5 Important Security Policy Issues

Deziree Johnson

CYSE 300

Dr.Kovacic

Sep 17, 2023

Designing a strong security policy for a corporate information system is extremely important to protect valuable assets, even more so when it comes to on-premises web, application, and database servers that store very sensitive data. In this paper, we will look at five important security policy issues.

The first important security policy that is needed to help protect a corporate information system is data encryption. Due to the sensitive data, encryption is an essential part of the security policy. This will make it so even if someone tries to steal the sensitive data, it will be unreadable without the right key. Therefore the data will stay a secret and it will be secure. Kamariotou & Kitsios (2023) emphasize the importance of encryption as a way to protect against data compromise. The next important security policy that is needed to help protect a corporate information system is access control. This will make it so they can control who gets to access what. This is done to make sure only the right people have access to the keys. An example of this would be extra security checks, like two-factor authentication. Another security policy that is needed to help protect a corporate information system is having an incident response plan. Although there will be a lot of plans to protect, things do go wrong. When things do go wrong, a plan is needed. Having an incident response plan will ensure a quick and organized response. It will outline the steps to follow if a breach happens. Eloff (1988) emphasizes the importance of having a well-thought-out response plan in place to lessen the results of security incidents. Regular security updates are another important security policy that is needed to help protect a corporate information system. Keeping everything up to date needs to be required because over time, vulnerabilities may come, and when they do, staying updated will ensure that there aren't any holes that hackers can use. Lastly, employee training and development is an important security policy that is needed to help protect a corporate information system. Human error is inevitable and is a significant cause of security incidents. To lessen this risk, employees have to be well-informed and educated about security practices. Training them to spot problems, create strong passwords, and take care of information the correct way. Eloff (1988) emphasizes that a well-informed workforce plays a big role in the organization's security.

In conclusion, creating a strong security policy for a corporate information system, especially when dealing with sensitive data on servers, is important. We've discussed five key security areas: data encryption, access control, incident response, regular updates, and employee training. Together, they build a strong defense against potential threats, protecting data's integrity and confidentiality. These policies also ensure a quick and organized response to security issues. As emphasized by Kamariotou & Kitsios (2023) and Eloff (1988), a well-structured security policy is important for protecting an organization's assets.

References

Eloff, J. (1988). Computer security policy: Important issues. Computers & Security, 7(6), 559-562.

Kamariotou, M., & Kitsios, F. (2023). Information Systems Strategy and Security Policy: A Conceptual Framework. Electronics (Basel), 12(2), 382.