Online finantsteenuste turvariskid ja kuidas ettevõtted nendega toime tulevad

12. aprill 2019 - 13:34 Autor: AM

Hinnanguliselt 40-50% kõikidest pangaülekannetest tehakse täna interneti vahendusel, 30% nendest tehakse nutitelefoniga. Need arvud on tõusutrendis ja tõenäoliselt tehakse mõne aasta pärast juba üle poolte pangaülekannete internetis ning eelistatakse aina mugavamaid lahendusi. Suurenenud maht eeldab ka paremaid turvameetmeid, sest tehingute arvu suurenedes suureneb ka turvaaukude hulk. Et maandada võimalikku riski, tuleb tarkvara teravana hoida.

Peamised turvariskid

Hetkel moodustavad sularahaautomaatidega tehtud tehingud vaid ligi 5% kõikidest tehingutest. Tähendab, et raha liigutamine ja vahendamine koondub online keskkonda. Ühiskond soovib aina enam oma rahaasju isiklike seadmete abil joonde ajada. Nad ei taha, või pole neil aega, et traditsiooniliselt pangakontorisse pöörduda. Pealegi, kellele ikka paberitükk näpus oma numbrit oodata meeldib. See on arusaadav, et kiire elutempoga maailmas inimesed oma aega väärtustavad. Paraku, eeldab sellise kliendipoolse usalduse olemasolu ettevõttelt ka teatud turvastandardite tagamist. Tarbija tahab olla kindel, et tema tehingud on kontrollitud. Mõned võimalikud ohud internetis raha liigutamise juures on näiteks parooli lekked, andmevargus, identiteedi vargus jne. Peamiselt seotud tarbija enda vigadega, kuid ka etetvõtte tulemüüride ja andmete kodeerimsie võimekusega.

Ebamugavusena saab kindlasti välja tuua sõltuvuse internetiühendusest ja elektrivõrgustikust. Kui üks nendest kahest üles ütleb, siis kogu süsteem lakkab töötamast. Mõlemad võrgustikud on küll võrdlemisi vastupidavad, kuid aeg-ajalt tuleb ikka ette, et loodus soovib sekkua.

Online finantsteenuste eelised

Lisaks kiiretele toimingutele ja praktiliselt olematule ooteajale, pakuvad interneti vahendusel toimivad finantsteenused reeglina 24/7 kliendituge ja lisamugavusi. Tarbija ei pea dokumendid näpus esinduskontorisse tormama, 10 enne viit ja heas usus, et esindus pole enneaegselt sulgenud. Ta saab peale tööd julgelt koju minna (vajadusel isegi toidupoest läbi astuda) ja oma toimingud endale sobival ajal korda saata. Samad dokumendid on andmebaasides olemas ja ühtegi paberilehte ei tule tindiga määrida. Raha saab ka sekundiga üle kanda. Oleks sellist stsenaariumit 30 aastat tagasi kellelegi selgitanud, oleks ta küsinud, et kus ta nii head ulmekirjanudst lugeda saaks? Ilmselt siiski mitte, kuid üsna uskumatu areng on see siiski.

Näiteks Soomes on praegu võimalik ettevõtetel ja eraisikutel fintech valdkonnas tegutsevatelt eraettevõtetelt nutitelefoni appi apil kiirelt, soodsalt ja turvaliselt finantseeringut saada. Kusjuures, nad kasutavad samasid turvameetmeid, mida kasutavad rahvusvahelised pangad. Selline võimalus viib kontrolli üksikutelt asutustelt paljudele väiksematele asutustele ja annab tarbijale võimaluse oma laenutingimused ise paika seada, suurendades raha vaba liikumist ja maandades riske. Tulevatel aastatel on ilmselt selline mudel ka Eestisse jõudmas.

Mõned näited turvasüsteemidest

Üks kindlamaid praeguse aja turvameetmeid on mitmetasandiline tuvastamine. See tähendab, et kui tarbija oma kasutajaga sisse tahab logida, tuleb tal näiteks telefonile saadetud kood sisestada. Kui häkker tahaks kasutajat varastada, tuleks tal ka tarbija telefon varastada. See teeb kasutajale sissemurdmise ebatõenäolisemaks. Loomulikult ei tähenda, et tarbija võiks muretult parooliks numbriloendi või oma koera nime panna ja asja ära unustada. Parool peab vastama vähemalt mingile standardile ning paroole tuleb ka aeg-ajalt muuta.

Wi-fi ja interneti ühenduse teenuste kasutamisel tuleb jälgida, millises võrgus oma isiklike andmetega teenuseid kasutatakse, sest iga tegevus jätab n-ö jalajälje ning tarbija liikumist on võimalik võrgu andmetest selgelt vaadelda. Osav häkker võib käigu pealt andmed varastada, sest need saadetakse läbi avaliku võrgu (kuhu on ka teised ühendatud).

Tulemüürid ja andmete kodeerimine. Ettevõtted peavad oma andmeid kaitsma. Üks asi on varastada tarbija enda kaudu tema andmed, teine on varastada ettevõtte andmebaasidest mitme tarbija andmed korraga. Selle ärahoidmiseks kasutavad ettevõtted tugevaid tulemüüre, et häkkerid ei pääseks andmebaasidele ligi ning nad kodeerivad oma andmed ära, et kui mingil põhjusel häkker peaks tulemüürist läbi saama, siis ei saa ta andmeid niisama lihtsalt lugeda.

Kõrgetasemelised turvameetmed ei ole enam suurte pankade luksus, vaid pigem finantsteenustega tegelevate ettevõtete standard. Endale parima teenusepakkuja valimisel tuleb ettevõtte turvameetmete taset samuti jälgida, et oleks süda rahul ja isiklik info kaitstud.

- Uudised