



Socialna omrežja

V trenutku lahko ostanete brez vsega

..SOCIALNA OMREŽJA SO POSTALA PRIROČNO SREDSTVO SPLETNIH KRIMINALCEV TAKO ZA KRAJO IDENTITET KOT IZVAJANJE NAJHUŠIH OBLIK KAZNIVIH DEJANJ..

Socialna omrežja so med spletnimi deskarji vse bolj priljubljena. Mnogim so namreč v veliko pomoč predvsem pri ohranjanju osebnih, poslovnih in družinskih stikov. Trenutno najbolj priljubljeno socialno omrežje Facebook uporablja že več kot 750 milijonov uporabnikov, pri čemer njihovo število še vedno narašča. Priljubljenost socialnih omrežij žal s pridom vse bolj izkoriščajo spletni kriminalci. Ti namreč na njih lahko na sila preprost in hiter način pridobijo veliko uporabnih informacij za organiziranje in izvedbo raznovrstnih kriminalnih dejanj.

Spletni kriminalci so v zadnjih nekaj letih spoznali, da neposreden napad na tehnologijo ni več smiseln. Ta je namreč postala že tako izpopolnjena, da jo lahko računalničarji prelističijo le še z zelo specifičnimi in naprednimi znanji ter večletnimi izkušnjami. Zaradi tega spletni kriminalci veliko raje kot tehnologijo napadajo ljudi. Učinkovitost napada na ljudi oziroma spletna uporaba socialnega inženiringa za krajo zaupnih podatkov se je pred časom pokazala v primeru napada na podjetje RSA, ki proizvaja in trži varnostne sisteme. Tu so kriminalci napredne varnostne sisteme prelističili na način, da so dvema skupinama zaposlenim poslali sporočilo z zadevo Plan zaposlovanja 2011. V njem je bila pripeta okužena datoteka. Čeprav je varnostni sistem podjetja RSA pošto označil kot neželeno (SPAM), je enega izmed zaposlenih sporočilo vseeno za-



mikalo in je »sprožil« okuženo datoteko. Na ta način je spletni kriminalci dobil najvišje pravice na sistemu in iz njega odtujil zaupne podatke o sistemu za avtentikacijo SecurID. Čeprav je podjetje RSA sprva zatrdilo, da napad ni bil uspešen, je na koncu vseeno priznalo, da uporaba sistema SecurID zaradi napada ni več varna. Za odpravo škode je moralo podjetje odšteti na sto tisoče ameriških dolarjev.

Socialni inženiring za pridobitev neupravičenega dostopa do podatkov zaupne narave oziroma za izvedbo kriminalnih dejanj se uporablja že toliko časa, kolikor obstaja človek. Tu gre za prefinjene napade na človeka, kot so gledanje čez ramo (shoulder surfing), anketiranje (mail-outs), neposredni pristop (direct approach), pomembni uporabnik (important user), nemočen uporabnik (helpless user), osebje za tehnično pomoč (technical support), nasprotni socialni inženiring (reverse social engineering) in še bi lahko naštevali. Danes je že več kot 28 odstotkov spletnih napadov usmerjenih v zaposlene, pri čemer se delež letno povečuje za dobrih 16 odstotkov. Žal ti napadi niso le zelo učinkoviti in po večini uspešni, ampak jih je zelo težko odkriti in napadi pogosto ostanejo nekaznovani. Mogoče ste še vi pred kratkim bili žrtev socialnega inženi-

ringa, pa tega sploh niste prepoznali. To še posebno velja v primeru, ko spletni kriminalci za napad uporabljajo socialna omrežja. Samo na Facebooku je namreč več kot 750 milijonov potencialnih žrtev (od tega več kot 650 tisoč Slovencev), med katerimi je kar 20 odstotkov takih, ki z uporabniki delijo svoje geslo.

Edina učinkovita obramba pred socialnim inženiringom je izobraževanje. To velja tako za posameznike kot varnostne inženirje, informatike, tajnice in ostale zaposlene v podjetju. Spletni kriminalci za izvedbo kriminalnega dejanja namreč potrebuje informacije zgolj od ene osebe, in če vas je v podjetju zaposlenih 100, bo to izjemno lahka naloga za kriminalca, saj ima ta kar 96 odstotno možnost, da mu napad uspe.

Da bi se lahko učinkoviteje zoperstavili sodobni obliki spletnega kriminala in da ne bi prav vi postali žrtev socialnega inženiringa in podjetju ali sebi povzročili nepopravljivo škodo, smo v družbi S&T Slovenija, d. d., pripravili izobraževalni enodnevni tečaj z naslovom »Hekanje s pomočjo socialnih omrežij: Kako ga izvesti in prepoznati ter kako se mu izogniti«. Na seminarju bodo prikazane najpogostejše tehnike, ki jih kriminalci uporabljajo na področju socialnega inženiringa, praktični primer uporabe socialnih omrežij za pridobitev zaupnih podatkov, ki so potrebni za izvedbo vdora v informacijski sistem, ter načini, kako se lahko tem napadom učinkovito zoperstavimo. V svet hekanja s pomočjo družbenih omrežij vas bo popeljal Matej Saksida, priznan strokovnjak s področja varovanja informacij. (P.R.)

HEKANJE S POMOČJO SOCIALNIH OMREŽIJ: KAKO GA IZVESTI IN PREPOZNATI TER KAKO SE MU IZOGNITI

Termin 1: 2. september 2011

Termin 2: 21. november 2011

Kotizacija: 190 eur + DDV

Več informacij o tečaju in prijavi je na voljo na spletnem naslovu <http://goo.gl/WPEc8>.

Kontaktna oseba: Petra Militarev, vodja izobraževalnega centra

Za dodatne informacije nas lahko obiščete na sedežu podjetja na Leskoškovi cesti 6 v Ljubljani ali pa pokličete na telefon 01 585 56 91. Lahko nam tudi pišete na znanje@snt.si ali pa nas poiščite na spletu, na <http://znanje.snt.si>.



Consulting. Integration. Outsourcing.

S&T Slovenija d.d.
 Leskoškova cesta 6
 1000 Ljubljana
 Tel.: 01 585 52 00
 Faks: 01/585 52 02,
 spletni naslov: www.snt.si