Bhardwaj & Goundar, 2017). Endpoint security solutions protect devices from malware and other threats, ensuring that compromised devices do not become entry points for attackers.

On-Premises Email Services:

Overview

On-premises email services at Tech Solutions Inc. must be secured to protect against phishing, malware, and other email-based threats.

Security Measures

1. **Email Filtering:** Use advanced email filtering solutions to detect and block spam, phishing attempts, and malicious attachments (Bhardwaj & Goundar, 2017). Email

filtering solutions scan incoming and outgoing emails for malicious content, protecting users from phishing attacks and malware.

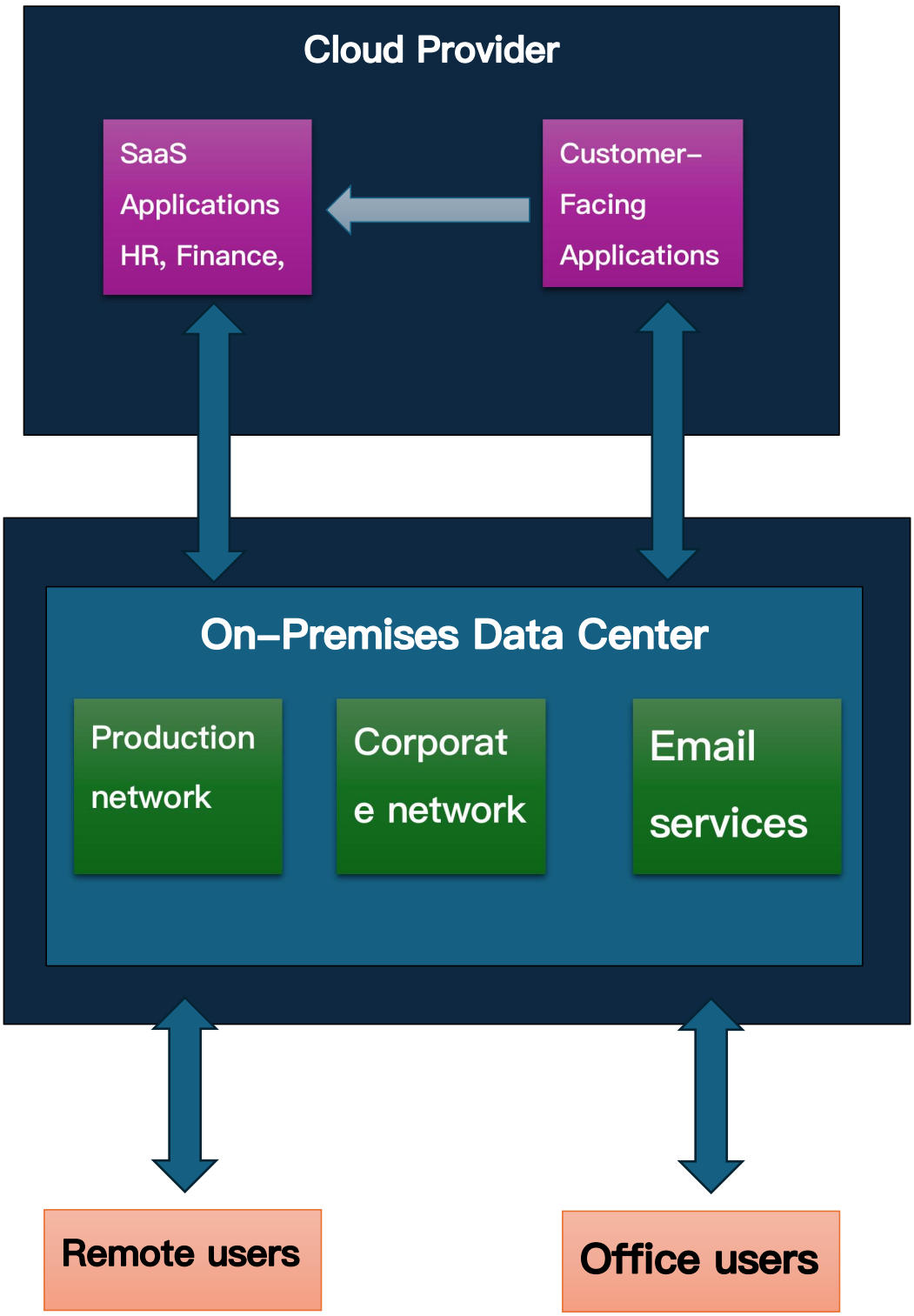
2. **Encryption:** Encrypt email communications to protect the confidentiality and integrity of messages (Force, 2013). Email encryption ensures that email messages are only readable by intended recipients, protecting sensitive information from being accessed by unauthorized parties.
3. **User Training:** Conduct regular security awareness training for employees to recognize and report suspicious emails (Dhiman et al., 2024). Security awareness training educates employees on how to identify and respond to phishing attempts and other email-based threats, reducing the likelihood of successful attacks.

Logical Architecture Drawing

Below in figure 1 is the logical architecture for Tech Solutions Inc., depicting the high-level overview of the company's hybrid environment. This includes the on-premises data center, cloud provider, SaaS applications, and the connectivity between remote employees, the corporate network, and the production network.

Figure 1

High-Level Logical Architecture of Tech Solutions Inc.



***Note**:* The diagram reflects the hybrid nature of Tech Solutions Inc.'s environment, highlighting the integration of zero-trust principles for cloud-based and SaaS applications, and a defense-in-depth strategy for legacy on-premises systems. This comprehensive approach ensures robust security across the entire IT infrastructure, protecting sensitive data and maintaining secure access to products and services. The diagram details how different components interact and are protected.

Cloud Provider

- **SaaS Applications (Software as a Service):** Used for internal processes like HR and finance. Secure access through VPNs (Virtual Private Networks) or SASE (Secure Access Service Edge) and conditional access policies ensure trusted device and user access (Samaniego & Deters, 2018).
- **Customer-Facing Applications:** Deliver products and services to customers. Security includes IAM (Identity and Access Management), encryption, and continuous monitoring (Samaniego & Deters, 2018).

On-Premises Data Center

- **Production Network:** Hosts legacy applications, utilizing network segmentation, firewalls, IDPS (Intrusion Detection and Prevention Systems), RBAC (Role-Based Access Control), MFA (Multi-Factor Authentication), and regular audits to ensure security.
- **Corporate Network:** Supports internal business functions with network segmentation and endpoint protection.
- **Email Server:** Secured with filtering, encryption, and user training to protect against phishing and malware.

Users

- **Remote Users:** Access resources securely via VPNs or SASE, with endpoint security measures in place.
- **Office Users:** Directly connect to the corporate network and SaaS applications through secure access solutions.

Connections and Security Measures

- **Cloud to Data Center:** Secured with encryption and continuous monitoring to protect data in transit.
- **User Access:** Ensures trusted access through conditional policies and endpoint security.

This architecture leverages zero-trust principles and hierarchical management to validate infrastructure and transactions, ensuring robust security across Tech Solutions Inc.'s hybrid IT environment (Samaniego & Deters, 2018).

Conclusion

The proposed security architecture for Tech Solutions Inc. addresses the unique challenges of a hybrid environment, balancing the requirements of a zero-trust model for cloud-based and SaaS applications with a traditional defense-in-depth strategy for legacy on-premises applications. By implementing these measures, Tech Solutions Inc. can ensure robust protection of its sensitive data and secure access to its products and services. The integration of advanced security measures, continuous monitoring, and user education ensures that the company remains resilient against evolving cyber threats.

References

Bhardwaj, A., & Goundar, S. (2017). Security challenges for cloud-based email infrastructure. Network Security, 2017(11), 8-11.

Dhiman, P., Saini, N., Gulzar, Y., Turaev, S., Kaur, A., Nisa, K. U., & Hamid, Y. (2024). *A review and comparative analysis of relevant approaches of zero trust network model*. *Sensors*, *24*(4), 1328. https://doi.org/10.3390/s24041328

Force, J. T., & Initiative, T. (2013). *Security and privacy controls for federal information systems and organizations.* NIST Special Publication, 800(53), 8-13.

Rose, S., Borchert, O., Mitchell, S., Connelly, S., *National Institute of Standards and Technology, Advanced Network Technologies Division, Stu2Labs, & Cybersecurity & Infrastructure Security Agency.* (2020). *Zero trust architecture*. https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf

Rukhsara, L., Aklam, F., Nawer, T., Chauhan, N. S., & Islam, M. N. (2016, May). *A conceptual cloud-based model for developing e-commerce applications in context of Bangladesh. In 2016 5th International Conference on Informatics, Electronics and Vision (ICIEV*) (pp. 117-121). IEEE.

Samaniego, M., & Deters, R. (2018). Zero-Trust Hierarchical Management in IoT. *IEEE International Congress on Internet of Things*. https://doi.org/10.1109/ICIOT.2018.00019