**Final Project Reflection**

**Yuan Tan ,Yongxin Guo,Shivam Sinha**

1. **Proposed solution**

For the Target data breach incident in 2013, our team proposed focusing on enhancing the identify and protect functions to prevent data from being leaked again. For the solution to this incident, firstly, we need to strengthen the management of suppliers and risk assessment, and implement strict third-party risk management by establishing a third-party risk assessment process to conduct comprehensive reviews and background investigations of cooperative suppliers to determine whether the third parties have the ability to implement network security protection measures and improve network security. At the same time, implement third-party access restrictions by limiting the third-party's management access rights to ensure that the third-party's network access rights are limited within a controlled range, such as network system security permissions, which can prevent third parties from attacking and stealing customer information and payment information through permission attacks, thereby improving network security and protecting customer information.

We also need to segment customer payment information, customer personal information, and system security systems to prevent attackers from stealing customer information while attacking the network system. In addition, we need to use more advanced network traffic monitoring and detection systems to improve network threat detection. When abnormal behavior is detected, potential threats can be identified through machine learning and behavioral analysis.

Strengthening data protection and secure storage can prevent data from being leaked during transmission. Encrypt sensitive data with stronger algorithms during transmission, especially during the transmission of payment information. Implement end-to-end data encryption to protect customer payment information from device to server security.

To further enhance our solution, we designed a robust AWS-based architecture that incorporates multiple security layers and scalability features to mitigate the risks associated with data breaches. This architecture integrates AWS services strategically to strengthen both the **identify** and **protect** functions.

In this architecture, we implemented **AWS Web Application Firewall (WAF)** and **Amazon CloudFront** at the network perimeter to filter incoming requests and protect against threats like SQL injection and DDoS attacks. These services ensure that only legitimate traffic reaches the internal network. **Amazon GuardDuty** and **AWS Security Hub** were deployed for continuous monitoring and threat detection, allowing for real-time identification and response to potential security threats.

The application is segmented into three distinct tiers—**Web**, **Proxy**, and **App**—each within its own **Virtual Private Cloud (VPC)**. This segmentation isolates sensitive components and ensures controlled access across different parts of the system, which protects customer information, payment data, and critical system configurations. Each VPC has its own **Network Load Balancer** to distribute traffic efficiently, while **Auto Scaling** on Amazon EC2 instances enables dynamic resource management based on demand, ensuring high availability without over-provisioning resources.

To secure data during transmission and storage, we used **AWS Key Management Service (KMS)** for strong encryption protocols. Sensitive information, especially customer payment data, is encrypted end-to-end, safeguarding it across all points from the client device to AWS storage. This comprehensive architecture reinforces data protection at multiple levels, ensuring that security measures are in place to prevent unauthorized access, detect potential threats early, and respond swiftly to any incidents.

1. **How we approached the solution**

To address the vulnerabilities exposed in the Target data breach, our team concentrated on fortifying identity management and protective functions within Target’s network architecture. Our solution mitigated risks through comprehensive third-party oversight, rigorous access controls, and intricate network segmentation, effectively reducing the attack surface while enhancing threat detection and response capabilities.

**Supplier Management and Risk Assessment**

Our initial priority was to implement a structured third-party risk management process. This included the development of a detailed risk assessment framework, utilizing tools like **AWS Config** for compliance monitoring and **AWS Trusted Advisor** for security best practices. We established criteria for evaluating supplier cybersecurity postures through **AWS Identity and Access Management (IAM)** roles and permissions, conducting thorough background checks and security audits. Each vendor underwent assessments based on criteria such as data protection protocols, incident response strategies, and adherence to standards like **NIST SP 800-53**. This proactive assessment allows for the identification of vulnerabilities in suppliers' security capabilities before granting access to Target's sensitive data.

**Access Control and Restrictions for Third Parties**

To mitigate the risk of unauthorized access, we implemented stringent access control measures for third-party suppliers through **IAM policies**. We adopted a **role-based access control (RBAC)** model that employed fine-grained permissions, ensuring that third-party access was limited to the minimum necessary resources and actions within the system. This involved defining permissions in **IAM policies** that restricted access to specific Amazon VPC resources, including subnets, EC2 instances, and RDS databases. The segmentation of permissions was designed to minimize the potential damage from a compromised supplier account, thereby creating logical barriers that protect customer information and preventing third parties from leveraging excessive privileges that could compromise payment and personal data.

**Network Segmentation and Enhanced Threat Detection**

Our network segmentation architecture utilizes a **multi-VPC design** complemented by targeted subnet configurations to isolate functions and enhance security controls across Target’s infrastructure. Each **Virtual Private Cloud (VPC)** is tailored to specific operational roles, facilitating secure access, controlled data flow, and advanced threat detection.

1. **Web Tier VPC**: This tier is deployed within a **public subnet (10.0.1.0/24)**, hosting **Amazon Elastic Load Balancers (ELB)** that distribute incoming traffic to EC2 instances running web servers. We implemented **AWS WAF (Web Application Firewall)** and **Amazon CloudFront** as part of our perimeter defense strategy to mitigate DDoS attacks and filter out malicious requests, including SQL injections. The ELB is configured to route only validated requests to the Application Tier VPC, thereby blocking unauthorized traffic effectively.
2. **Application Tier VPC**: Configured within **private subnets (10.0.2.0/24)**, this tier hosts **Application Load Balancers (ALB)** that manage traffic between EC2 instances executing application logic. The private subnets are designed to be fully isolated from the public internet, with access tightly controlled through **Network ACLs (NACLs)** and **security groups** that restrict inbound and outbound traffic to only necessary protocols and IP addresses. The security configurations ensure that direct access from external sources to application instances is rigorously prohibited.
3. **Database Tier VPC**: This tier is strictly contained within private subnets (10.0.3.0/24), facilitating communication solely with the Application Tier VPC. **Amazon RDS** instances are deployed here, configured with **AWS Key Management Service (KMS)** to provide encryption at rest for sensitive data such as customer payment information. RDS security groups enforce access rules, allowing only specific application servers, identified by their instance IDs, to interact with the database layer, thereby maintaining a stringent data protection posture.
4. **Threat Detection and Monitoring**: For comprehensive security monitoring, we integrated **AWS GuardDuty** and **AWS Security Hub** across all VPCs to provide continuous monitoring for anomalies and potential threats. These services utilize machine learning algorithms to analyze network traffic, VPC flow logs, and DNS logs, identifying deviations from normal operational patterns indicative of intrusion attempts. Alerts generated by these services facilitate rapid incident response, enabling security teams to investigate and remediate threats effectively.

This multi-layered network segmentation strategy enforces strict access control through isolated subnets, intricate IAM roles, and automated threat detection, reducing the attack surface while ensuring operational resilience and compliance with industry standards.

**Data Encryption for Secure Transmission**

Our final approach emphasized robust end-to-end data encryption, employing protocols such as **TLS (Transport Layer Security)** for secure data transmission. We implemented encryption algorithms like **AES-256** for sensitive data in transit, including payment information and personal customer data. The end-to-end encryption strategy ensures that customer data is securely transmitted across all points in the communication chain, from the initial transaction on the customer’s device to its secure storage in **Amazon S3** or **Amazon RDS**. This approach not only protects data during transmission but also fortifies the entire network against potential interception by unauthorized parties.

Through this implementation, our team learned that a multi-layered security strategy is essential for comprehensive data protection. We recognized that safeguarding sensitive data requires a combination of strict supplier evaluations, rigorous access controls, and robust encryption mechanisms. Furthermore, the integration of advanced threat detection and real-time monitoring services proved critical in enabling timely interventions against potential breaches, significantly enhancing our overall cybersecurity framework.

**III. Learned Reflection**

Throughout the project, our team gained critical insights into implementing a robust cybersecurity framework. We learned that effective protection of sensitive data requires a multi-layered security strategy, integrating defensive measures that work together to address diverse vulnerabilities. Enhancing both identity and protection functions allowed us to proactively mitigate risks across multiple access points.

A significant takeaway was the critical need for **third-party risk management**. Our rigorous **third-party risk assessment process** emphasized the importance of thoroughly vetting external partners, revealing potential vulnerabilities when access control is inadequately monitored.

Our approach to **network segmentation** and **data isolation** proved essential for bolstering security within Target's infrastructure. By isolating customer payment information, personal data, and system configurations, we minimized the risk of a single breach affecting all data types. This compartmentalization strategy effectively mitigated the impact of potential incidents by limiting attackers' access to multiple data layers.

We also gained a deeper understanding of **advanced threat detection** and **monitoring tools**. Implementing **machine learning algorithms** for behavioral analysis showcased the effectiveness of proactive monitoring in identifying anomalous patterns and potential threats. Real-time monitoring not only strengthened incident response but also highlighted the importance of early detection in reducing breach impacts.

The implementation of **end-to-end encryption** underscored the necessity of secure data transmission. By ensuring that sensitive payment data is encrypted during transit—from the user's device to storage in **Amazon S3** or **Amazon RDS**—we demonstrated the critical role of encryption protocols in maintaining data confidentiality.

The project reinforced that effective cybersecurity is a multifaceted endeavor requiring ongoing vigilance, comprehensive assessments, and the integration of advanced technologies to create a secure and resilient network environment.