Puudulik küberhügieen läheb kalliks maksma

Näpunäited turvaliseks autentimiseks

Digitaliseeritud ühiskonnas on isikute turvaline autentimine üha olulisem. Organisatsioonid peavad turvalisuse tagamiseks kasutusele võtma meetmeid, mis võimaldavad kasutajatel süsteeme võimalikult ohutult kasutada. Ammu enam ei saa piisavaks lugeda autentimise vahendit, mis sõltub üksnes kasutajatunnusest ja salasõnast. Küberründed ei tähenda filmidest tuntud „häkkimist“. Ründajatel on süsteemidesse sissepääsu saamine palju lihtsam, kasutades nõrkasid, varastatud või muul viisil ohtu seatud volitusi. Identiteedist on saanud küberrünnakute vastu võitlemisel uus turvalisuse väli.

Majandustegevuse halvamise kaudu püüavad kurjategijad ettevõtetelt välja pressida suuri summasid. Isegi, kui organisatsioon otsustab väljapressimisele mitte alluda ja loobub kompromiteeritud süsteemist, kaasneb sellega siiski ühel või teisel määral nii mainekahju kui ka varaline kahju.

Turvalisuse tagamiseks ja riskide maandamiseks on soovituslik kaaluda tõhusamate meetmete rakendamist. Üheks variandiks on kaheastmeline autentimine, mis, nagu nimigi viitab, eeldab kahe erineva autentimisviisi kasutamist. Kõige levinum on kasutajalt millegi teadmispõhise küsimine (näiteks salasõna) ja millegi (näiteks nutiseadme või ID-kaardi) omamise tuvastamine. ID-kaardiga isikutuvastamisel küsitakse kasutajalt PIN koodi ning tuvastatakse asjaolu, et kasutajal on tema isikuga seotud füüsiline kaart, mille ta on sisestanud kaardilugejasse. Nutiseadme kasutamisel kaheastmelise autentimise jaoks võidakse kasutajalt küsida salasõna ja saadetakse seadmesse teade, millele reageerides kasutaja tuvastatakse.

Salasõnad, mida kasutatakse, peaksid loomulikult olema võimalikult tugevad. Paraku, mõeldes kui palju kasutame erinevaid teenuseid, millele ligipääsuks on tarvis meeles pidada mingisugust salasõna, pole ilmselt imestada, et paljud lõpuks lihtsama vastupanu teed lähevad ja ühte lihtsat parooli mitme teenusepakkuja juures kasutavad. Tugevat salasõna on tahes-tahtmata keeruline meeles pidada.

Lisaks eeltoodule on siiski ka rida teenuseid, mida ei ole võimalik autentida teisiti kui läbi salasõna. Kõige tuntuma näitena saab esile tuua *wallet*-teenuseid, millele ligipääs on takistatud, kui kasutajal läheb parool meelest või keegi kolmas vahetab parooli ära.

Salajase võtme hoiustamise teenus

Tekib küsimus, mis juhtub, kui salasõna mis tahes põhjusel kaotsi läheb. Kujutame ette olukorda, kus manalateele läinud isiku pärandvara on suures osas hoiustatud virtuaalses rahakotis, mille salasõna pärijatel ei ole. Sellisel juhul jääbki vara igaveseks ajaks küberruumi hõljuma.

Tasuks kaaluda võimalust kõige olulisemate salasõnade ja salajaste võtmete hoiustamiseks, et need ei kaoks ka siis, kui meie endiga midagi juhtub. Paraku on keeruline leida turvalist ja usaldusväärset teenust, mis tundlike salasõnade kaotsimineku riski maandaks. Üheks võimalikuks variandiks võiks siinkohal olla nii-öelda paroolihaldamisteenuste kasutamine, mis aga ei pruugi kõigile andmeturvalisuse osas täiesti meelepärased olla. Õhku jääb ka küsimus sellest, mis juhtub, kui kaotsi läheb salasõna, mis paroolihaldurile endale juurdepääsu tagab.

Ehk oleks tulevikus ruumi mõnele tsentraalsele lahendusele tundlike andmete hoiustamiseks. Variandiks võiks olla teatud mõttes analoog notarile hoiule antud testamendiga, mis tähendab, et kõige olulisemad salasõnad jäetakse kindlasse kohta. Samas tuleb arvestada, et salasõnasid on aeg-ajalt vaja muuta. Seda näiteks andmelekke või üldise küberhügieeni pärast. Seetõttu võib notariaalne teenus osutuda liigselt ebamugavaks ja kulukaks.

Kaalumist vääriks Eesti ID-kaardi infrastruktuuri kasutamine uue teenuse loomiseks, mis võimaldaks tundlikke salasõnasid ja salajasi võtmeid turvaliselt hoiustada, aga vajadusel ka jagada. Seda kõike viisil, mis oleks piisavalt lihtne, kiire ja dünaamiline, arvestades digitaalsete vahendite omapäraga, turvalisuses grammigi järeleandmata.

HENRIK LINK
VANDEADVOKAAT

(+372) 66 76 440
HENRIK.LINK@NJORDLAW.EE

LIISI JÜRGEN
VANDEADVOKAAT, PARTNER

(+372) 66 76 440
LIISI.JURGEN@NJORDLAW.EE