eBCM Assurance: **INFORMATSIOONI TURVALISUS, KÜBER-IDENTITEET JA USALDUSVÄÄRSUS**

LEARNING OBJECT #08

# Turvalisus

Usaldusväärsuse alus e-äris

## Sisukord



## Sissejuhatus

Äripartnerite vahel usaldust luues tuleb arvestada väga paljude erinevate teemadega, mis mõjutavad ettevõtte reputatsiooni. Siin tuleb silmas pidada kõike, mis on tajutav ja mõeldav usaldusväärsuse all, nii traditsioonilises äris kui ka võrgu keskkonnas. Võimalike ohtude mõistmine ja IKT turvalisust tagavate vahendite tundmine on stabiilse e-äri keskkonna tagamiseks oluline. Alljärgnevalt anname ülevaate IKT varade väärtusest ja üldlevinud IKT turvalisuse teemadest.

E-äri on oma olemuselt tavapäraste äriprotsesside rakendamine IKT vahendite ja interneti teenuste abil (nt kaupade ost-müük interneti vahendusel). E-äri puhul toimivad kõik äritehingud internetis ja veebikeskkonnas. Kõik äri teenused peavad olema ühendatud ja interneti vahendusel kasutajaile kättesaadavad. Hea kvaliteedi seisukohast on oluline kättesaadavus, lihtsus ja selgus juhtimisel. Analüüsides äriprotsesse on soovitav dokumenteerida kõik tööprotseduurid ja tegevused, et neid oleks hiljem võimalik kontrollida. Absoluutselt kõik äriprotsessid on võimalik üle kanda interneti-põhisesse keskkonda: kommunikatsioon ja foorumid, e-mail, hindamised, ladu, ostud, dokumendihaldus, projekti juhtimine, programmi juhtimine jne.

### Turvalisuse väärtus

**IKT vahendid peavad võimaldama andmetele juurdepääsu, kättesaadavuse, kontrolli ja turvalisuse. Vigade vältimiseks ja andmete uuendamiseks tuleb andmeid perioodiliselt sünkroniseerida. IKT turvalisuse tagamiseks ettevõttes tuleb välja töötada ühtne IKT turvapoliitika kogu organisatsiooni jaoks. IKT turvapoliitika on dokumentatsioon, mis kirjeldab infovarade juhtimist, haldust ja kaitset organisatsioonis. Infovarade alla kuuluvad:**

- Andmed (informatsioon, teadmus...erinevas vääringus ja vormis)
- IKT seadmed: arvutid, riistvara jne füüsilised seadmed ja vahendid
- Telekommunikatsiooni kanalid ja võrgud
- Tarkvara (IT süsteemid, programmid)

### IKT rakendamine ja kasutuselevõtt

IKT turvapoliitika rakendamine nõuab süstemaatilisi tegevusi kogu organisatsioonis tervikuna. See eeldab erinevatel tasanditel juhtide ja spetsialistide koostööd: kaasata tuleb IT juhid, spetsialistid, ärijuhid, finantsjuhid jne.

Süsteemi turvalisuse tagamisel on väga tähtis sobiva IT lahenduse valik (kuna e-äri põhineb alati mingisugusel infosüsteemil). IT lahendust valides tuleb hoolikalt kaaluda ja esitada endale järgnevad küsimused:

- Missugune lahendus on parim spetsiaalselt meie ettevõttele?
- Kas süsteemi arendamine jätkub ka tulevikus, on seal arenguruumi?
- Kui palju maksavad kõik ressursid (riistvara, tarkvara, rakendus, integreerimine, koolitused jne)?
- Kas uus e-äri süsteem on integreeritav juba olemasoleva tarkvara ja süsteemidega (erinevad tarkvara platvormid: ladu, müük, raamatupidamine jne)?
- Missugused on täiendavad nõudmised ja vajadused autoriseerimisele, krüpteerimisele, andmete turvalisusele?
- Infosüsteemi modelleerimine ja loomine: kas mõeldi läbi kõik turvalisuse aspektid?

## Infovarade väärtus ettevõtte jaoks

Enamasti me teame, et igas süsteemis võivad ilmneda vead. Me saame süsteemi taas-käivitada, probleemiga töötada ja isegi mõneks ajaks süsteemi töö katkestada. Kahjuks need valikud ei ole alati võimalikud järgnevatel juhtudel:

- Katkestus põhjustab suurt majanduslikku kahju;
- Katkestus või viga ohustab inimelusid;
- Infosüsteemi toimimine funktsioonidele mitte vastavalt on sotsiaalselt vastutustundetu.

Antud tüüpi süsteemile on iseloomulik, et süsteemi missioon on ise on põhjus, miks see süsteem loodi. Seega süsteemi ebaõnnestumine ei ole aktsepteeritav. Sellised süsteemid on missioonikriitilised. Süsteemi väärtus on võimalik välja selgitada, vastates järgnevatele küsimustele:

- Mis juhtub, kui süsteem ei tööta korrektselt 1 minut/ 1 tund/ 1 päev/ 1 nädal (küsimus on selles, kui kiiresti saab süsteemi tööle, kui midagi tõsist juhtub)?
- Mis juhtub, kui süsteemid andmed kaovad?
- Mis juhtub, kui süsteemi andmed saavad avalikult kättesaadavaks?

Kui organisatsioon saab süsteemi tõrgete korral äritegevust jätkata, siis antud süsteem ei ole missiooni-kriitiline. Ka süsteemi kiirus ja täpsus on tähtsad ja olulised otsuste tegemisel.

## IKT turvalisus ja konfidentsiaalsus

Tõhusad ärisuhted põhinevad äripartnerite vahelisel usaldusel, kus informatsiooni turvalisus on üks võtme-elemente. See kehtib igat liiki ettevõtete, eriti aga e-äride kohta. Konfidentsiaalsus on elementaarne, näiteks igaüks tohi juurde pääseda e-arvetele, hinnakirjadele jne.

Andmete terviklikkus on üks olulisemaid teemasid e-äri turvalisuses. Terviklikkus tähendab IKT turvalisuse seisukohast seda, et andmeid ei ole volitamata muudetud või kustutatud, neil pääsevad ligi vaid selleks volitatud isikud. Selleks on nõutav autoriseerimine jms vahendid.

Adekvaatsed andmed peavad olema alati kasutamiseks valmis. Andmete kättesaadavus sõltub süsteemi töö stabiilsusest, süsteemi operatsioonidele kuluvast ajast ja võimalusest saata elektroonilisi sõnumeid. Ettevõtte või süsteemi usaldusväärsuse tunnuseks on sõnumi kättesaamise kinnituse küsimine ja märku andmine, et sõnum on kohale jõudnud.

## Peamised ohud IKT turvalisusele

Küber-kuritegude näol on tegemist kuritegudega, mis pannakse toime arvutite abil või arvutivõrkudes (nagu nt arvutitesse sisse häkkimine) ja ka tavapäraste kuritegude võimaldamine läbi arvutikasutuse või arvutivõrgu (nagu nt alaealiste pornograafilised leheküljed, identiteedivargused, krediitkaardiarvete vargused jne). Küberkuritegudeks loetakse ka arvutikasutus kriminaalsetel eesmärkidel, nt andmete saamiseks. Kuigi need tegevused ei pruugi iseenesest olla keelatud, muutuvad need kriminaalseks siis, kui saadud informatsiooni vastavalt ära kasutatakse. Arvutitehnoloogia areng on loonud palju uusi väljakutseid sotsiaalpoliitikas, sellistel teemadel nagu privaatsus ja andmekaevandamine jms.

Identiteedivargus ja identiteedipettus on terminid, mida kasutatakse viidates kuriteole, mis on toime pandud kasutades kellegi teise isikuandmeid, tavapäraselt majandusliku kasu saamise eesmärgil.

Häkkimine (sissetung) on omavoliline arvutikasutus, püüdes infosüsteemi või võrgu turvalisuse mehhanismidest kõrvale hiilida. Häkkimine võib ohustada arvutisüsteemi, kuna see annab sissetungijale täieliku kontrolli süsteemi üle, kust ta saab varastada salajasi andmeid, kahjustada või hävitada süsteemi vms.

*Key-logger* (klaviatuurivajutuste salvestaja) on seade, mis monitoorib igat kasutaja klaviatuurivajutust arvutil. Riistvaraline *key-logger* on väike patareisuurune seade, mis paigaldatakse klaviatuuri ja arvuti vahele. Kuna seade sarnaneb tavalisele klaviatuuri pistikule, on suhteliselt kerge seda paigaldada ja kasutaja käitumist jälgida. Seade salvestab iga kasutaja poolt tehtava klahvivajutuse oma miniatuursele andmekandjale. Hiljem võib seadme paigaldaja sel viisil kogutud informatsioonile ligi pääseda. Tarkvaraline *key-logger* ei nõua ka otseselt füüsilist juurdepääsu kasutaja arvutile, jälgimiseks saab internetist alla laadida nuhkvara ja panna see toimima nn Trooja hobusena. *Key-logger* programm salvestab iga kasutaja klahvivajutuse ja uuendab informatsiooni perioodiliselt üle interneti, kus iganes see programm on installeeritud.

Ohud kommunikatsioonivahendite kasutamisel - MSN, Skype jt programmid – peamine soovitus on mitte käivitada kahtlasi faile, mis kasutajale saadetakse.

Ohud veebilehitseja kasutamisel: nuhkvara, “küpsised”[1] jne – peamine soovitus on seadistada oma veebilehitseja nii, et “küpsised” ei oleks lubatud.

## Võimalikud ründekanalid

Ründamiseks on erinevad kanalid ja neid peaks turvama erinevate vahendite ja võimalustega.

- Wi-Fi - Wi-Fi on juhtmevaba arvutivõrgu tehnoloogia. Wi-Fi i rakendusi kasutatakse internetti pöördumiseks ja IP telefonikõnede tegemiseks, aga ka mängudeks jms.[2]
- VPN - virtuaalne privaatvõrk (*virtual private network*) tehakse tunnelina läbi avaliku võrgu (interneti). VPN tagab kasutaja autentsuse ja krüpteerib edastatavad andmed. VPN on privaatvõrk, mis kasutab avalikku telekommunikatsiooni infrastruktuuri, säilitades samal ajal privaatsuse ja turvalisuse. Turvalisuse tagamiseks kasutatakse tunneldamist[3] ja vastavaid turvaprotseduure.
- WLAN - wireless LAN or WLAN on traadita kohtvõrk või raadiokohtvõrk, mis ühendab kaks või enam arvutit omavahel juhtmeid kasutamata. Selline kohtvõrk, kus ringi liikuv (mobiilne) kasutaja saab kohtvõrguga ühendust pidada raadiokanali (traadita ühenduse) kaudu.
- Bluetooth - Bluetooth on mobiilside võrkude spetsifikatsioon. See kirjeldab, kuidas mobiiltelefonid, sülearvutid ja elektronmärkmikud (PDA) saavad lihtsal viisil andmeid vahetada nii omavahel kui ka kodu- või töötelefonide ja arvutitega lühikese vahemaa pealt. Bluetooth võimaldab mobiiltelefonide, ja pihuarvutite või elektronmärkmike kasutajatel endale hankida kõiki kolme funktsiooni ühendava mobiiltelefoni. Et taoline mobiiltelefon saaks suhelda arvuti, printeri, faksiaparaadi, lauatelefoni vms seadmega, tuleb kõigisse neisse seadmetesse monteerida vastav mikroskeem.
- Muud (sh töötajad).

## IKT turvalisuse tagamise vahendid

Võimalikud vahendid IKT turvalisus tagamiseks ja rünnete ära hoidmiseks on kasutada järgnevaid lahendusi:

- Antiviiruse tarkvara – paigaldada arvutisse ja uuendada regulaarselt;

[1] Cookie – küpsis – Internetis tähendab see sõna väikest andmeplokki (tekstifaili), mille veebiserver saadab teie veebibrauserile ja mis salvestatakse teie arvuti kõvakettale. Edaspidi iga kord, kui brauser pöördub uuesti sama veebisaidi poole, saadab ta sinna ka küpsise. Sõltuvalt küpsise tüübist ja brauseri seadetest võib brauser küpsise vastu võtta või sellest keelduda. Kasutaja saab ka ära määrata, kui kaua küpsis kõvakettal säilitatakse. Vt lähemalt http://www.vallaste.ee/

[2] Wireless - Terminit "traadita side" kasutatakse telekommunikatsioonisüsteemide kohta, kus signaalikandjaks on mitte traatjuhtmed nagu tavalistes telefonivõrkudes, vaid elektromagnetlained (raadio- või infrapunalained). Mõnikord kasutatakse traadita ühenduse tarvis ka helilaineid (näit. hoonete valvesüsteemides). Vt lähemalt http://www.vallaste.ee/

[3] tunneldamine - Meetod ühe võrgu andmete edastamiseks läbi teise võrgu. Selle meetodi puhul sisaldavad võõras võrgus edastatavad andmepaketid lisaks andmetele ka oma võrguprotokolli. Näiteks Microsofti PPTP meetod võimaldab kasutada Internetti andmete edastamiseks virtuaalses privaatvõrgus (VPN). Selleks manustatakse oma privaatne võrguprotokoll Interneti kaudu edastatavatesse TCP/IP pakettidesse. Vt lähemalt http://www.vallaste.ee/

- Tulemüür;
- Rämpsposti filter;
- Elektroonilised isikutunnistused/ sertifikaadid;
- Krüpteeritud autentimine;
- Digitaalallkiri ja ID tuvastus;
- Internetis liikudes hoidu nuhkvara eest.

## Kuidas käituda turvaliselt

Organisatsioonis tuleb välja töötada IKT turvapoliitika ja soovitav on määratleda peamised eesmärgid infovarade kasutamisel. IKT turvapoliitika peab kaasama infopoliitika ja ettevõtte äripoliitika. Soovitav on defineerida meetodid, kuidas turvariskid lahendatakse erinevatel juhtudel, sh ka riskianalüüs. Tähtis osa IKT turvapoliitikas on iga töötaja vastutusel. IKT turvapoliitika peab katma järgnevad valdkonnad:

- Riistvara ja tarkvara turvalisus peab kaasama:
  - Kasutaja tuvastamine ja õigsuse kontroll;
  - Juurdepääsu tagamine;
  - Kustutamised, ründetarkvara (informatsiooni muutmine);
  - Arvutite turvalisus (lauaarvutid ja sülearvutid).

- Andmeside turvalisus peab kaasama:
  - Võrkude infrastruktuuri kontroll ja tagamine;
  - Side krüpteerimine;
  - Soovitav on mõningatel juhtudel veebiserveri teenused sisse osta (veebilehe majutus).

- Füüsiline turve peab kaasama:
  - Hoone ja teenuste turvalisuse;
  - Juurdepääsu arvutitele ja andmekandjatele (andmebaasid, infosüsteemid).
  - Ohtude avastamine ja nendest teavitamine reguleerida;
  - Seadmete kaitse (vargused).
  - Teenuste ja hoolduste reguleerimine.

- Dokumentide ja andmekandjate turvalisus peab kaasama (infokandjad igasuguses formaadis):
  - Andmete säilitamine;
  - Andmete edastamine;
  - Andmete kustutamine.

**E-äri turvalisuseks on soovitav sisse seada kindlad reeglid:**

- Loo alati varukoopiad;
- Mõtle läbi nn eriolukordade strateegiad, levinuimad turvaintsidendid (rünnak, andmeleke jne);
- Tööta välja juhised ja IKT turvapoliitika dokumentatsioon;
- Töötajate teadlikkuse tõstmiseks korralda regulaarselt turvalisuse ja IT koolitusi;
- Tuleta meelde e-maili kasutamise turvareegleid – mitte avada kahtlasi manuseid ja faile. Ära avalda oma e-maili aadressi avalikult veebis;
- Kasuta salasõnu ja hoia neid turvaliselt (juurdepääsuks võrku ja e-äri süsteemidesse);
- Töö lõpetades logi alati arvutist välja (kasutaja identifitseerimine);
- Kustuta andmeid turvaliselt (faili saatmine arvuti prügikasti ei kustuta seda ja andmed on taastatavad).