Intervju

Varnost v e-bančništvu

..Z Mihom Culibergom, direktorjem poslovne enote mobilne finančne storitve podjetja Halcom, smo se pogovorili o varnostnih dilemah e-bančništva..

Kako varno je elektronsko bančništvo?

Tako kot to velja za druga področja, tudi pri elektronskem bančništvu popolne varnosti ni mogoče doseči – vedno je treba izbrati nek kompromis med stopnjo zaščite, ki jo določen mehanizem nudi, ter uporabnostjo tega zaščitnega mehanizma. Banke uporabljajo najrazličnejše načine varovanja svojih elektronskih bank – od relativno preprostih (uporabniško ime in geslo) do veliko bolj naprednih, kot so npr. digitalna potrdila na aktivno varovanih medijih. Lahko pa trdimo, da slovenske elektronske banke za pravne osebe z vidika varnosti ne zaostajajo za podobnimi rešitvami v tujini (saj uporabljajo zaščito PKI na aktivno varovanih medijih), elektronske banke za fizične osebe pa so primerljive z rešitvami v tujini, saj aktivno spremljajo razvoj varnostnih mehanizmov in postopkov.

Koliko primerov "odpovedi" elektronskega bančništva poznamo pri nas?

V Sloveniji obstaja varnostni center SI-CERT (Slovenian Computer Emergency Response Team), ki deluje v okviru Akademske in raziskovalne mreže Slovenije (ARNES). Center SI-CERT zbira podatke o mrežnih vdorih in varnostnih incidentih v Sloveniji, zato ta center najverjetneje upravlja z najpopolnejšim seznamom vseh prijavljenih vdorov in incidentov v Sloveniji. Mi teh podatkov nimamo.

Na kaj moramo biti pozorni pri elektronskem poslovanju?

Pri elektronskem poslovanju moramo biti pozorni na dejstvo, da so digitalna potrdila shranjena na disku računalnika, ki je skrbno varovan (požarni zid, antivirusni programi) in ki se ne uporablja za nameščanje nepreverjene programske opreme ali pregledovanje sumljivih spletnih strani. Tu bi bil lahko nasvet uporabnikom sledeč: če si to lahko privoščijo, naj uporabljajo en računalnik za zabavo in enega, ki ga skrbno vzdržujejo (redno posodobljena antivirusna oprema, požarni zid) za resno delo in dostopanje do zaupnih podatkov.

Zakaj so ljudje še vedno nezaupljivi glede elektronskega bančništva?

V medijih se v zadnjem času pojavlja kar nekaj člankov na to temo in praktično ne mine dan, da povprečen uporabnik interneta nekje ne bi zasledil namiga, da so posodobitve programske opreme in nameščena protivirusna zaščita in požarni zidovi ne samo priporočljivi, temveč praktično že obvezni za normalno življenje v elektronskem svetu. Do težav prihaja, ko zlikovci uporabijo največjo varnostno luknjo vsakega osebnega računalnika – psihologijo njihovega uporabnika. Večina modernih napadov na osebne računalnike zdaj izkorišča t. i. tehnike socialnega inženiringa, ko uporabnik bodisi zaradi svoje naivnosti, radovednosti ali pomanjkanja znanja naredi kaj, kar mu nato škodi. Pri tem je pomembno izobraževanje in ozaveščanje uporabnikov, ki pa je dolgotrajen proces, ki se ne more končati kar čez noč. Stopnja, ko katere se lahko nekdo izobrazi in izuči prepoznavati take napade, se razlikuje od posameznika do posameznika. In to ni posebnost elektronskega poslovanja – tudi v vsakdanjem življenju obstajajo ljudje, ki v stanovanje spustijo prijazne prodajalce najrazličnejše krame, nato pa jim iz denarnice izgine vsa gotovina.

V katero smer gre razvoj elektronskega bančništva?

Cilj razvoja varnostnih rešitev za področje e-bančništva je, da so varnostne tehnologije vedno en korak pred zlikovci. Seveda pa pri tem ne smemo pozabiti, da tehnološki napredek izboljšuje tudi varnostne mehanizme ali principe, ki se uporabljajo že danes – primer takega napredka je tehnologija WPKI (Wirless Public Key Infrastructure oziroma mobilni certifikat). S prenosom digitalnih potrdil in varnega elektronskega podpisa na pametno SIM kartico v mobilnem telefonu tako uporabnik dobi varno okolje za potrjevanje vstopa v elektronsko banko in potrjevanje plačil. S tem smo poleg varnosti, ki jo nudi PKI tehnologija, uspešno ločili napravo, ki je namenjena plačilu (PC), in napravo, ki je namenjena potrditvi plačila (mobilni telefon). Morebitni zlikovec bi tako moral prevzeti nadzor nad uporabnikovim osebnim računalnikom in pametno SIM kartico v telefonu hkrati, če bi želel brez uporabnikove vednosti prenesti denar na kak nepooblaščen račun. To pa je že nekaj, česar do sedaj še nismo imeli priložnosti videti. (P.R.)