Specialized Security Policy

Paul Cumiskey

School of Cybersecurity, Old Dominion University

Cyse 300 26972

Dr. Md Morshed Alam

2/2/25

Security Policy for Corporate Information Systems

In the past twenty years, the corporate world has been revolutionized due to the advancement of digital technology, especially the Internet. The embracement of technology has allowed for unimaginable efficiency and profit; however, there are also some severe risks. Cyber threats have increased at a rapid rate along with the online corporate world. This is why securing corporate information systems is vital. Protecting these systems also protects sensitive company data, and business continuity, and ensures compliance with laws regulating data security. To successfully accomplish this it is important to create a comprehensive security policy that addresses all aspects of cybersecurity. This paper will go over the five crucial issues that need to be addressed in the security policy for a corporate information system consisting of on-premises web, application, and database servers.

Network Security

One of the largest and most important security issues is network security. To combat this issue the creation of a strong and secure network security is needed. The security policy should enforce the use of such as intrusion detection systems (IDS), intrusion prevention systems(IPS), as well as firewalls for the cybersecurity and IT departments. The policy should also address the organization of the network to ensure that best practices such as network segmentation are used. Network Segmentation allows traffic to be divided into categories and also helps limit the movement of bad actors in case of a breach. Lastly, the policy should ensure that there are regular vulnerability assessments. (Security Policy Rule Best Practices, n.d.)

Access Control

Another critical security issue that should be addressed in the policy is Access Controls. Access controls help defend against unauthorized access to the many servers in the corporate network. The policy should ensure that role-based access control (RBAC) and Multifactor authentication are used to ensure that users have access to what they need and only what they need. Other simple yet easily overlooked access controls are password complexity, length, expiration, and lockout requirements. (Ibm, 2024)

Employee Training

Another major issue that is often overlooked is employee training. Many data breaches are caused by human error this is why the security policy needs to address employee training. Employees should be required to be trained on phishing attacks, how to handle secure data and safe internet usage. Testing employees is also recommended if the company has the resources to do so. Most importantly the establishment of a security-focused culture is extremely important for the success and security of the company.(*Cybersecurity Framework | NIST*, 2025)

Server Security

Due to the corporate network hosting so many different servers, being web, application, and database servers, it is very important to secure those servers. This is why the security policy should include required server security techniques such as patching, vulnerability scanning, and secure configurations. Patching servers regularly is essential to ensure that all services are

up-to-date and secure. This is especially important due to the amount of different services that run on each different server. Vulnerability scanning also helps find areas bad actors would target to gain unauthorized access to the servers. Lastly, configuring each server with security in mind will make a huge difference by decreasing the amount of attack angles open on each server. (*What Is Server Security? | Glossary*, n.d.)

Monitoring and Logging

Monitoring and logging should be required by the security policy. This is because it allows users to be held accountable and for incidents to be traced. Unfortunately, if a breach does occur and there is no monitoring or logging it may take years to find out what was tampered with and how. Monitoring and Logging help us find out immediately what happened, how it happened when it happened, and what it happened to. There are some best practices and methods to increase the usefulness of monitoring and logging. One of which is centralized logging to help collect and analyze events across the many different servers. Real-time monitoring also assists by reducing response time to threats. Regular log analysis helps the cybersecurity team to understand what typically happens versus what is an anomaly. (*Security Policy Rule Best Practices*, n.d.)

Conclusion

In conclusion, a strong security policy is a necessary first step in protecting any company's data and systems. For a corporate information system consisting of on-premises web, application, and database servers the main issues that need to be addressed within the security

policy include: Network security, Access controls, Employee training, Server security, and Monitoring and logging. Combating these threats with the techniques given will drastically reduce the risk and severity of cyber breaches. This would ensure that business could run continuously as well as ward off legal trouble or stolen data.

References

Security policy rule best practices. (n.d.). https://docs.paloaltonetworks.com/best-practices/security-policy-best-practices/security-policy-best-practices/deploy-security-policy-best-practices/security-policy-rule-best-practices#:~:text=For%20investigation%20purposes%2C%20ensure%20that,in%20the%20URL%20Filtering%20Log.

Ibm. (2024, December 19). Database security. *What is database security?* https://www.ibm.com/think/topics/database-security

Cybersecurity Framework | NIST. (2025, January 14). NIST. https://www.nist.gov/cyberframework

What is Server Security? | Glossary. (n.d.). HPE. https://www.hpe.com/us/en/what-is/server-security.html