STRIDE FRAMEWORK FOR CYBERSECURITY

Introduction

The STRIDE framework is a comprehensive approach to cybersecurity threat modeling, which can identify and mitigate potential threats to an organization's information systems, such as spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege. Cybersecurity solutions designed to address the threats outlined in the STRIDE framework can provide significant benefits, but limitations must be considered.

Discussion

One strength of cybersecurity solutions based on the STRIDE framework is their ability to provide a systematic approach to identifying and mitigating potential threats. By focusing on specific categories of threats, such as Spoofing or Tampering, these solutions can provide a targeted and practical approach to securing an organization's systems (Saxena et al., 2022). This approach can be precious for organizations with complex IT environments or limited resources for cybersecurity.

Another strength of cybersecurity solutions based on the STRIDE framework is their ability to provide specific recommendations for mitigating threats. For example, a STRIDE-based solution might recommend using multi-factor authentication to address Spoofing threats or encryption to address Tampering threats. These recommendations can benefit organizations unsure of how to address specific threats or looking for guidance on best practices.

The STRIDE framework covers various potential threats, including Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. This makes it a comprehensive tool for identifying potential security issues. For example, Microsoft has used the STRIDE framework to identify security threats in its operating systems, software applications, and cloud services.

The STRIDE framework is also designed specifically for security analysis, which ensures that the focus remains on identifying potential security threats to the system (Budimansyah et al., 2021).

This can help prevent security issues from being overlooked or downplayed in favor of other concerns, such as usability or performance. For example, the US Department of Defense has used the STRIDE framework to identify security threats in its military software systems.

However, cybersecurity solutions based on the STRIDE framework also have limitations. One potential weakness is their inability to address emerging threats or threats that fall outside the categories outlined in the framework. For example, a STRIDE-based solution may not be effective at addressing threats related to social engineering or phishing attacks. Some STRIDE-based solutions may be costly to implement and maintain, which can be a barrier for organizations with limited resources.

An example of a cybersecurity solution based on the STRIDE framework is the Microsoft Threat Modeling Tool. This tool uses the STRIDE framework to help organizations identify potential threats to their systems and provides specific recommendations for mitigating those threats (Kim et al., 2022). Another example is the OWASP Threat Dragon, an open-source tool that uses the STRIDE framework to help organizations identify potential security threats and vulnerabilities in their software applications.

Conclusion

In conclusion, cybersecurity solutions based on the STRIDE framework can provide valuable benefits, but they also have limitations that must be considered. Organizations should carefully evaluate the strengths and weaknesses of these solutions before deciding which ones to implement.

Reference

Kim, K. H., Kim, K., & Kim, H. K. (2022). STRIDE-based threat modeling and DREAD evaluation for the distributed control system in the oil refinery. *ETRI Journal*. https://onlinelibrary.wiley.com/doi/abs/10.4218/etrij.2021-0181

Budimansyah, A., Soetomo, M. A. A., & Lim, C. (2021, October). Risk and Privacy Evaluation for RDAP System. In *2021 6th International Conference on New Media Studies (CONMEDIA)* (pp. 129-134). IEEE. https://ieeexplore.ieee.org/abstract/document/9617166/

Saxena, P., & Patel, R. B. (2022). MODELING THREAT TREES THROUGH STRIDE MODEL CONCEPT FOR THE BANKING SECTOR. *Ann. For. Res*, *65*(1), 11071-11086. https://www.e-afr.org/login/pdf/11071.pdf