Info Security Policy and Procedure

PART 1

INTRODUCTION AND GENERAL POLICY DEVELOPMENT DISCUSSION

1. Importance of Information Security Policies

Information security policies form the foundation of an organization's cybersecurity posture, preventing and mitigating cybersecurity incidents. They establish a clear framework for protecting information assets, aligning with standards, guidelines, and procedures for effective implementation.

2. Policy Development Process

A systematic policy development process ensures comprehensive and effective information security policies. Key steps include:

Identify Stakeholders: Engage all relevant parties to address their needs and concerns.

Conduct Risk Assessment: Prioritize information security risks to develop targeted policies.

Draft Clear and Concise Policies: Translate risk assessment findings into actionable guidelines.

Rigorous Review: Refine policies through stakeholder feedback before finalization.

Obtain Formal Approval: Secure management support for policy implementation.

Implement and Train: Deploy technical controls and train employees on new guidelines.

Regular Review and Update: Adapt policies to evolving risks and requirements.

PART 2

ADDRESSING VULNERABILITIES IN POLICIES

GODADDY

1. Background

Millions of GoDaddy customers were impacted by the major cybersecurity trouble that occurred in December 2022 due to a malware attack. The attackers made use of a number of holes in GoDaddy's systems, such as weak passwords, insufficient intrusion detection and prevention systems (IDS/IPS), and a deficiency in routine infrastructure security checks.

Weak Passwords: Due to GoDaddy's lax password enforcement, hackers were able to enter its shared hosting environment with cPanel. This infrastructure was a prime target for attackers because it housed millions of consumer websites. Employees and consumers of GoDaddy unintentionally provided easy access points for hackers to take advantage of by utilizing weak passwords.

Inadequate IDS/IPS: GoDaddy's intrusion detection and prevention system (IDS/IPS) was not properly set to detect and prevent the attack. This gave attackers the opportunity to work for a long time in the compromised environment without being noticed. GoDaddy may have suffered less harm if an enhanced IDS/IPS had warned them about the attack sooner.

Lack of Regular Security Audits: GoDaddy was exposed to undiscovered vulnerabilities as a result of its inability to perform routine security audits of its infrastructure. Frequent audits could have found and fixed the vulnerabilities that attackers eventually took advantage of. Regular audits were neglected, which raised GoDaddy's risk of a serious security breach.

2. Policy Elements and Style

The GoDaddy malware assault emphasizes how crucial it is to modify policy components in order to address certain vulnerabilities. In order to remedy the vulnerabilities that gave rise to the attack, GoDaddy's policies should have a clearly defined purpose, scope, duties, and policy declarations.

Policies must be enforceable, succinct, and of clear understanding. To promote uniform application and prevent misunderstandings, policies should be drafted in plain and intelligible language. Additionally, they have to be succinct and concentrate on the particular weaknesses they seek to resolve. To ensure that policies are properly implemented, they should also include explicit enforcement procedures and repercussions for non-compliance.

3. Information Security Framework

Aligning policy creation with established information security frameworks has proven beneficial, as evidenced by the GoDaddy malware attack. GoDaddy should think about using a framework to direct the creation of its policies, like the ISO/IEC 27001 or the NIST Cybersecurity Framework (CSF).

These frameworks offer an organized method for handling information security risks, which includes risk identification, assessment, and prioritization in addition to the choice and application of suitable security policies. Organizations may make sure that their policies are thorough, efficient, and in line with industry best practices by lining them up with these frameworks.

4. Governance and Risk Management

The GoDaddy malware attack highlights how crucial governance structures are to guarantee the application of policies. To make sure that policies are properly applied and adhered to, GoDaddy should clearly define roles and duties for policy creation, review, and enforcement.

Developing policies also requires effective risk management. To identify, evaluate, and rank information security threats, GoDaddy should integrate risk management techniques into its policy creation process. Then, the company should create rules that reduce those risks to a manageable degree.

5. Asset Management Policies

Access Control Policy

Purpose:

To create a thorough framework for controlling access to GoDaddy's infrastructure, data, and systems, making sure that only people with the proper authorization may use the tools they require to do their jobs.

Policy Statement:

Least Privilege: The principle of least privilege will govern the allocation of access to systems, data, and facilities. This means that individuals will only be permitted the minimal level of access required to carry out their approved tasks.

User Authentication: All users must authenticate their identity using strong passwords or multi-factor authentication (MFA) before gaining access to systems and data.

Authorization: Role-based access control (RBAC) and access control lists (ACLs) are examples of authorization techniques that are used to limit access to systems and data to approved users and roles.

Segregation of Duties: Important duties, such as managing the system and handling money transfers, should be divided among several people in order to stop illegal activity and lower the possibility of fraud.

Access Reviews: Access permissions shall be reviewed regularly to ensure that they are aligned with current job roles and responsibilities.

Physical Access Control: Physical access controls, such as security cameras, biometrics, and access cards, are required to limit physical access to facilities and sensitive areas.

Remote Access: Remote access to systems and data shall be controlled through secure remote access methods, such as virtual private networks (VPNs) and two-factor authentication.

6. Physical and Environmental Security Policies

Physical and Environmental Security Policy

Purpose:

To establish comprehensive guidelines and procedures for safeguarding GoDaddy's physical infrastructure and environmental controls, ensuring the protection of critical assets and the continuity of operations.

Policy Statements:

Perimeter Security:

a. Implement physical barriers, such as fences, gates, and security checkpoints, to restrict unauthorized access to GoDaddy's facilities.

b. Install and maintain intrusion detection systems (IDS) and access control systems (ACS) to monitor and control access to facilities.

c. Conduct regular physical security assessments to identify and address potential vulnerabilities.

Data Center Security:

a. Implement secure access controls for data centers, including strong passwords, multi-factor authentication (MFA), and biometrics.

b. Employ physical security measures, such as mantrap doors, security cameras, and surveillance systems, to protect data center infrastructure.

c. Establish strict access control procedures for visitors, contractors, and third-party personnel entering data centers.

Environmental Controls:

a. Maintain appropriate temperature, humidity, and power supply conditions to protect IT equipment and data storage devices.

b. Implement preventive maintenance procedures for HVAC systems, power generators, and other critical infrastructure components.

c. Establish disaster recovery and business continuity plans to prepare for and respond to natural disasters, power outages, and other disruptive events.

7. Access Control Management Policies

Access Control Management Policy

Purpose

To establish a comprehensive framework for managing access to GoDaddy's systems, data, and facilities, ensuring that only authorized individuals have access to the resources they need to perform their job duties.

Policy Statements

Least Privilege: Access to systems, data, and facilities shall be granted based on the principle of least privilege, whereby individuals are granted only the minimum level of access necessary to perform their authorized tasks. This principle helps to minimize the potential damage that can be caused by unauthorized access.

User Authentication: All users must authenticate their identity using strong passwords or multi-factor authentication (MFA) before gaining access to systems and data. Strong passwords should be at least 8 characters long and include a mix of upper and lowercase letters, numbers, and symbols. MFA adds an extra layer of security by requiring a second factor of authentication, such as a code sent to a mobile phone, in addition to a password.

Authorization: Access to systems and data shall be controlled through authorization mechanisms, such as access control lists (ACLs) and role-based access control (RBAC), to restrict access to authorized individuals and roles. ACLs grant or deny access to specific files or resources, while RBAC assigns permissions based on job roles and responsibilities.

Segregation of Duties: Critical tasks, such as system administration and financial transactions, shall be segregated among multiple individuals to prevent unauthorized actions and reduce the risk of fraud. By separating duties, no single individual has the authority to perform all steps of a sensitive task, making it more difficult to commit fraud or misuse access.

Access Reviews: Access permissions shall be reviewed regularly to ensure that they are aligned with current job roles and responsibilities. Regular reviews help to identify and remove outdated or unnecessary access permissions, reducing the risk of unauthorized access.

Physical Access Control: Physical access to facilities and sensitive areas shall be restricted through physical access controls, such as access cards, biometrics, and security cameras. These controls help to prevent unauthorized physical access to critical assets.

Remote Access: Remote access to systems and data shall be controlled through secure remote access methods, such as virtual private networks (VPNs) and two-factor authentication. VPNs create a secure tunnel over the internet, while MFA adds an extra layer of security for remote access.

PAYPAL

1. Background

On December 6, 2022, a combination of technological flaws and governmental regulations led to the PayPal data leak. The incident's top three vulnerabilities were found to be:

Weak Authentication Mechanisms: Not asking users to give additional verification beyond a username and password when using multi-factor authentication (MFA). MFA offers an extra layer of protection.

Failing to patch systems for known vulnerabilities: It's critical to patch known vulnerabilities as soon as possible to reduce the amount of time attackers have to take advantage of them.

Inadequate logging and monitoring: Suspicious activity or possible breaches may be quickly discovered with the use of adequate logging and monitoring, which offer insightful information about system activity.

2. Policy Elements and Style:

General Purpose: Clearly state the policy's overarching objective while highlighting the significance of addressing particular flaws that were found in the event, such as shoddy access restrictions, insufficient patch management, and weak authentication. For instance, a policy addressing MFA implementation should clearly state that its purpose is to enhance authentication security by mandating the use of MFA for all users.

Scope: The scope explicitly specify the systems, data, and individuals that are covered by the policy's requirements for addressing vulnerabilities. For instance, a vulnerability management strategy should make it obvious whose data and systems are covered by it as well as who is in charge of finding, addressing, and fixing vulnerabilities.

Responsibility: Policies have to specify precisely who is in charge of carrying them out, keeping an eye on compliance, and taking appropriate action when there are infractions. A data protection strategy, for example, should specify exactly who is in charge of categorizing data, putting access restrictions in place, and routinely reviewing rights for data access.

Standards: Standards set forth particular technical requirements that must be fulfilled in order to abide by the policy. To guarantee that passwords are strong enough to thwart unauthorised access, a policy addressing password management, for instance, could set standards for password complexity, length, and usage limits.

Protocols: Procedures can guarantee that vital activities, like incident response or vulnerability remediation, are carried out reliably and efficiently while addressing vulnerabilities. An incident response strategy, for example, need to include specific steps for locating, looking into, containing, and recovering from security events.

3. Information Security Framework:

For strong and efficient security measures, policy development must be in line with existing information security standards in the wake of the December 2022 PayPal data breach. Frameworks for information security offer an organized method for handling and safeguarding sensitive data. These frameworks provide a uniform set of guidelines, norms, and processes that organizations may utilize to create efficient rules and guidelines.

The vulnerabilities could have been mitigated by aligning policy development with established information security frameworks. Frameworks, such as the NIST Cybersecurity Framework or the ISO 27001 standard, provide guidance on implementing controls that address these specific weaknesses.

For the purpose of developing comprehensive and effective policies that meet the always changing cyber threat landscape, policy creation must be in line with recognised information security frameworks. Strong standards and processes must be put in place to secure sensitive data, as the PayPal data leak provides as a reminder.

4. Governance and Risk Management:

The Information security rules must be implemented and enforced effectively, and governance structures are essential to this process.To Establishing transparent governance frameworks is essential for accountability, supervision, and communication in light of PayPal's data leak.

The strength of the governance institutions that support policy enforcement determines its efficacy. For this reason, in order to support their information security policy framework, organizations should invest in developing robust governance structures.

Developing effective information security rules requires risk management. Policy formulation in the light of PayPal's data breach necessitates a knowledge of and mitigation of risks associated with vulnerabilities. Developing policies requires careful consideration of risk, especially when it comes to cybersecurity. Businesses may greatly lower their chance of experiencing data breaches and other security events by recognizing, evaluating, and mitigating possible risks and vulnerabilities. In order to keep ahead of changing risks, organizations should have a continuous risk management strategy, making necessary adjustments to their policies and processes.

5. Asset Management Policies:

Policy 1: Identification of Assets

Every IT asset in the company has to be recognised and included in the asset inventory.

Information like the asset type, location, serial number, purchase date, and custodian should all be included in the asset inventory.

Policy 2: Classification of Assets

Assets ought to be categorized according to how important they are to the running of the company and how sensitive the data they hold is.It is necessary to create a categorization scheme to specify various criticality and sensitivity levels.

Policy 3: Protection of Assets

It is necessary to safeguard vital resources from unwanted usage, access, disclosure, interruption, alteration, or destruction.Depending on the classification level of the assets, both logical and physical security measures should be put in place to safeguard them.

6. Physical and Environmental Security Policies:

Policy 1: Physical Access Control

Policy 2: Physical Security Monitoring

Policy 3: Environmental Controls

These policies help address the vulnerabilities discovered in the incident analysis by:

Limiting Physical entry to Critical places: Policy 1 reduces the danger of insider threats and unauthorized entry by restricting access to sensitive places.

Monitoring Critical Areas for Security Vulnerabilities: In order to detect and react quickly to attempts at unauthorized entry, Policy 2 encourages monitoring and intrusion detection.

Preventing Data Loss and Downtime by Providing Protection against Fire, Water Damage, and Power.

Protecting IT Infrastructure from Environmental Hazards: Policy 3 safeguards critical IT equipment from fire, water damage, and power outages, preventing data loss and downtime.

7. Access Control Management Policies:

The creation of thorough Access Control Management Policies is essential in reaction to the vulnerabilities found in the December 2022 PayPal data breach. These regulations, which limit access to facilities, data, and systems, should tackle the vulnerabilities brought about by insufficient access controls and unauthorized access.

Policy 1: Access Control Policy

Policy 2: Access Control for Facilities

Policy 3: Access Control Incident Response

The vulnerabilities found in the PayPal data breach are immediately addressed by these rules by:

Putting MFA into Practise for High-danger Accounts: Policy 1 requires MFA for accounts that pose a danger to sensitive data by providing an additional layer of protection.

Limiting Physical Access to Facilities: In order to avoid unwanted entrance and possible data breaches, Policy 2 restricts physical access to sensitive places.

Creating an Access Control Incident Response Plan: Policy 3 offers a structure for handling access control breaches in a way that minimizes harm and exposes as little data as possible.

SOLARWINDS SUNBURST ATTACK

1. Background:

Technical Aspects of the Top Three Vulnerabilities:

Usage of Weak and Default Passwords:

Weak and default passwords are easily guessable or readily available, making them susceptible to brute-force attacks and credential theft. In the SolarWinds Sunburst Attack, attackers exploited weak passwords to gain initial access to SolarWinds' customers' internal systems.

Customers Not Adhering to Least Privilege Practices:

The least privilege dictates that SolarWinds' Orion should have access only to the resources and data necessary to perform their assigned tasks. Customers failed to adhere to least privilege practices and ended up granting excessive privileges to SolarWinds' Orion software, increasing the attack surface and potential impact of breaches.

Usage of External Drives in the Internal Network:

Though it is unclear how the attack entered the SolarWinds development environment in the first place, some reports claim that malicious USB drives were scattered in the parking lot, which some employees unintentionally plugged into SolarWinds systems. Unauthorized or uncontrolled use of external drives can introduce malware or data exfiltration risks.

Technical Criteria for Selecting Vulnerabilities:

Vulnerabilities are selected for policy consideration based on their likelihood of being exploited, their potential impact, and the availability of mitigation measures. In the context of the SolarWinds Sunburst Attack, the three vulnerabilities identified above meet these criteria:

Likelihood of Exploitation: Weak passwords, lack of least privilege, and use of external drives are common vulnerabilities that attackers frequently exploit.

Potential Impact: These vulnerabilities can lead to unauthorized access, data breaches, and malware infections, causing significant damage to organizations.

Availability of Mitigation Measures: There are well-established mitigation measures for each of these vulnerabilities, such as password strength policies, least privilege controls, and device management policies.

2. Policy Elements and Style:

Tailoring Policy Elements to Address Vulnerabilities:

Purpose: Clearly articulate the purpose of the policy, emphasizing the importance of strong password practices, least privilege principles, and secure external device usage.

Scope: Define the applicability of the policy, specifying which systems, users, and data are covered.

Responsibilities: Outline the roles and responsibilities of individuals and departments in enforcing and complying with the policy.

Standards: Establish clear and measurable standards for password strength, least privilege access, and external device usage.

Procedures: Provide step-by-step procedures for implementing and maintaining the policy, including password reset processes, access request workflows, and external device management guidelines.

Enforcement: Outline enforcement mechanisms, such as audits, reviews, and disciplinary actions, to ensure compliance with the policy. Emphasis on Clarity, Conciseness, and Enforceability. Use simple, unambiguous language that is easily understood by all users. Keep policies concise and to the point, avoiding unnecessary details. Establish clear consequences for non-compliance to ensure enforceability.

3. Information Security Framework:

Aligning Policy Development with Established Frameworks:

Information security frameworks, such as NIST Cybersecurity Framework and ISO 27001, provide a structured approach to identifying, assessing, and managing security risks. Aligning policy development with these frameworks ensures that policies are comprehensive, consistent, and aligned with industry best practices.

Framing the Creation of Effective Policies:

The framework guides the creation of effective policies by providing a structured approach to:

Risk Identification: Identifying and prioritizing security risks based on likelihood and impact.

Policy Development: Creating tailored policies to address identified risks, incorporating risk assessment findings.

Policy Implementation: Implementing policies through training, education, and technical controls. Policy Monitoring and Review: Regularly monitoring policy effectiveness and reviewing them for updates. By aligning policy development with established frameworks, organizations can ensure that their policies are effective in addressing identified vulnerabilities and mitigating security risks.

4. Governance and Risk Management:

Effective governance structures with defined roles and senior management commitment are essential for mitigating cyber threats like the SolarWinds Sunburst attack. Incorporating risk management principles into policy development assists organizations in identifying and addressing vulnerabilities, ensuring informed decision-making and resource allocation for ongoing cybersecurity effectiveness.

5. Asset Management Policies:

Purpose: To establish a comprehensive framework for identifying, classifying, and protecting critical assets to minimize the risk of unauthorized access, loss, or damage.

Scope: This policy applies to all organization-owned or managed assets, including hardware, software, data, and intellectual property.

Responsibilities: The IT department is responsible for inventorying and tracking assets, assigning asset classifications, and implementing asset protection measures. All employees are responsible for reporting any suspected asset loss, damage, or unauthorized access.

Standards: Assets shall be classified based on their criticality to the organization's operations. Critical assets shall be subject to enhanced protection measures, including access controls, encryption, and regular backups. Asset inventories shall be maintained regularly and updated promptly upon asset acquisition, disposal, or changes in classification.

Procedures: Conduct regular audits to verify asset inventory accuracy and compliance with asset protection standards. Implement a secure asset disposal process to prevent unauthorized access to sensitive data. Provide training to employees on asset identification, classification, and reporting procedures.

Enforcement: Non-compliance with this policy may result in disciplinary action, up to and including termination of employment.

Addressing Identified Vulnerabilities: This asset management policy addresses the identified vulnerabilities by Establishing a process for identifying and classifying critical assets, ensuring that adequate protection measures are implemented based on their importance. Requiring regular audits and reviews to identify and address any gaps in asset protection, minimizing the likelihood of unauthorized access, loss, or damage.

6. Physical and Environmental Security Policies:

Purpose: To establish a comprehensive framework for securing physical infrastructure and environmental controls to protect against unauthorized access, damage, and disruption.

Scope: This policy applies to all organization-owned or managed facilities, equipment, and data centers.

Responsibilities: The IT department is responsible for implementing physical security measures, such as access controls, surveillance systems, and environmental monitoring systems. Facility management is responsible for maintaining physical infrastructure and ensuring compliance with environmental regulations. All employees are responsible for reporting any suspected physical security breaches or environmental hazards.

Standards: Access to sensitive areas shall be restricted to authorized personnel. Surveillance systems shall be installed and maintained to monitor critical areas. Environmental monitoring systems shall be in place to detect fire, water leaks, and other potential hazards. Regular physical security assessments shall be conducted to identify and address vulnerabilities.

Procedures: Implement a multi-factor authentication system for physical access control. Establish clear visitor access procedures and conduct thorough background checks for visitors. Implement regular maintenance and testing of security systems. Provide training to employees on physical security procedures and incident reporting.

Enforcement: Non-compliance with this policy may result in disciplinary action, up to and including termination of employment.

Addressing Identified Vulnerabilities: This physical and environmental security policy addresses the identified vulnerabilities by Limiting physical access to critical areas and implementing multi-factor authentication, reducing the risk of unauthorized entry and potential data theft. Establishing surveillance systems and environmental monitoring measures, enabling early detection and response to potential security breaches or environmental hazards.

7. Access Control Management Policies:

Purpose: To establish a comprehensive framework for governing access to systems, data, and facilities to protect against unauthorized access, modification, or destruction.

Scope: This policy applies to all organization-owned or managed systems, data, and facilities.

Responsibilities: The IT department is responsible for implementing access control systems, assigning access privileges, and reviewing access logs regularly. Data custodians are responsible for classifying data based on sensitivity and ensuring that access is granted only to authorized personnel. All employees are responsible for complying with access control policies and reporting any suspected unauthorized access.

Standards: Access to systems and data shall be granted based on the principle of least privilege, ensuring that users only have access to the resources necessary to perform their jobs. Access privileges shall be reviewed regularly and revoked when no longer needed. Strong passwords and multi-factor authentication shall be required for all user accounts.

Procedures: Implement a tiered access control model based on user roles and responsibilities. Conduct regular audits to verify compliance with access control policies and identify unauthorized access attempts. Provide training to employees on access control procedures and password management practices.

Enforcement: Non-compliance with this policy may result in disciplinary action, up to and including termination of employment.

Addressing Identified Vulnerabilities: This access control management policy addresses the identified vulnerabilities by Implementing role-based access controls and regular reviews of access privileges, reducing the risk of unauthorized access to sensitive systems and data. Requiring strong passwords and multi-factor authentication, enhancing the security of user accounts and preventing unauthorized access attempts.

References

CSF. (n.d.). *AC: Access Control*. CSF Tools. Retrieved November 23, 2023, from https://csf.tools/reference/nist-sp-800-53/r4/ac/

CSF. (n.d.). *ID.AM: Asset Management*. CSF Tools. Retrieved November 23, 2023, from https://csf.tools/reference/nist-cybersecurity-framework/v1-1/id/id-am/

CSF. (n.d.). *Physical devices and systems within the organization are inventoried*. CSF Tools. Retrieved November 23, 2023, from https://csf.tools/reference/nist-cybersecurity-framework/v1-1/id/id-am/id-am-1/

Cybersecurity Framework | NIST. (n.d.). National Institute of Standards and Technology. Retrieved November 23, 2023, from https://www.nist.gov/cyberframework

NIST Special Publication (SP) 800-22 Rev. 1, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. (2010, April 30). NIST Computer Security Resource Center. Retrieved November 23, 2023, from https://csrc.nist.gov/pubs/sp/800/22/r1/upd1/final

NIST Special Publication (SP) 800-46 Rev. 2, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security. (2016, July 29). NIST Computer Security Resource Center. Retrieved November 23, 2023, from https://csrc.nist.gov/pubs/sp/800/46/r2/final

NIST Special Publication (SP) 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations. (n.d.). NIST Computer Security Resource Center. Retrieved November 23, 2023, from https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

NIST Special Publication (SP) 800-61 Rev. 2, Computer Security Incident Handling Guide. (2012, August 6). NIST Computer Security Resource Center. Retrieved November 23, 2023, from https://csrc.nist.gov/pubs/sp/800/61/r2/final

NIST Special Publication (SP) 800-83 Rev. 1, Guide to Malware Incident Prevention and Handling for Desktops and Laptops. (2013, July 22). NIST Computer Security Resource Center. Retrieved November 23, 2023, from https://csrc.nist.gov/pubs/sp/800/83/r1/final

Search | CSRC. (n.d.). NIST Computer Security Resource Center. Retrieved November 23, 2023, from https://csrc.nist.gov/publications/sp800

Security and Privacy Controls for Information Systems and Organizations. (2020, September 5). NIST Technical Series Publications. Retrieved November 23, 2023, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf