Designing a Security Policy for a Corporate Information System

Modern organizations rely heavily on corporate information systems that include on-premises web servers, application servers, and database servers. These systems often store sensitive data such as customer information, financial records, and proprietary business data. Because database servers typically contain the most sensitive information, they must be strongly protected through a well-defined security policy. A security policy provides guidelines and rules that help reduce risk, ensure confidentiality, integrity, and availability, and support consistent security practices across the organization. This paper discusses five important security policy issues that should be addressed when designing a security policy for a corporate information system.

One important issue that must be addressed in a security policy is access control and authentication. The policy should clearly define who is allowed to access web, application, and database servers and under what conditions access is permitted. This includes implementing role-based access control (RBAC) so users are only granted access necessary to perform their job functions. Strong authentication methods, such as multi-factor authentication (MFA), should be required for privileged accounts and database access. Limiting access reduces the risk of unauthorized users gaining entry to sensitive systems and helps protect confidential data (NIST, 2020).

A second key issue is data protection and encryption. Since database servers store highly sensitive information, a security policy should require encryption of data both at rest and in transit. Encryption helps prevent attackers from reading sensitive data even if they gain unauthorized access to systems or intercept network traffic. The policy should also define standards for encryption algorithms, key management, and secure storage of encryption keys. Protecting data through encryption is essential for maintaining confidentiality and meeting regulatory and compliance requirements (Stallings, 2018).

The third important security policy issue is network security and segmentation. A corporate information system should not allow unrestricted communication between web servers, application servers, and database servers. The security policy should require network segmentation using firewalls and access control lists to limit traffic between system components. For example, database servers should only accept connections from authorized application servers and not directly from the internet. Network segmentation helps reduce the attack surface and limits how far an attacker can move within the system if a breach occurs (NIST, 2020).

Another critical issue is logging, monitoring, and incident response. A security policy should require continuous logging and monitoring of system activity across all servers. Logs should capture authentication attempts, access to sensitive data, and system changes. The policy should also define procedures for reviewing logs and responding to security incidents. Having an incident response plan ensures the organization can quickly detect, contain, and recover from security events. Effective monitoring helps identify suspicious activity early and reduces the potential impact of an attack (Stallings, 2018).

The fifth security policy issue is patch management and system maintenance. Vulnerabilities in web, application, and database servers are often exploited when systems are not properly updated. A security policy should require regular patching, system updates, and vulnerability assessments. The policy should also define timelines for applying critical security patches and assigning responsibility

for maintenance tasks. Keeping systems up to date reduces exposure to known vulnerabilities and strengthens the overall security posture of the organization (NIST, 2020).

In conclusion, designing an effective security policy for a corporate information system is essential for protecting sensitive data stored on database servers. Addressing access control, data encryption, network segmentation, monitoring and incident response, and patch management helps reduce security risks and supports a strong defense-in-depth strategy. A well-defined security policy provides clear guidance for protecting systems and ensures consistent security practices across the organization.

References

National Institute of Standards and Technology. (2020). Security and privacy controls for information systems and organizations (SP 800-53 Rev. 5). https://www.nist.gov

Stallings, W. (2018). Effective cybersecurity: A guide to using best practices and standards. Addison-Wesley.