

VARNOSTNI PREGLED INFORMACIJSKE INFRASTRUKTURE



Ali zaupate vsem členom vaše IT?

S polnim razmahom elektronskih komunikacij je postala varnost informacijskih sistemov ključnega pomena za poslovanje organizacij. Varna postavitve in vzdrževanje informacijske infrastrukture sta še posebej pomembna, saj s kompleksnostjo in raznolikostjo informacijskih sistemov narašča možnost varnostnih pomanjkljivosti, težje pa jih je tudi odkriti. Varnost celotnega informacijskega sistema je namreč odvisna od najšibkejšega člena. Že ena varnostna pomanjkljivost lahko izniči številne vpeljane varnostne ukrepe (npr. privzeta administrativna gesla).

Splošni pregled ranljivosti

S takšnim pregledom boste dobili osnovno informacijo o izpostavljenosti vaše informacijske infrastrukture zlonamerni kodi in najpogostejšim grožnjam, ki jih zaradi znanih ranljivosti ali napak v konfiguraciji lahko izkoristijo že neizkušeni napadalci. Pregled se izvede z avtomatiziranimi orodji, ki z različnimi tehnikami in posebno oblikovanimi zahtevki sistematično preverijo dostopnost storitev in znane ranljivosti. Tovrstni pregledi se najpogosteje izvajajo v organizacijah, ki so dolžne redno preverjati stanje informacijske varnosti zaradi zahtev IT revizorjev.

Zunanji varnostni pregled (vdorno testiranje)

Namenjen je odkrivanju morebitnih varnostnih groženj, ki pretijo informacijski infrastrukturi iz javno dostopnega omrežja. Pri tem se uporabljajo metode in orodja, ki so prisotna ob dejanskih spletnih napadih. Ciljni sistemi, ki se preverjajo, so spletni strežniki in spletne poslovne aplikacije, poštni strežniki in druge podporne storitve, uporabljeni varnostni sistemi in mehanizmi zaščite (požarni zidovi, IPS itd.) ter druge javno dostopne storitve organizacije.

Notranji varnostni pregled

Namen je odkriti morebitne varnostne grožnje in ranljivosti informacijske infrastrukture ob namernih ali nenamernih škodljivih aktivnostih zaposlenih oziroma ob napadu iz notranjega omrežja. Zajema pregled ustreznega načrtovanja informacijskega sistema, pregled dostopnosti ter nastavitve strojne in programske opreme, pregled VoIP/IP telefonije, pregled brezžičnega omrežja in mobilnih naprav, pregled ustreznosti varnostne politike in pravil vzdrževanja sistemov ter varnostni pregled ključne programske opreme.

Informacije

SIQ Ljubljana

Preverjanje informacijskih tehnologij

T: 01 4778 345

E: infosec@siq.si