PROJECT: IAM | SaaS Tech Start-up

Scenario: As a new SaaS company in the market, they have developed a cloud-based application that offers their clients a platform to manage their customer relationship management (CRM) needs. Their platform provides a range of features, including lead management, sales forecasting, opportunity tracking, and marketing automation.

They understand that their client's data is their most important asset, and they must protect it from unauthorized access, use, disclosure, or modification.

To address this concern, they have hired an IAM person to manage access to their software, systems, and data. As the IAM person, I will be responsible for developing and implementing the IAM program to ensure their platform is secure and accessible to authorized users.

My role will involve defining the IAM strategy for the startup by identifying the business and regulatory requirements, defining IAM policies and standards, and developing an IAM roadmap. I will also be responsible for implementing IAM controls to enforce the policies and ensure they work as intended.

Overall, they aim to provide their clients with a secure and reliable platform that meets their needs and expectations while complying with industry best practices and regulatory requirements.

Mission: Define the IAM strategy for the startup by identifying the business and regulatory requirements, defining IAM policies and standards, and developing an IAM roadmap

Define IAM policies and standards for the SaaS company.

(I used NIST and ISO/IEC 27001 framework to help me come up with my steps in defining my policies and standards.)

1. Conduct a risk assessment.
2. Define the IAM objectives.
3. Establish IAM policies and procedures.
4. Define roles and responsibilities.
5. Implement IAM controls.
6. Monitor and review.

NIST Cybersecurity Framework.

Identify: Conduct a risk assessment

Protect: Define IAM objectives and establish IAM policies and procedures

Detect: Implement IAM controls

Respond: Define roles and responsibilities

Recover: Monitor and review

ISO/IEC 27001

Risk assessment: Conduct a risk assessment.

Security Objectives: Define IAM objectives and establish policies and procedures.

Controls implementation: Implement IAM controls.

Roles and Responsibilities: Define roles and responsibilities.

Performance evaluation: Monitor and review.

Conduct a risk assessment!

Identify the risks and threats to the SaaS startup's systems and data and determine the potential impact on the business if those risks were to be exploited.

Focusing on 3.

1. Unauthorized access: If someone gains unauthorized access to their systems or data, they could steal sensitive information, manipulate data, or cause other types of damage.
2. Malware and ransomware: These attacks can be devastating for the SaaS startup and result in significant financial and reputational damage.
3. Third-party risks: As a SaaS startup, they may rely on third-party vendors for certain aspects of their business. Third-party vendors may pose risks to their systems and data if they do not have good security measures in place.

Unauthorized Access: Threat Modeling

For this project, I want to use the **STRIDE** framework.

Identify the asset: The sensitive data that can be accessed by unauthorized individuals.

Threat Evaluation:

- **Spoofing**: Attackers may try to impersonate legitimate users to gain access to sensitive data
- **Tampering**: Attackers may try to modify and manipulate sensitive data
- **Repudiation**: Attackers may try to deny or dispute their actions, making it difficult to track and investigate unauthorized access
- **Information Disclosure**: Attackers may try to access and view sensitive data.
- **Denial of servic**e: Attackers may try to overwhelm systems with traffic to prevent legitimate users from accessing sensitive data
- **Elevation of privilege**: Attackers may try to gain escalated privileges to access sensitive data.

Mitigation:

- **Spoofing:** Implementing strong authentication measures like multi-factor authentication, biometric authentication, or smart cards to prevent attackers from impersonating legitimate users
- **Tampering:** Use encryption to protect sensitive data and implement integrity checks to detect any modifications or tampering
- **Repudiation:** Implement logging and auditing to track all access and actions performed on sensitive data and use digital signatures or any other means of nonrepudiation.
- **Information disclosure:** Use access controls and permission levels to restrict access to sensitive data, and implement DLP measures to detect and prevent data exfiltration attempts
- **Denial of service:** Implement measures such as rate-limiting throttling or using a Content Delivery Network
- **Elevation of privilege:** Implement role-based access control (RBAC) to restrict access to sensitive data and implement the principle of least privilege to minimize access to only necessary users. Also, monitor user activity and detect any unusual or suspicious behavior.

Malware and Ransomware: Threat Modeling

Identify the asset: The SaaS startup's systems and data.

Threat evaluation:

- **Spoofing:** Attackers may spoof legitimate-looking emails or websites to trick employees into downloading malware or providing sensitive information.
- **Tampering:** Attackers may tamper with software or data to inject malware or ransomware.
- **Repudiation:** Attackers may attempt to deny their actions or the impact of their malware/ransomware.
- **Information disclosure:** Malware and ransomware may disclose sensitive information or make it publicly available.
- **Denial of Service:** Malware and ransomware may consume system resources or cause systems to crash.
- **Elevation of privilege:** Malware and ransomware may gain administrative privileges to perform unauthorized actions or access sensitive data.

Mitigate the threats:

- **Spoofing:** Implement email and web filtering to block known malicious websites and emails. Train employees on how to identify and report suspicious emails and websites.
- **Tampering:** Implement strong access controls and software validation processes to prevent unauthorized changes to software or data. Use anti-malware and anti-ransomware software to detect and block malicious code.
- **Repudiation:** Implement strong logging and auditing practices to track system activity and identify potential threats. Use digital signatures or other methods to prove the integrity of data.
- **Information disclosure:** Use encryption to protect sensitive data at rest and in transit. Implement access controls and data classification to restrict access to sensitive information.
- **Denial of service:** Implement redundancy and failover mechanisms to minimize the impact of a DoS attack. Use traffic analysis tools to identify and block DoS traffic.
- **Elevation of privilege:** Implement least privilege access controls and role-based access controls to restrict access to sensitive data and functions. Use strong authentication methods such as multi-factor authentication to prevent unauthorized access.

Third-Party Risk: Threat Modeling

Identify the Asset: The asset in this scenario is the SaaS startup's systems and data that are being accessed by third-party vendors.

Threat evaluation:

- **Spoofing:** A third-party vendor could impersonate a legitimate user to gain access to the startup's systems and data.
- **Tampering:** A third-party vendor could tamper with the startup's systems and data, causing damage or manipulating information.
- **Repudiation:** A third-party vendor could deny having performed certain actions, leading to difficulties in determining responsibility in the event of a security incident.
- **Information Disclosure:** A third-party vendor could access and disclose sensitive information without authorization.
- **Denial of Service:** A third-party vendor could intentionally or unintentionally disrupt the availability of the startup's systems and data.
- **Elevation of Privilege:** A third-party vendor could gain elevated access to the startup's systems and data beyond what is necessary for their role.
- **Evaluate and Prioritize Threats:** Based on the likelihood and impact of each threat, the following priorities can be established:
- **Spoofing:** High priority due to the potential for unauthorized access to the startup's systems and data.

Mitigate Threats:

- Thoroughly vetting and selecting vendors with good security practices and strong contractual security obligations.
- Regularly monitoring and auditing vendor access to the startup's systems and data.
- Implementing multi-factor authentication for vendor access.
- Encrypting sensitive data being shared with vendors.
- Having incident response plans in place to address security incidents involving third-party vendors.

Define the IAM objectives.

Based on the three risks, what would the potential risk be if they were to be exploited?

Unauthorized access: Could cause a Data Breach > PROTECT THE DATA

- I would need to establish strong authentication and authorization mechanisms to prevent unauthorized access. The IAM policies should ensure that users are authenticated and authorized before accessing systems and data. This includes implementing multi-factor authentication (MFA), enforcing strong password policies, and using role-based access control (RBAC) to restrict access to sensitive data.

Malware and ransomware: Could cause Service disruption.

- To prevent malware and ransomware attacks, I should ensure that the systems and data are protected by anti-virus and anti-malware software. I should also establish policies for patching and updating software to ensure that vulnerabilities are addressed promptly. Regular data backups also are conducted to ensure that they can recover from an attack if one occurs.

Third-party risks: Could cause Reputation damage.

- To manage third-party risks, I would need to establish clear policies and procedures for vetting and monitoring the vendors. The IAM policies should require vendors to have appropriate security measures, including access controls and data encryption. I can also establish contractual security and data protection requirements and regularly monitor and audit the vendors to ensure compliance with these requirements.

Establish IAM policies and standards.

Unauthorized access:

- Policy: All users must be authenticated and authorized before accessing our systems and data.
- Standard: Multi-factor authentication (MFA) must be enabled for all users.
- Standard: Passwords must be at least 12 characters long, and must be changed every 90 days.
- Standard: Role-based access control (RBAC) must be implemented to restrict access to sensitive data.
- Standard: Access requests must be approved by the appropriate manager or data owner.

Malware and ransomware:

- Policy: All employees must use company-provided devices to access our systems and data.
- Standard: All devices must have up-to-date antivirus and anti-malware software installed.
- Standard: All email attachments must be scanned for viruses and malware before being downloaded.
- Standard: Employees must be trained on how to identify and report suspected malware or ransomware attacks.

Third-party risks:

- Policy: All vendors must undergo a thorough security vetting process before being granted access to our systems and data.
- Standard: Vendor contracts must include specific security and data protection requirements, such as data encryption and data retention policies.
- Standard: Vendors must be required to notify us in the event of a security breach or data loss.
- Standard: Vendor access to our systems and data must be monitored and logged.

Define roles and responsibilities.

IAM Manager: This person would be responsible for overseeing the implementation and enforcement of IAM policies and standards. They would work closely with other stakeholders to ensure that the company's IAM program is effective and aligned with business objectives. (Azure Priviliged Role Administrator- User Administrator – Azure Information Protection Admin – Authentication Policy Administrator – Authentication Administrator -

IAM Administrator: This person would be responsible for managing user access to company systems and data, including creating, modifying, and revoking user accounts. They would also be responsible for enforcing IAM policies and standards, monitoring user activity, and reporting on potential security incidents.

System Administrator: This person would be responsible for managing the technical aspects of IAM, such as configuring identity and access management systems, setting up authentication and authorization protocols, and maintaining user directories.

Data Owners: These are the individuals or teams responsible for specific data sets within the company. They would be responsible for defining access controls and permissions for their data, in accordance with IAM policies and standards.

Managers: Managers would be responsible for ensuring that their teams comply with IAM policies and standards. They would also be responsible for reporting potential security incidents to the IAM Manager and working with the IAM team to investigate and mitigate any issues.

End Users: End users would be responsible for following IAM policies and standards, including creating strong passwords, protecting their devices and login credentials, and reporting any suspicious activity to their manager or the IAM team.

(Each company has different names they give their job titles)