VARNOSTNI PREGLED APLIKACIJ

Ali imajo uporabniki aplikacij res dostop le do svojih podatkov?

Varnostni pregled aplikacij je namenjen odkrivanju morebitnih varnostnih groženj in pomanjkljivosti posameznih aplikacij. Le-te lahko ob zlonamernem napadu omogočijo izvedbo nepooblaščenih sprememb, ki lahko vplivajo na zaupnost, razpoložljivost in celovitost podatkov v sami aplikaciji (npr. nepooblaščen dostop, spreminjanje podatkov, nedelovanje aplikacije).

V ozadju delovanja aplikacij so lahko različne tehnologije (spletne, mobilne, klasične). Ne glede na njihovo vrsto so lahko varnostne grožnje na strani:

- odjemalca,
- omrežja oz. transportne poti ter
- strežniške infrastrukture.

Celovit varnostni pregled aplikacij zato poteka v več fazah, znotraj katerih podrobno preučimo arhitekturo aplikacije, gradnike in samo delovanje aplikacije. Tipične pomanjkljivosti aplikacij so:

- dostop do podatkov brez prijave;
- neustrezna lokalna hramba podatkov;
- izvedba akcij v imenu drugega uporabnika, kot so izvedba transakcij, vklop/izkop storitev itd.;
- sprememba gesla drugega uporabnika in s tem prevzem njegovega uporabniškega računa;
- eskalacija privilegijev uporabniških pravic, ki uporabniku omogočijo več možnih aktivnosti, npr. spremembo cen itd.;
- dostop do podatkov oziroma spreminjanje podatkov drugega uporabnika.

S podrobnim varnostnim pregledom, ki vključuje tudi uporabniško prijavo, dobite nedvoumen odgovor, ali so varnostne kontrole v aplikaciji ustrezne.

Najpodrobneje pa lahko varnostne pomanjkljivosti odkrijemo s pregledom izvorne kode aplikacij, saj so prav napake v kodiranju primarni vir težav. Pri tem je pomembno, da izvorno kodo preverijo neodvisni strokovnjaki za aplikacijsko varnost, ki niso sodelovali pri razvoju aplikacije. Pregled izvorne kode aplikacije poteka v več korakih, pri čemer naročnik zagotovi vse razpoložljive informacije (princip »bele škatle«). V prvem koraku se uporabi namensko programsko orodje, ki prepozna varnostno problematična mesta v programski kodi. Le-ta se nato ročno natančno preveri v sodelovanju z razvijalcem programske opreme na strani naročnika ter svetovalcem za varnost in razvojnim specialistom na strani izvajalca. V zadnjem koraku se s penetracijskim testom nedvoumno še potrdi ugotovljene varnostne pomanjkljivosti.

Informacije

SIQ Ljubljana
Preverjanje informacijskih tehnologij
T: 01 4778 345
E: infosec@siq.si

www.siq.si