2024/25_N17 - Threat Modeling in Modern Software Architectures

Proposta de Bolsa/Estágio na Altice Labs

ID do Projeto	2024/25_N17
Departamento	SSO
Proponente	Mafalda Gimarães Nunes Paulo Miguel Vieira
Data de validade	31-Dec-2024

IDI - Áreas Chave

Security & Privacy

Tema / Título

Threat Modeling in Modern Software Architectures

Contexto

An interconnected world with an increasing number of systems, products, and services relying on the availability, confidentiality, and integrity of sensitive information is vulnerable to attacks and incidents. Unfortunately, the threat landscape expands and new threats, threat agents, and attack vectors emerge at all times. Threats can come from outside or within organizations, and they can have devastating consequences. Recent cyber attacks (such as MOVEit and AT&T attacks) and the approval of more strict regulations (like the European GDPR and the NIS2 Directive) put tremendous pressure on the need for various industries to ascertain the security of their products and services. Attacks can disable systems entirely or lead to the leakage of sensitive information, which would diminish the consumer's trust in the system provider. Defending against these threats requires that organizations are aware of such threats and threat agents.

Threat modeling plays a vital role in architecting and designing systems with security in mind. It is a process by which potential threats, such as structural vulnerabilities, can be identified, enumerated, and prioritized all from a hypothetical attacker's point of view. By incorporating threat modeling into the design process, organizations can proactively address security concerns and build robust and resilient systems.

Objetivos do Projeto

Altice Labs incorporates security-by-design principles in its software development lifecycle, which includes performing threat modeling. In this regard, the Microsoft Threat Modeling Tool (TMT) is used to draw flow diagrams, identify threats, and propose mitigations. The main goal of this project is to improve the current threat modeling process at Altice Labs, by incorporating threats and mitigations specific to modern software architectures (microservices, Kubernetes, Cloud, etc.) in the used tool. This includes the gathering of state-of-the-art threats, mitigations, and best practices in these modern architectures, as well as the development of Microsoft TMT templates with the respective threats and mitigations. The developed templates should then be tested with an Altice Labs system and the respective mitigations implemented, where applicable, to validate the templates' ability to address Altice Labs needs.

Aspetos Inovadores

- Threat Modeling;
- Microservices;
- Kubernetes;
- Cloud.

Ferramentas a utilizar

- Microsoft Threat Modeling Tool (TMT);
- Kubernetes;
- Private Cloud (OpenShift) and Public Cloud (AWS).

Referências Bibliográficas

- https://www.linkedin.com/pulse/role-threat-model-architecting-designing-security-mind-rahul-baviskar
- https://cheatsheetseries.owasp.org/cheatsheets/Threat_Modeling_Cheat_Sheet.html
- https://microsoft.github.io/Threat-Matrix-for-Kubernetes/
- https://attack.mitre.org/matrices/enterprise/containers/
- https://cheatsheetseries.owasp.org/cheatsheets/Kubernetes_Security_Cheat_Sheet.html
- https://cheatsheetseries.owasp.org/cheatsheets/Microservices_Security_Cheat_Sheet.html
- https://attack.mitre.org/matrices/enterprise/cloud/
- https://cheatsheetseries.owasp.org/cheatsheets/Secure_Cloud_Architecture_Cheat_Sheet.html

Atividades

- Research state-of-the-art best practices concerning modern software architectures (Microservices, Kubernetes, Cloud);
- Develop Microsoft TMT templates with the researched threats and mitigations for modern software architectures;
- Test the developed templates in the context of an Altice Labs application;
- Write a final report with the main findings of the project.

Competências Chave Requeridas

- Security knowledge, more specifically regarding microservices, Kubernetes, and cloud security;
- Critical thinking;
- Good communication skills.

Orientador (nome e e-mail)

Mafalda Nunes - mafalda-g-nunes@alticelabs.com

Paulo Vieira - paulo-m-vieira@alticelabs.com

Para concorrer podes enviar a tua candidatura, envia e-mail para o Programa GENIUS: genius@inova-ria.pt