David Garlisch

MSCIA Capstone

D490 - Task 3

Enhancing Security Through Multi-Factor Authentication and Least Privilege

**A and A1. Project’s Main Policies**

**Policy 1: The Enforcement of Multi-Factor Authentication (MFA) -**

**Description:**  
The MFA policy will mandate the implementation and internal use of multi-factor authentication across all critical systems, and user accounts that access, store, or utilize sensitive information. The policy ensures that an additional layer of security is added besides a user or attacker using just a password to authenticate themselves. This requires users to provide two or more verification factors to access resources.

**Improves Cybersecurity Decision-Making:**  
By enforcing MFA, decision-makers will reduce the risk of unauthorized access, especially from the ongoing phishing attacks targeting the company. MFA immensely decreases the likelihood of a security breach by making it significantly harder for attackers to access systems. This ensures that the account remains protected even if an attacker obtains a user's password. The enforcement of the MFA policy helps decision-makers prioritize higher-risk systems and privileged accounts for enhanced security. This helps lead to a more effective, efficient, and informed approach in protecting critical assets.

**Policy 2: Utilizing The Principle of Least Privilege with Role-Based Access controls (RBAC) –**

**Description:**Utilizing the least privilege policy helps us implement the principle of least privilege across the organization by using role-based access controls. Users are given only the permissions necessary to perform their specific job functions. This will greatly reduce the risk of excessive privileges and potential of insider threats.

**Improves Cybersecurity Decision-Making:**By enforcing least privilege, decision-makers can better control access, grouping users into roles for use of RBAC. This, in turn, will mitigate insider threats. It simplifies the oversight of permissions and privilege creep and ensures that employees do not have unnecessary access to sensitive systems. We can also automate this process by creating groups for users to be placed in with the correct permissions. This is especially beneficial, not to mention efficient, when one user moves to another role, a new employee gets hired on, or when an employee leaves the company. This policy effectively allows security administrators to monitor access and make better-informed decisions when revoking or modifying privileges, reducing both internal and external risks.

**B. The Solution Meets Assurance Criteria**

**Promotes Automation:**The solution promotes automation by leveraging Role-Based Access Control (RBAC), simplifying managing user permissions. We can do this by grouping users into specific roles. RBAC allows for permissions to be automatically given or revoked based on each user’s position or responsibilities within the company. This will ensure that if users move between roles, join or leave the company, their access rights are adjusted without manual intervention. This not only reduces the risk of human error, but also makes it more efficient for administrators to maintain the principle of least privilege across the organization.   
  
Multi-factor authentication (MFA) also contributes to solution automation by automatically prompting users to verify their identity through additional authentication factors when accessing critical systems or sensitive information, such as Personally Identifiable Information (PII). This helps ensure that secure authentication is enforced effectively and consistently without requiring constant manual oversight by the security team.   
  
Both of these automated processes enhance the efficiency of security operations and reduce the likelihood of errors, bolstering the company's overall security.

**Improves/Modernizes Security:**The solution significantly modernizes the organization’s security by addressing authentication and access control vulnerabilities. MFA replaces outdated single-factor authentication systems that are highly susceptible to phishing and brute force attacks. With MFA, even if a user’s password is compromised, the account remains secure because the attacker would also need a second form of authentication. This is a significant improvement in the organization’s defense against unauthorized access.   
  
RBAC helps guarantee that employees are only given access to the data and systems they need to perform their job functions. Implementing the principle of least privilege helps the organization reduce its attack surface and mitigate the risks associated with excessive permissions, insider threats, and any compromised accounts. The solution also tasks the IT Security team with ongoing monitoring and regular updates to security protocols, both of which enhance the company's ability to respond to emerging threats and maintain a secure environment.

Together, these measures improve and modernize the company’s overall security posture.

**Implements Industry-Standard Security Tools and Infrastructure or Environment:**The solution leverages industry-standard security tools and infrastructure, ensuring adherence to best practices and regulatory requirements, including GDPR and PCI-DSS. By utilizing Microsoft Azure Entra ID P1 for both RBAC and MFA, the solution employs one of the most widely recognized platforms for identity and access management, providing secure and compliant handling of user permissions. SolarWinds Access Rights Manager is also used to audit access controls and monitor user permissions, offering comprehensive audit trails and allowing the company to achieve compliance with GDPR and PCI-DSS. These tools are aligned with the strict requirements set by frameworks such as the NIST Cybersecurity Framework and ISO/IEC 27001. This helps ensure that the solution adheres to a cybersecurity gold standard or best practices for securing sensitive information and maintaining regulatory compliance.

**C. Solution with Digital Evidence and Implementation Elements**

**Digital Evidence:**The solution collects digital evidence through our ongoing monitoring and auditing of user activities across critical systems and the rest of the organization. SolarWinds Access Rights Manager allows the IT Security team to capture detailed logs of access attempts, any changes to permissions, and important security events. These logs provide a record of system activities, which shows who accessed which resources and at what date and time. This is paramount for conducting forensic analysis during security incidents because it allows investigators to trace any unauthorized access or data breaches. Microsoft Azure Entra ID P1 also tracks authentication events, any MFA prompts for users, and failed login attempts. These tools combined ensure the organization has the necessary data for forensic investigations, breach analysis, and compliance audits to enhance the company’s IT Security team the ability to respond quickly and accurately to security incidents.

**Implements CIA:**The solution addresses confidentiality, integrity, and availability using RBAC and MFA. Confidentiality is protected by limiting access to sensitive data while making sure the user has the correct permissions to view that data. This ensures only authorized personnel can access critical systems and PII. MFA adds an addition layer of protection by requiring users to authenticate their identity through multiple factors to make unauthorized access more difficult even if credentials are compromised by an attacker. Integrity is maintained by enforcing least privilege access, which reduces the chance of unauthorized changes to data or systems. Limiting what actions users can take helps prevent accidental or purposely malicious data alterations. Availability is supported through continuous monitoring and regular security protocol updates to ensure we have an up-to-date defense against any availability attacks, such as a DDOS attack. This then ensures the systems and data remain accessible to authorized users even during any potential disruptions.

**D.  Mitigates Cybersecurity Incidents**

With the use of SolarWinds and Microsoft Azure, we can take advantage of their auditing and logging tools to help provide detailed records of access attempts on user accounts and systems, any permissions changes, and security events. These tools can be used in real-time by our IT security team to stop or mitigate threats. Analyzing logs can help track incidents to see where and how they started. MFA also utilizes logs and can help our team when looking at these failed attempts to log into a user account or system. To mitigate more threats and risks the company will implement Role-Based Access Controls which will further prevent unauthorized actions by users who do not have the correct permissions. Lastly, continuous monitoring and keeping systems and policies up-to-date based on the guidelines provided by NIST Cybersecurity Framework and ISO/IEC 27001 will also help address and mitigate even more vulnerabilities.

**E. Cybersecurity Plans, Standards, or Procedures**

**Plans, Standards, or Procedures:**  
The cybersecurity plans, standards, and procedures developed for this project will focus on improving security while achieving regulatory compliance with GDPR and PCI-DSS. This includes the implementation of MFA and RBAC’s. MFA adds an extra layer of security by requiring multiple verification factors for users accessing critical systems, while RBAC utilizes the principle of least privilege and ensures that users are granted only the necessary permissions based on their job roles and functions.

The project follows industry standards, such as the NIST Cybersecurity Framework and ISO/IEC 27001, which will guide the deployment of MFA, RBAC, and continuous monitoring after implementing these tools to keep our systems up-to-date or adjust them as needed. Regular audits and system monitoring are vital to the project because they help us maintain compliance with GDPR and PCI-DSS. These processes allow for ongoing protection by identifying potential access control gaps and weaknesses, unauthorized access attempts, and opportunities for security improvements.

By integrating tools like Microsoft Azure for identity management and SolarWinds for access audits, the company can automate many security tasks for increased efficiency and accuracy of issues, and will help guarantee that systems and data remain protected from unauthorized access.

**E1. Initiatives and Regulatory Compliance:**

GDPR and PCI-DSS require strong authentication mechanisms and access control policies to protect their sensitive data in order for the company to achieve compliance. Implementing MFA adds an additional layer of authentication for users accessing any PII. The solution for PCI-DSS compliance is MFA because PCI-DSS compliance specifically requires the use of MFA for authentication for accessing systems containing payment card information. RBAC will enforce strong access controls and the principle of least privilege by limiting user access to the minimum level necessary for them to perform their job function. Using RBAC, the company can significantly reduce the risk of data breaches and unauthorized access, which helps us comply with GDPR’s data protection requirements. The solution also aligns with the company’s internal cybersecurity initiatives by focusing on mitigating insider threats and preventing unauthorized access by enforcing strong access controls.

**E2. Applications, Tools, Installation Guides, or User Guides  
  
Applications and Tools:**

* Microsoft Azure Entra ID P1: This tool was used to deploy both MFA and RBAC. It provides a unified platform for managing user identities and enforcing least privilege access controls.
* SolarWinds Access Rights Manager: This tool was used to audit access controls and monitor user activities across systems. It provides detailed reports and logs to track access attempts and changes in permissions.
* Cofense PhishMe: This tool was used for the phishing simulation program integrated into the security awareness and training program. It helped employees learn how to spot and respond to phishing attacks.

**Installation Guides:**

* The IT security team was provided a guide that outlines the process for implementing MFA across all the systems in the organization, including the critical systems.
* The RBAC configuration Guide was created by and for the IT team to easily automate the process for creating role-based access controls. This will easily allow for the users to be placed in the correct roles with the appropriate permissions efficiently and effectively without much room for error. The guide also suggests the team review and modify the roles as needed.

**User Guides:**

* MFA User Guide: This document was created to assist employees in setting up MFA on their accounts. It covered completing the authentication process using a password and a second verification method.
* Security Awareness Training Materials: The materials created with Articulate 360, provide clear instructions on using MFA, follow the principle of least privilege, and identify phishing attempts. The training also covers compliance, helping users understand their role in meeting GDPR and PCI-DSS requirements.

**F.  Post Implementation Environment:**   
With the implementation of MFA and RBAC, new systems were deployed to bolster the company’s security infrastructure further. Microsoft Azure was deployed to manage user authentication as well as enforce the principle of least privilege with RBAC. We also used SolarWinds to help log, monitor, and audit across all critical systems throughout the company. This will provide real-time information for the Security Team or Compliance Officers to review. The post-implementation environment also makes it mandatory for employees to complete the security awareness and training program, which covers MFA, RBAC, compliance with GDPR and PCI-DSS, password policies, and how to handle phishing attacks. A network diagram was created to map out the company’s new infrastructure. It shows the flow of data as well as user access points. It highlights how MFA and RBAC are applied to these systems and how SolarWinds tracks the user authentication attempts.

**1.  Improved Security Posture:**

MFA improved security posture by adding an additional layer of protection to the authentication process. This will greatly reduce the risk of unauthorized access at the company as if an attacker gains a user’s password, MFA ensures access is still denied because other additional authentication factors are still needed. This makes it much more difficult for an attacker to actually gain access to a user’s account or system at the company.   
  
The principle of least privilege with RBAC helps bolster the security at the company by only allowing the minimum amount of permissions for a user or even admin to perform heir job function. This not only reduces insider threats, but helps simplify and automate access management by automating role assignments. The IT security team can now easily audit these user permissions while granting or revoking permissions as necessary, ensuring the correct permissions are assigned and that privilege creep doesn’t happen.  
  
Our Security Awareness and Training program helps educate our users on MFA, least privilege, password policies, phishing attacks, and how to comply with GDPR and PCI-DSS regulations. This is a very important part of strengthening our overall security throughout the company. This will help reduce insider threats, reduce phishing attacks being successful, and make sure the company is compliant.

Lastly, SolarWinds will help us audit and continuously monitor, allowing for constant visibility into any access attempts and system usage by users. It will allow the IT security team to react more accurately and efficiently, as well as help with maintaining compliance with GDPR and PCI-DSS. It will help streamline our operations and decrease the likelihood of security breaches. The IT team can now automate routine access control tasks, reducing manual oversight and improving operational efficiency. This in turn enhances our overall operational efficiency, bolstering the company’s security.

**2.  Analyze New Data:**  
Utilizing SolarWinds and Microsoft Azure helps generate detailed logs and reports on user authentication and system usage and gives us additional information on the users' account permissions. The new reporting tools streamline audits, allowing them to be conducted more efficiently and effectively while identifying and rectifying security gaps. MFA can give us information on authentication prompts, which includes time stamps and user/device details. RBAC can also help the company quickly detect security threats when reviewing these controls and permissions.

**3.  Summative Evaluation Plan:**

The summative evaluation plan involved testing the MFA and RBAC systems. This included regular vulnerability scans and penetration testing to assess the effectiveness of the controls. The test showed significant improvements in preventing unauthorized access attempts, especially through MFA, which reduced phishing-related incidents plaguing the company. Though some users initially faced challenges with adapting to using MFA, additional training was given to them to help ease the adoption period.

Based on some of users finding it difficult to adopt the use of MFA, a plan of action was developed to enhance the user training program. The program focused on ease of use and understanding the importance of these security controls. We also identified a few legacy systems that struggled with full RBAC implementation, and the plan includes updating or replacing these systems to ensure compatibility with the new controls. Regular system audits and ongoing monitoring will continue to ensure that any future deficiencies are identified and corrected promptly.

**4.  Post-Implementation Risks:**

**MFA Resistance:**

* **Likelihood:** Moderate
* **Impact:** Users struggling to adapt to MFA may face delays in accessing systems or bypass security steps, increasing the risk of unauthorized access and reduced productivity. This can lead to disgruntled employees as it affects what they are used to in their daily workflow and can also cause project delays if adoption issues are widespread throughout the company.
* **Mitigation:** To address this, ongoing user training will be provided, along with simplifying MFA prompts where possible. Regular feedback will also be gathered to improve the user experience and ensure smooth adoption, which is one of the reasons we are using an Agile Framework Methodology with this project.

**Risk: Managing Access Rights:**

* **Likelihood:** Low
* **Impact:** With the use of RBAC, the IT security team will be informed on how to use these newfound controls, but there could still be mistakes made by human error. Misconfigurations or improper role assignments in RBAC could lead to unauthorized access, making insider threats that expose sensitive data easier.
* **Mitigation:** Regular audits and reviews of user permissions will be conducted to catch and correct any errors. Automation of access control processes will also help reduce the chances of human error.

5.  **F5. Meeting Stakeholders' Needs**

**Executive Management:**

* **Executive Management Needs:** Reduces risk, ensures regulatory compliance with GDPR, PCI-DSS, and protects the company's reputation.
* **Solution Meets Their Needs:** The implementation of MFA and RBAC directly supports these goals by significantly improving access control and reducing the likelihood of unauthorized access or data breaches. The solution also is in compliance with GDPR and PCI-DSS, ensuring that the company meets industry standards and maintains regulatory compliance by the use of regular audits and monitoring.

**IT Security Team:**

* **IT Security Team Needs:** The IT security team needs the tools, policies, and guides to effectively implement MFA and RBAC, monitor access, and maintain these systems with minimal disruption.
* **Solution Meets Their Needs:** Microsoft Azure for MFA and RBAC provides the IT team with automated controls to manage user access securely and efficiently. They will also be equipped with training and guides to help the team with these new tools and policies. The IT Security team will use SolarWinds, which allows them to identify and remediate security incidents quickly. Microsoft Azure helps them automate RBAC role assignments so the team can focus on other critical tasks.

**Employees:**

* **Employee Needs:** Employees require an easy-to-use system for authentication that doesn’t disrupt their daily workflows.
* **Solution Meets Their Needs:** The MFA system is user-friendly and integrated seamlessly into their daily work processes, providing enhanced security without creating significant barriers to system access. The training program developed for employees simplifies the process of using MFA and RBAC and shows them the importance of utilizing these new tools. This, in turn, will reduce user resistance and increase overall security awareness. We’ll make the systems for MFA intuitive and provide ongoing support even after their mandatory training program for a smoother transition.

**Compliance Officers:**

* **Compliance Officer Needs:** Compliance officers need solutions to meet strict regulatory standards and provide audit trails for GDPR and PCI-DSS compliance.
* **Solution Meets Their Needs:** SolarWinds is a tool that will help audit and monitor, allowing for continued compliance with GDPR and PCI-DSS. Regular audits and the tracking of access control measures ensure the company remains compliant with data protection regulations.

**G.  Post-Implementation Maintenance Plan**

**Continuous Monitoring and Audits:**With the use of SolarWinds, we will continuously monitor user access for failed MFA attempts and suspicious activity. Regular audits of logs and access controls will ensure we remain compliant with GDPR and PCI-DSS, identifying gaps or unauthorized access in real-time. These reviews will also confirm that user permissions align with the principle of least privilege.

**Security Awareness and Training Program | Feedback:**The security awareness and training program will remain mandatory for all employees and new hires, continuing beyond the project’s completion. Employees will receive ongoing education on MFA, RBAC, phishing attacks, password policies, regulatory compliance, and security best practices. Phishing simulations and security newsletters will reinforce awareness, ensuring users stay informed. Feedback will be actively gathered to identify any challenges or areas for improvement for adjustments to enhance the user's overall experience.

**Patch Management and Access Control Review:**Microsoft Azure and SolarWinds will be regularly updated to address new vulnerabilities and maintain the latest security standards. Regular reviews of RBAC will be conducted to ensure that all user permissions remain accurate and up-to-date, reducing the risk of unauthorized access.

**H.  Security Policy:  
  
Multi-Factor Authentication (MFA) Policy (University of Arkansas Information Technology Services, n.d.)**

**Purpose:**This policy aims to strengthen the organization's security posture by requiring an additional layer of authentication for users accessing systems that contain sensitive information or critical resources. This will protect against threats like phishing attacks and unauthorized access while ensuring compliance with industry standards such as GDPR and PCI-DSS.

**Scope:**This policy applies to all employees accessing the organization's critical systems, networks, and sensitive data. It includes all new and existing accounts where MFA is supported for implementation.

**Policy:**

1. **MFA Requirements:**
   * All new accounts must activate MFA before access to systems or data. Existing accounts are required to enable MFA within 30 days from the effective date of this policy
   * MFA is required for systems and applications that store or process sensitive information, especially those exposed to external networks
   * MFA will be required for remote users
   * MFA is mandatory for all accounts with administrative access to critical systems
2. **Authentication Methods:**Users must provide at least two forms of authentication chosen from the following:
   * A password or PIN
   * A mobile authentication app
   * Physical security tokens or biometric authentication (e.g., fingerprint, facial recognition)
3. **User Responsibilities:**
   * Users must register their MFA devices promptly to ensure uninterrupted access to company systems
   * If your MFA device is lost or stolen, the user must report the incident immediately to the Information Security team for remediation
4. **Monitoring and Compliance:**
   * User activity, including login attempts and MFA prompts, will be monitored through SolarWinds and other monitoring platforms to ensure compliance with this policy. Alerts will be triggered for failed login attempts or unusual activities, allowing the IT security team to investigate promptly
5. **Exemptions:**
   * Any requests for exemptions to this policy must be submitted in writing and approved by the Information Security team. Exemptions will only be considered after a comprehensive risk assessment is conducted

**Enforcement:**Failure to comply with this policy may result in restricted access to systems or other corrective actions until MFA is fully enabled on the user's account. Repeated violations could result in termination of employment.

**Effective Date:**This policy is effective as of January 1, 2025.

**Approval:  
Approved by:** Bilbo Baggins, Chief Information Officer (CIO) **Date:** January 1, 2025

**References**

University of Arkansas Information Technology Services. (n.d.). Multi-factor authentication policy. University of Arkansas. <https://its.uark.edu/about/policies/mfa-policy.php>