TESTIRANJE KIBERNETSKE ODPORNOSTI S SIMULACIJO NAPADOV

Marko Pust, Simon Simčič
SRC, Tržaška 116, 1000 Ljubljana
marko.pust@src.si, simon.simcic@src.si

Večina organizacij ima večplastno zaščito svojega IT-okolja, sestavljeno iz požarnih zidov, dvo-stopenjske avtentikacije, zaščite delovnih postaj. Pogosto pa se zastavi vprašanje, ali so naši varnosti sistemi ustrezni, ali bi zaznali kibernetski napad in bi se znali naj ustrezno odzvati.

Testiranje kibernetske odpornosti je ključni del upravljanja tveganj v sodobnih organizacijah. Testiranje organizacijam omogoča, da odkrijejo ranljivosti v svojih informacijskih sistemih, preverijo postopke in učinkovitost varnostnih ukrepov ter ocenijo pripravljenost osebja na kibernetske napade. Proces preverjanja kibernetske odpornosti je relativno širok pojem. Največkrat ga povezujemo z vdornimi testi, ki pomagajo razumeti, kako bi napadalec izkoristil varnostne luknje. Nadgradnja vdornih testov so tako imenovane »red teaming« vaje, kjer želimo z dejanskimi obnašanjem napadalcev preveriti, kako dobro lahko organizacija zazna in se odziva na kibernetske incidente. Tudi socialni inženiring je ena od vrst testiranja kibernetske odpornosti, kjer želimo preveriti odziv zaposlenih na pridobivanje zaupnih informacij preko prevar, kot so lažno predstavljanje (phising) ali podobno.

V zadnjem času pa se vse bolj uveljavljajo testiranja kibernetske odpornosti s simulacijo kibernetskih napadov. Simuliramo lahko različne vektorje napada glede na okvir MITRE ATT&CK. Lahko uporabimo zgolj posamezno tehniko, ali pa simuliramo celotno taktiko izbrane »hackerske« skupine. Prednost simulacije kibernetskega napada je nedvomno v tem, da lahko v relativno kratkem času preverimo širok spekter različnih varnostnih groženj. Ker pri tem naredimo tudi integracijo z varnostnimi sistemi, kot so požarni zidovi, SIEM ali EDR, dobimo odgovor katere napade bi naš sistem zaznal, blokiral in kateri bi bili uspešni. Z vključitvijo oseb, ki skrbijo za kibernetsko varnost, dobimo tudi informacijo kako hitro in kako uspešno se odzovejo na kibernetski napad.

V prispevku bomo pokazali kako se v podjetju SRC ukvarjamo s simulacijami kibernetskih napadov, obenem pa bomo predstavili tudi nekaj praktičnih izvedb simulacij in njihovih rezultatov.

Ključne besede: kibernetska odpornost; simulacije kibernetskih napadov; MITRE ATT&CK; vdorni testi; odziv na kibernetske napade; red team vaje.

TESTING OF CYBER RESILIENCE WITH ATTACK SIMULATION

Cyber resilience testing through the simulation of cyber-attacks is becoming increasingly common. We can simulate various attack vectors based on the MITRE ATT&CK framework. We might use a single technique or simulate the entire tactics of a chosen hacker group. The advantage of cyber-attack simulation is undoubtedly that we can test a wide range of different cyber-attacks in a relatively short time. In doing so, we also integrate with security systems such as firewalls, SIEM, or EDR. This provides insights into which attacks our systems would detect, which it would block, and which would be successful. If we include individuals responsible for cybersecurity in the simulation, we can also obtain information on how quickly and effectively they respond to a cyber-attack.

Keywords: cyber resilience; cyber-attack simulations; MITRE ATT&CK; penetration tests; response to cyber-attacks; red team exercises.