OKVIRJI MODELIRANJA INFORMACIJSKO VARNOSTNIH GROŽENJ

Nika Jeršič[1], Muhamed Turkanović[1]
[1] Fakulteta za elektrotehniko, računalništvo in informatiko, Koroška cesta 46, 2000 Maribor
nika.jersic@um.si, muhamed.turkanovic@um.si

Modeliranje informacijsko varnostnih groženj je namenjeno identifikaciji, kategorizaciji in ublažitvi varnostnih groženj v programski in strojni opremi, sistemih, ter organizacijskih procesih. Za ta namen so bili razviti številni okvirji in metodologije, pri čemer ima vsaka svoj specifični fokus in področja uporabe.

Z okvirji izvajamo analizo stopnje resnosti in analizo možnosti izkoriščevanja groženj, s strani napadalcev. Takšne analize, še posebej v začetnih korakih razvoja sistema, nam v le-teh pomagajo, da se lahko v prihodnosti izognemo morebitnim ranljivostim.

Kljub prednostim, ki jih prinašajo, se zaradi dolgih postopkov, ki so povezani z izvedbo takšnega modeliranja informacijsko varnostnih groženj, le-ti v praksi ne uporabljajo pogosto.

V prispevku bomo podrobneje predstavili nekatere znane okvirje, tj. STRIDE, Attack Tree, LINDDUN in PASTA. Prav tako bomo predstavili rezultate raziskave, kjer smo s pomočjo laboratorijskega eksperimenta analizirali uporabniško izkušnjo omenjenih metod med študenti. Ti so se tekom svojega študija na Fakulteti za elektrotehniko, računalništvo in informatiko, izobraževali v dveh modulih, Informacijska varnost in Informacijski sistemi. V okviru raziskave smo tudi ugotavljali, kako so študentje, glede na izbran modul sprejeli uporabniško izkušnjo posameznih metod.

Ključne besede: Kibernetska varnost; analiza ranljivosti; modeli analiziranja ranljivosti.

INFORMATION SECURITY THREAT MODELLING FRAMEWORKS

Information security threat modelling aims to identify, categorise and mitigate security threats in software, hardware, systems and organisational processes. Several frameworks and methodologies have been developed for this purpose, each with its own specific focus and application areas. The frameworks are used to analyse the severity level and the potential for attackers to exploit threats. Such analyses, especially in the initial steps of system development, help us to avoid potential vulnerabilities in the future.
Despite their advantages, they are not widely used in practice due to the lengthy procedures involved in carrying out such modelling of information security threats.
In this paper, we will present in more detail some of the well-known frameworks, i.e. STRIDE, Attack Tree, LINDDUN and PASTA. We will also present the results of our research, where we analyzed the user experience of the mentioned methods among students by means of a laboratory experiment. During their studies at the Faculty of Electrical Engineering, Computer Science and Informatics, these students were trained in two modules, Information Security and Information Systems. The survey also investigated how students perceived the user experience of each method, depending on the module chosen.

Keywords: Cyber security; threat analysis; threat modeling methods.