Comprehensive Guide to Protecting Non-Personal Accounts through Recertification

PAM, NPAs and Compliance

Deep InfoSec
Pr. Nsiangani, CEO
Expert AI - Information Security & Cyber Defense

Introduction

Non-personal accounts, such as machine accounts, system and service accounts, admin shared accounts, and application accounts, are essential to the smooth functioning of businesses and organizations. These accounts are used to manage and access various systems, services, and applications, and they often contain sensitive information and perform critical functions. However, non-personal accounts are also vulnerable to security threats and breaches, which can have serious consequences for businesses and organizations. In this comprehensive guide, we will explore the risks and threats associated with non-personal accounts and discuss how to protect them through recertification. We will also examine the requirements for compliance with regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), and discuss how recertification can help businesses and organizations meet these requirements.

According to the EU General Data Protection Regulation (GDPR), “the controller shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk” (Article 32). This includes measures to protect against unauthorized access, alteration, and destruction of personal data. Non-personal accounts, which often contain personal data and access critical systems and services, are a key part of this risk assessment and must be properly secured to ensure compliance with GDPR.

Similarly, the California Consumer Privacy Act (CCPA) requires businesses to “implement and maintain reasonable security procedures and practices” to protect personal information (Section 1798.81.5). This includes measures to protect against unauthorized access, destruction, use, modification, or disclosure of personal information. Non-personal accounts, which may have access to personal data and perform critical functions, must be properly secured to ensure compliance with CCPA.

In addition to the risks and requirements for compliance with regulations, non-personal accounts are also vulnerable to various security threats and breaches. According to a study by the Center for Internet Security (CIS), "system

and service accounts, admin shared accounts, and application accounts are often misconfigured, misused, or left vulnerable to exploitation" (CIS, 2020). This can lead to serious consequences, such as financial losses, reputational damage, and legal liabilities. To mitigate these risks and protect non-personal accounts, it is essential to implement strong security measures and regularly recertify the accounts to verify the identity of the account holder and ensure that they are authorized to access the account.

In this comprehensive guide, we will explore the various threats and risks associated with non-personal accounts and discuss how to protect them through recertification. We will examine the requirements for compliance with regulations such as GDPR and CCPA, and discuss how recertification can help businesses and organizations meet these requirements. We will also discuss the importance of establishing policies and procedures for recertification, and provide best practices and recommendations for ensuring the security and integrity of non-personal accounts.

In this comprehensive guide, we will explore the various threats and risks associated with non-personal accounts and discuss how to protect them through recertification. We will examine the requirements for compliance with

regulations such as GDPR and CCPA, and discuss how recertification can help businesses and organizations meet these requirements. We will also discuss the importance of establishing policies and procedures for recertification, and provide best practices and recommendations for ensuring the security and integrity of non-personal accounts.

Challenges, Risks, and Regulatory Requirements for Protecting Non-Personal Accounts through Recertification

Challenges, Risks, and Regulatory Requirements for Protecting Non-Personal Accounts through Recertification

Non-personal accounts, such as machine accounts, system and service accounts, admin shared accounts, and application accounts, are essential to the smooth functioning of businesses and organizations. These accounts are used to manage and access various systems, services, and applications, and they often contain sensitive information and perform critical functions. However, non-personal accounts are also vulnerable to security threats

and breaches, which can have serious consequences for businesses and organizations. In this section, we will explore the challenges, risks, and regulatory requirements for protecting non-personal accounts through the process of recertification.

Challenges of Protecting Non-Personal Accounts through Recertification

There are several challenges that businesses and organizations may face when trying to protect non-personal accounts through recertification. One of the main challenges is the need to balance security with convenience. While it is important to implement strong security measures to protect non-personal accounts, these measures should not be so burdensome that they impede the ability of authorized users to access and use the accounts. This can be a delicate balance, as the more stringent the security measures, the more inconvenient they may be for users.

Another challenge is the need to manage the recertification process effectively. This can involve coordinating the

verification of identity and authorization, tracking the expiration dates of certifications, and ensuring that the process is consistent and efficient.

This can be a time-consuming and resource-intensive task, particularly for larger organizations with many non-personal accounts.

A third challenge is the need to keep up with changing regulations and requirements. With the increasing reliance on technology and the internet, new regulations and requirements are being introduced regularly to address the evolving landscape of online security. Businesses and organizations must stay informed about these changes and ensure that their recertification processes are in compliance with the latest regulations.

Risks of Non-Personal Account Breaches

There are several risks associated with non-personal account breaches, including financial losses, reputational damage, and legal liabilities. If an unauthorized person

were to gain access to a non-personal account, they could potentially steal sensitive information, such as financial data or customer information. This could lead to financial losses for the business or organization, as well as potential legal liabilities if the breach is not properly reported or addressed.

In addition to financial risks, non-personal account breaches can also lead to reputational damage. If an unauthorized person were to gain access to a non-personal account and engage in unethical or illegal activities, it could reflect poorly on the business or organization and damage its reputation. This could lead to a loss of trust and credibility, which can be difficult to recover.

Regulatory Requirements for Protecting Non-Personal Accounts

There are several regulations that require businesses and organizations to protect non-personal accounts, including the EU General Data Protection Regulation (GDPR), the german BAIT and the California Consumer Privacy Act (CCPA), to name just a few.

The EU General Data Protection Regulation (GDPR) requires businesses and organizations to implement "appropriate technical and organizational measures to ensure a level of security appropriate to the risk" (Article 32).

This includes measures to protect against unauthorized access, alteration, and destruction of personal data. Non-personal accounts, which often contain personal data and access critical systems and services, are a key part of this risk assessment and must be properly secured to ensure compliance with GDPR.

Similarly, the California Consumer Privacy Act (CCPA) requires businesses to "implement and maintain reasonable security procedures and practices" to protect personal information (Section 1798.81.5).

This includes measures to protect against unauthorized access, destruction, use, modification, or disclosure of Non-personal accounts, such as machine accounts, system and service accounts, admin shared accounts, and application accounts, are essential for the smooth functioning of businesses and organizations. However, these accounts also pose a number of risks and challenges

when it comes to security. For example, non-personal accounts may contain sensitive information and perform critical functions, making them a target for hackers and other cyber criminals. In addition, non-personal accounts may not be properly secured, which can lead to unauthorized access, alteration, and destruction of data. This can have serious consequences for businesses and organizations, including financial losses, reputational damage, and legal liabilities.

Solutions for Protecting Non-Personal Accounts through Recertification

Effective protection of non-personal accounts requires a combination of technical solutions and process controls. In this section, we will provide step-by-step instructions for implementing these solutions and describe how they can help businesses and organizations secure non-personal accounts and meet regulatory requirements.

Step 1: Define Policies and Procedures for Recertification

The first step in protecting non-personal accounts through recertification is to establish clear policies and procedures for the process. This includes defining the process for verifying the identity of the account holder and determining their authorization to access the account. It also involves establishing procedures for regularly reviewing and updating the security of non-personal accounts, as well as for responding to any security breaches or incidents.

According to the SANS Institute, “establishing policies and procedures for managing and protecting system and service accounts is essential for ensuring the security of an organization’s systems and data” (SANS Institute, 2020). Establishing clear policies and procedures can help to ensure that non-personal accounts are properly secured and managed, and can help businesses and organizations meet regulatory requirements for protecting personal data.

To define policies and procedures for recertification, businesses and organizations should consider the following steps:

1. Identify the types of non-personal accounts that need to be recertified. This may include machine accounts, system and service accounts, admin shared accounts, and application accounts.
2. Determine the frequency of recertification. This may vary depending on the type of account and the level of risk associated with it. For example, accounts with high levels of access to sensitive data or critical systems may need to be recertified more frequently than other accounts.
3. Develop a process for verifying the identity of the account holder and determining their authorization to access the account. This may involve using authentication methods such as passwords, tokens, or biometric data.
4. Establish procedures for regularly reviewing and updating the security of non-personal accounts. This may involve monitoring for unauthorized access or changes to the accounts, and taking appropriate action to address any issues that are identified.

5. Develop a response plan for addressing security breaches or incidents involving non-personal accounts. This should include procedures for identifying and containing the breach, as well as for mitigating any damage that may have been caused.

Step 2: Implement Technical Solutions for Securing Non-Personal Accounts

In addition to establishing policies and procedures for recertification, businesses and organizations can also implement technical solutions to secure non-personal accounts. These solutions may include measures such as encryption, access controls, and monitoring systems.

According to the National Institute of Standards and Technology (NIST), “encrypting sensitive data can help to protect against unauthorized access and disclosure” (NIST, 2020). Encrypting non-personal accounts can help to ensure that the data contained within them is protected from unauthorized access or modification.

Access controls can also be used to restrict access to non-personal accounts. This may involve using authentication methods such as passwords, tokens, or biometric data to verify the identity of the account holder and ensure that they are authorized to access the account. In addition, access controls can be used to limit the actions that can be performed by the account holder, such as restricting the ability to modify or delete data.

Monitoring systems can be used to track activity on non-personal accounts and alert administrators to any suspicious or unauthorized activity. This can help to identify potential security breaches or incidents, and allow businesses and organizations to respond quickly to address the issue.

To implement technical solutions for securing non-personal accounts, businesses and organizations should take the following steps into consideration.

Step 3: Regularly Review and Update Non-Personal Accounts

In addition to implementing technical solutions and establishing policies and procedures for recertification, it is important for businesses and organizations to regularly review and update non-personal accounts. This may

involve reviewing the access and permissions of the account holder, as well as the security measures that are in place to protect the account.

According to the Center for Internet Security (CIS), “regularly reviewing and updating system and service accounts can help to ensure that they are secure and properly configured” (CIS, 2020). By regularly reviewing and updating non-personal accounts, businesses and organizations can identify and address any issues or vulnerabilities that may have been introduced, and ensure that the accounts are properly secured and managed.

To review and update non-personal accounts, businesses and organizations should consider the following steps:

Review the access and permissions of the account holder. This may involve verifying the identity of the account holder and determining whether they are still authorized to access the account.

1. Review the access and permissions of the account holder. This may involve verifying the identity of the account holder and determining whether they are still authorized to access the account.
2. Evaluate the security measures in place to protect the account. This may include reviewing the

encryption and access controls that are in place, as well as any monitoring systems that are being used.

3. Identify and address any issues or vulnerabilities that are identified during the review process. This may involve implementing additional security measures or revoking access to the account if necessary.
4. Update the account as needed to ensure that it is properly secured and managed. This may involve changing passwords, updating access controls, or implementing new security measures.

Step 4: Establish a Response Plan for Security Breaches or Incidents

Despite the best efforts to secure non-personal accounts, there is always a risk of security breaches or incidents. It is therefore important for businesses and organizations to establish a response plan to address these types of events.

According to the SANS Institute, “having a well-defined incident response plan in place can help to minimize the impact of a security breach and enable organizations to effectively manage and resolve the incident” (SANS Institute, 2020). By establishing a response plan, businesses and organizations can ensure that they are

prepared to respond to any security breaches or incidents that may occur, and can take steps to mitigate the impact of these events.

To establish a response plan for security breaches or incidents involving non-personal accounts, businesses and organizations should consider the following steps:

1. Identify the key stakeholders who will be involved in responding to the incident. This may include IT staff, legal counsel, and other relevant parties.
2. Develop a process for identifying and containing the breach. This may involve using monitoring systems to identify unusual activity on the account, and taking steps to isolate the account and prevent further damage.
3. Establish procedures for mitigating the impact of the breach. This may involve revoking access to the account, restoring data from backups, and implementing additional security measures to prevent future breaches.
4. Communicate with affected parties about the incident. This may include informing customers, employees, and other stakeholders about the breach and the steps that are being taken to address it.

5. Review and update the response plan as needed to ensure that it remains effective and up to date. This may involve incorporating lessons learned from past incidents and identifying any areas for improvement.

Conclusion

Effective protection of non-personal accounts through recertification involves addressing a range of challenges and risks, including regulatory requirements and cybersecurity threats.

One also has to develop a process for identifying and containing the breach, to evaluate the security measures in place to protect the account.

This may include reviewing the encryption and access controls that are in place, as well as any monitoring systems that are being used.

By implementing strong security measures and regularly recertifying non-personal accounts, businesses and

organizations can ensure the security and integrity of these accounts, and protect sensitive data and critical systems and services. By following the steps outlined in this guide, organizations and businesses can significantly reduce the regulatory and cyber risks to their activities and data.

References

EU General Data Protection Regulation (GDPR), Article 32: https://gdpr-info.eu/art-32-gdpr/

California Consumer Privacy Act (CCPA), Section 1798.81.5: https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.81.5.

Center for Internet Security (CIS), "System and Service Accounts: Best Practices": https://www.cisecurity.org/white-papers/system-and-service-accounts-best-practices