

# Tagavarakoopiate puudumine – risk või mitte?

Inimesed tajuvad riske erinevalt. Ühele on andmete tagavarakoopiate puudumine suur risk, teise jaoks pole see mingi probleem.

## Erkki Leego

Hansson, Leego ja Partneri juhatuse esimees

Teadmatust võib tagada hetkel rahulikuma une, aga seda rahutum võib elu olla pärast turvaintsidenti. Mure turvalisuse üle tõuseb hüppeliselt mõne intsidenti toimumise järel. Näiteks on tavapärase, et pärast arvuti varastamist kontoritist paigaldatakse paremad lukud, vaadatakse üle valvesüsteem ning sõlmitakse kindlustusleping. Samas on ka neid, kes arvavad piltlikult öeldes, et ega väik kaks korda ühte kohta sisse löö.

Ohte on meie ümber palju – alates maavärinast ja elektrikatkestusest andmete varguseni. Oht üksi ei tähenda, et ettevõttele on tekkinud kahju. Oht peab ära kasutama süsteemi kaitse nõrkust. Nõrk kaitse on näiteks vilets ukسلukk, mis varast pikalt kinni ei pea. Ohuks selles näites on vargus läbi sisse-murdmise.

Oht koos nõrkusega määrab ära riski kahju tekkimiseks. Kui süsteem on paremini kaitstud, on sama ohu korral risk väiksem. Kui uks ja ukسلukk on tasemel, ei saa varas sealtkaudu sisse ning kahju tekkimise tõenäosus ehk risk on selle ettevõtte jaoks väiksem. Hoone kokkuvarisemise risk on seda väiksem, mida tugevam on hoone konstruktsioon.

Varguse riski vähendamiseks saab paigaldada paremad lukud, kolida uude kontoris, paigutada olulised andmed seifi vms.

Ohud võivad pärineda looduslikust, tehnoloogilisest või inimallikast ning olla juhuslikud või sihilikud. Keskkonnaohud on näiteks äike, üleujutus ja kahjutuli, tehnoloogiaohud seadme rike ja toru purunemine, inimohud pealtkuulamine, vargus ning vead ja hooletus. Neist pealtkuulamine ja vargus on sihilikud, vead ja hooletus juhuslikud ohud.

Ohtude nimekiri on kõikide ettevõtete jaoks sama. Organisatsioonist, riigist ja kultuurist tulenevalt on erinev ohtude realiseerumise tõenäosus. Näiteks varguse toimumise tõenäosus on Eestis mõnest teisest riigist kindlasti suurem. Pikk elektrikatkestus on metsatalus tõenäolisem kui moodsas haiglas. Ükski ohtude loetelu ei saa olla ammendav.

Oluline etapp andmeturbe parandamisel on ohtude hindamine. Ohtude realiseerumise tõenäosuse alusel saab valida endale sobilikud (ka kulu mõttes) turvameetmed. Teades oma andmeturbe riske, saame kulutada kaitsemeetmetele just niipalju, kui meie andmed on väärt, unustamata sealjuures ära mõnda olulist nõrkust kaitses.

Näiteks ei ole meil mõtet kulutada palju raha turvafirma peale, kui kõik väärtuslik on ruumist võimalik ära viia kahe minuti jooksul. Kui maavärinat Eestis ei esine, pole vajadust maavärinakindlate seinte järele. Samas on kindlaid seinu vaja, et olla kaitstud pommiplahvatuse eest.

## Oht realiseerub vaid tänu nõrkusele

Ohtude hindamise juures tuleb pidada eraldi arvestust nõrkuste kohta. Kuna ohud saavad realiseeruda ainult siis, kui esineb nõrkus kait-

## Millised ohud ähvardavad minu ettevõtet?

■ Ohtude ja nõrkuste hindamise järel jõutakse tavaliselt väga lühikese nimekirjaga tõsiste ohtude juurde. Teiste ohtude realiseerumise tõenäosus on nii madal, et nendega ei ole otstarbekas tegeleda. Näiteks ei ole Eesti ettevõtetel maavärina ohuga suurt midagi peale hakata. Kõige tavalisemad ohud on vead ja tegemata jätmised, vargus ja pettus, tulekahju, majandusluure, kuritahtlik häkkimine, arvutiviirused.

Ohtude ja nõrkuste hindamise järel tuleb leida õiged meetmed nõrkuste vähendamiseks ning saavutada piisava turvalisuse tase. Kuidas riskianalüüsi oma ettevõttes mõnustasti läbi viia, sellest järgmises ITee numbris.

Erkki Leego

ses, peame teadma, kus on meie nõrgad kohad. Samuti tuleb hinnata, kui tõenäoliselt saab üks oht kasutada ära nõrka kohta.

## Halb elektrivõrk tähendab saamata tulu

Näiteks oht “elektritoite katkemine” kasutab ära nõrkust “ebastabiilne elektrivõrk” ja põhjustab kahju “töö katkemisest saamata jäänud tulu”. Mida ebastabiilsem on elektrivõrk, seda suurem on tõenäosus, et elektri kadumine põhjustab meile majanduslikku kahju.

Toon siinkohal mõned näited tavalistest nõrkustest valdkondade kaupa:

■ keskkond ja infrastruktuur – hoonete, uste ja akende füüsilise turbe puudumine (seda võib ära kasutada näiteks varguseohu);

■ riistvara – tundlikkus pinge kõikumiste suhtes (seda võib ära kasutada näiteks äikeseohu);

■ tarkvara – pääsuõiguste väär jaotamine (seda võib ära kasutada näiteks tarkvara volitamatu viisil kasutamise oht);

■ side – kaitsmata sideliinid (seda võib ära kasutada näiteks pealtkuulamise oht);

■ dokumendid – hooletus kõrvaldamisel (seda võib ära kasutada näiteks varguse oht);

■ personal – puudulikud tölevõtmise protseduurid (seda võib ära kasutada näiteks sihiliku kahjustamise oht).

Äri toimimist ähvardab palju ohte. Pole mõistlik suhtuda ohtudesse liiga üleolevalt ega ka liialt paranoiliselt. Kaine meelega riskide hindamine võimaldab paremini planeerida oma kaitsekulutusi ning maandada riske. Turvalisuse arendamine ei ole ainult ekspertide pärusmaa. Võtke üks tunnike ja mõelge ohtude ning nõrkuste teemal. Ehk avastate, et olete intuiitiivselt oma riskid juba suurepäraselt maandanud. Kui ei, võtke midagi ette. □

vaata ka  
Firma andmeid tuleb kaitsta terviklikult, Erkki Leego, ITee, august 2005

Efektive andmekaitse algab suhtumisest, Erkki Leego, ITee, september 2005

Andmeturbe nõuab kindlat vastutajat, Erkki Leego, ITee, oktoober 2005.