

Hekerski načini vdorov in zaščita pred njimi

Računalniki po vsem svetu sistematično postajajo žrtve nevarnih vdorov. Vdori niso zgolj zelo razširjen pojav, pač pa postajajo vse bolj brezhibni, tako da napadalec ogrozi sistem, ukrade vse, kar je vrednega, in popolnoma zbrši sledi za sabo v samo dvajsetih minutah.

Če želite hekerjem preprečiti vdiranje v vaše omrežje, morate najprej razumeti njihov način razmišljanja.

Pridružite se nam na tečaju Ethical Hacking and Countermeasures, spoznajte hekerske načine vdorov in zaščitite vaš sistem pred hekerji.

Kako lahko usposabljanje pripomore k večji varnosti vaših sistemov?

S tehničnega vidika je pomembno razumeti, da heker ne razmišlja v skladu s splošno sprejetimi normami. Usposabljanje za naziv certificiranega etičnega hekerja (Certified Ethical Hacker) vas nauči, kako razmišljati kot heker.

Z napredkom tehnologije in vse večje odvisnosti organizacij od nje, so informacije podjetja postale kritična komponenta preživetja. Cilj etičnega vdiranja je pomagati organizacijam, da odkrijejo vrzeli z vdiranjem v lastne sisteme, vse dokler ostajajo na meji legalnega. Ta filozofija izhaja iz ideje, da se da tatu ujeti, če razmišljamo kot on.

Če vdiranje vsebuje ustvarjalnost in nekonvencionalno razmišljanje, ranljivostni testi in varnostna preverjanja organizaciji ne nudijo varnostnega zagotovila. Da se organizaciji zagotovi ustrezno zaščito informacijskih pridobitev, mora pristopiti k zagotavljanju varnosti »iz globine«. To pomeni vdirati v lastno omrežje in oceniti njegovo varnostno ranljivost in izpostavljenost.

Za mnenje smo povprašali izvršnega direktorja informatike v organizaciji Security Systems Resource International v Londonu, g. Rajiva Kapoorja.



Katera je, po vašem mnenju, danes največja varnostna grožnja?

Dejal bi, da obstaja več pomembnejših groženj. Naj omenim le tri. Prva je kraja identitete. Poleg dejanske, osebne identitete, imamo danes vsi tudi virtualno identiteto. Če jo kdo ukrade, virtualno postane ta oseba. Trgovanje z ukradenimi identitetami je na spletu zelo razširjeno. Obstaja tudi nevarnost od znotraj. Vsi vemo, da kriminalci do sistemov dostopajo od zunaj, vendar pa največ škode podjetjem, organizacijam in njihovim sistemom povzročijo njihovi lastni zaposleni. Najbolj spektakularen primer tega je prevara v družbi Societe Generale, kjer je en sam človek povzročil izgubo v višini 4,9 milijarde EUR. Na tretjem mestu so priprave držav po vsem svetu na kibervojno. To povzroča novo tekmo v oboroževanju. Ste vedeli, da dobro obveščeni viri trdijo, da obstaja že 40.000 kitajskih hekerjev, ki zbira informacije iz ameriških podatkovnih zbirk?

Kako ocenjujete stanje v Sloveniji?

Tako bom rekel, voda vedno teče proti najnižji točki. S tem želim povedati, da je za varnost veliko bolje poskrbljeno v državah, ki so tradicionalno glavne tarče hekerjev, kot so Velika Britanija, Nemčija in ZDA. Poleg tega se v Sloveniji gospodarstvo hitro razvija. Ta dva dejavnika skupaj privabljata vedno večje število kriminalnih hekerjev. Isto razmišljanje je pripeljalo do tega, da so tarče postala mala in srednje velika podjetja, ker še niso dovolj vložila v varnost.

Poslovne pridobitve

- **Stalnost:** Redno boste lahko opravljali preizkuse in sprejemali protiukrepe.
- **Povrnitev naložbe:** Bolje boste izkoriščali varnostno strojno in programsko opremo, v katero ste že vložili.
- **Komunikacija in ocenjevanje:** Bolje boste komunicirali s svojimi zunanji ponudniki varnostnih storitev in ocenjevali njihovo delo.

Naložbe v varnostna usposabljanja vam bodo prihranile veliko težav in denarja.

