Informacijska varnost

Pogosta varnostna tveganja v družbah

..Kljub vsakdanjemu upravljanju s tehnologijo se večina podjetij ne zaveda pomembnosti varstva informacijskih sistemov in podatkov pred nezaželenimi posegi nepooblaščenih oseb..

Ti lahko z uporabo, spremembo, uničenjem ali krajo podatkov in intelektualne lastnine družbi povzročijo veliko premoženjsko škodo, izgubo ugleda in celo za določen čas onemogočijo poslovanje.

Najpogostejša tveganja

Največje tveganje družbi predstavlja kader. Ne samo škodoželjni nekdanji zaposleni, temveč tudi neprevidni in z informacijsko varnostjo pomanjkljivo seznanjeni zaposleni. Ti lahko nevede nepooblaščenim osebam, ki uporabljajo zvijačne in vedno bolj sofisticirane metode, omogočijo dostop do občutljivih podatkov. Tudi če storilci v prvi fazi dobijo samo navidezno neškodljive podatke o uporabniškem imenu in geslu elektronske pošte, pa lahko s tem pridejo do še občutljivejših informacij in gesel. Podatke pridobijo na različne načine, na primer s »pharmingom« – ko storilec napade strežnike DNS in uporabnike preusmeri na nezaželene spletne strani, čeprav so uporabniki vnesli pravilen naslov URL. Ker pa je spletna stran kopija originalne, se napake niti ne zaveda in vnese svoje podatke. Storilec nato lahko na pravi strani uporabi tako pridobljena gesla in uporabniška imena. Drugi primer je, ko s programom, ki ga je naš zaposleni ob odpiranju okužene pošte z zlonamerno kodo naložil na računalnik, prenašajo podatke z beleženjem tipkanja. Pozorni moramo biti tudi na primere »phishinga« (v elektronskem sporočilu banke, ki je videti legitimno, nas zvabijo na lažno stran, kjer vtipkamo geslo za dostop do TRR-ja družbe ali pa na Facebooku prek navidezne objave prijatelja kliknemo na zlonamerno stran) ali pa neposredne vdore v informacijske sisteme družbe.

Najpogostejši razlogi, ki ob izkoriščanju nevednosti kadra omogočajo storilcem dostop do podatkov, so:

- uporaba službenih telefonov, računalnikov in elektronske pošte v zasebne namene;
- dostop do službenih računalnikov in mobilnih naprav je omogočen sorodnikom in drugim nepooblaščenim osebam;
- uporaba zasebnih računalnikov v službene namene, saj zaposleni in svetovalci nimajo službenih;
- programska oprema se ne nadgrajuje oziroma posodablja, zaradi česar so naprave izpostavljene novejšim tehnikam vdorov;
- uporaba neavtoriziranih aplikacij;
- prenašanje službenih podatkov na zunanje diske in uporaba na domačih računalnikih;
- slaba gesla ali uporaba enega gesla na več straneh – storilec lahko na nekem računu, ki ni tako zelo pomemben, pridobi geslo, ki ga uporabi za dostop do občutljivega računa;
- shranjevanje podatkov v oblakih (Clouds);
- onemogočanje vzpostavljene varnostne kontrole zaradi enostavnejšega, hitrejšega dostopa v sistem;
- neprevidna uporaba naprav v javnosti, ko lahko storilec neposredno vidi vtipkano geslo;
- račune uporablja več zaposlenih ali pa ima več zaposlenih dostop do map s pomembnimi podatki.

Preprečevanje tveganj

Kako lahko poskrbimo za varnost podatkov in omrežij ter omejimo tveganja in preprečimo morebitne incidente?

Seveda je treba imeti dobre antivirusne programe, posodabljati programsko opremo, takoj po prenehanju zaposlitve delavca temu onemogočiti dostop do sistema in drugo. Zavedati pa se je treba, da je ravno tako pomemben del zaščite pred nezaželenimi in nezakonitimi vdori in krajami izobraževanje zaposlenih. Seznaniti jih je treba o pomembnosti kakovostnih gesel, ki jih je v določenem obdobju treba spreminjati, o socialnem inženiringu in njegovih pasteh, jih poučiti, da lahko kliknejo le na povezave, za katere so prepričani, da prihajajo od zaupanja vrednega pošiljatelja. Nekatera podjetja se odločajo tudi za interne poskuse »phishinga«, na podlagi katerega ugotovijo, kolikšen delež delavcev se odzove na tako prevaro. Stroški preventive so namreč veliko nižji, kot pa nas lahko stanejo težave, ki lahko nastanejo zaradi nepazljivosti oziroma nepoznavanja informacijske varnosti. (P. R.)

EUDACE, d. o. o.
Verovškova ulica 60
1000 Ljubljana
M: +386 (0) 31 337 392
T: +386 (0) 599 42 160
E: igor@eudace.eu
W: www.eudace.eu