Infoturve

http://www.ria.ee/iske

Anne-Mari Vunder
Üldosakonna juhataja
Tallinna Linnakantselei
16.02.2011

Üldist

- **Informatsioon** - teave, teadmus mis puudutab objekte (näiteks fakte, sündmusi, asju, protsesse või ideid, sealhulgas mõisteid) ja millel on teatavas kontekstis eritähendus;
- **Andmed** - teabe taastõlgendatav esitus formaliseeritud kujul, mis sobib edastuseks, tõlgenduseks või töötluseks; andmetel iseenesest ei ole mingit tähendust, teabe saamiseks tuleb andmeid tõlgendada kontekstis, nii et nad saaksid tähenduse;
- **Infosüsteem** - andmeid töötlev, salvestav või edastav tehniline süsteem koos tema normaalseks talitluseks vajalike vahendite, ressursside ja protsessidega; ;
- **Andmekogu** - infosüsteemis töödeldavate korrastatud andmete kogum;
- **Vahendid** – infrastruktuur (näiteks hooned, ruumid, kaablid, võrguühendus), arvutid (näiteks lauaarvutid, sülearvutid, pihuarvutid), lisaseadmed (näiteks printerid, faksid), andmekandjad (näiteks serverid, mälupulgad, CD-d, DVD-d, poolpüsimälu) jms.
- **Infovara** – teadmus või andmed, millel on organisatsiooni jaoks väärtus, või nendega seotud infotöötlusvahend; võivad kuuluda organisatsioonile või olla organisatsioonis vastutaval hoiul (näiteks isikuandmed);

Infoturve

- **Teabe turvalisus** - teabe väärtuste ja omaduste tagamine;
- **Infoturve** – riskihalduslik tegevus teabe turvalisuse säilitamiseks vastavalt organisatsiooni tegevuse eesmärkidele, sh andmekaitse realiseerimise vahend;
- **Infosüsteemide kolmeastmeline etalonturve** (ISKE) − infoturbe metoodika, mida rakendatakse andmekogudele ja mis sisaldab juhised, kuidas korraldada infoturbe haldust, määrata infovarade turbevajadust ning turvameetmete kataloogi.

Infoturbe eesmärk

- Teabe kaitsmine ohtude eest;
- Talituse jätkuvuse tagamine;
- Talitusriski minimeerimine;
- Investeeringute tasuvuse maksimeerimine;
- Õigusaktidele vastavuse tagamine;
- Kuvandi säilitamine.

Teabe turvalisuse põhikomponendid

- **Käideldavus** - (availability) – andmete kättesaadavus ja kasutatavus, nende käepärast olek, kehtivus; K0,1,2,3
- **Terviklus** - (integrity) – veendumus andmete õigsuses, nende puutumatus, terviklus, täielikkus; T0,1,2,3
- **Konfidentsiaalsus** (*confidentiality*) – teabe omadus olla kättesaamatu volitamata isikutele või protsessidele. S0,1,2,3

Turvaosaklassid

- Andmete käideldavuse alusel määratakse turvaosaklass järgmisest skaalast:
- K0 – töökindlus – pole oluline; jõudlus – pole oluline;
- K1 – töökindlus – 90% (lubatud summaarne seisak nädalas ~ ööpäev); lubatav nõutava reaktsiooniaja kasv tippkoormusel – tunnid (1÷10);
- K2 – töökindlus – 99% (lubatud summaarne seisak nädalas ~ 2 tundi); lubatav nõutava reaktsiooniaja kasv tippkoormusel – minutid (1÷10);
- K3 – töökindlus – 99,9% (lubatud summaarne seisak nädalas ~ 10 minutit); lubatav nõutava reaktsiooniaja kasv tippkoormusel – sekundid (1÷10).
- Andmete tervikluse alusel määratakse turvaosaklass järgmisest skaalast:
- T0 – info allikas, muutmise ega hävitamise tuvastatavus ei ole olulised; info õigsuse, täielikkuse ja ajakohasuse kontroll pole vajalik;
- T1 – info allikas, selle muutmise ja hävitamise fakt peavad olema tuvastatavad; info õigsuse, täielikkuse ja ajakohasuse kontroll erijuhtudel ja vastavalt vajadusele;
- T2 – info allikas, selle muutmise ja hävitamise fakt peavad olema tuvastatavad; vajalik on info õigsuse, täielikkuse ja ajakohasuse perioodiline kontroll;
- T3 – info allikas, selle muutmise ja hävitamise faktil peab olema tõestusväärtus; vajalik on info õigsuse, täielikkuse ja ajakohasuse kontroll reaalajas.
- Andmete konfidentsiaalsuse alusel määratakse turvaosaklass järgmisest skaalast:
- S0 – avalik info: juurdepääsu teabele ei piirata (st lugemisõigus on kõigil huvitatutel, muutmise õigus on määratud tervikluse nõuetega);
- S1 – info asutusesiseseks kasutamiseks: juurdepääs teabele on lubatav juurdepääsu taotleva isiku õigustatud huvi korral;
- S2 – salajane info: info kasutamine on lubatud ainult teatud kindlatele kasutajate gruppidele, juurdepääs teabele on lubatav juurdepääsu taotleva isiku õigustatud huvi korral;
- S3 – ülisalajane info: info kasutamine on lubatud ainult teatud kindlatele kasutajatele, juurdepääs teabele on lubatav juurdepääsu taotleva isiku õigustatud huvi korral.

Mõisted riskide hindamisel

- **Infovara** – teadmus või andmed, millel on organisatsiooni jaoks väärtus, või nendega seotud infotöötlusvahend; võivad kuuluda organisatsioonile või olla organisatsioonis vastutaval hoiul (näiteks isikuandmed);
- **Oht** – miski, mis võib kahjustada infovarasid; ohud võivad peituda infrastruktuuris, tehnoloogias, töötajates, töökorralduses;
- **Nõrkus** – selline koht infovarade juures, mis laseb ohul realiseeruda;
- **Risk** – tõenäosus, et oht kasutab ära nõrkuse ja tekitab infovarale kahju. Jääkrisk – risk mida on mõistlik aktsepteerida ja sellest tulenevalt riskiisu (*risk appetite*);
- **Meetmed** – tegevused riskide maandamiseks aktsepteeritavale tasemele.

Mittesihipärased (stiihilised) ohud

- **Keskkonnast** - liiga kuum, liiga külm, äike, vihm, lumi, …, vulkaanipurse;
- **Tehnikast** - elektrikatkestus, võrguühenduse katkestus, serveririke, …;
- **Inimestest** – inimliku nõrkuse ärakasutamine (*Social engineering*), eksimused teadmatusest, äpardused kogenematusest

Sihipärased ohud - ründed

Kes ja millistel ajenditel?

Kuidas korda saadetakse?

Puudused infrastruktuuris

- Ebapiisav kaitse füüsiliste ohtude eest – võivad realiseeruda keskkonnaohud või ründed;
- Meetmete osaline rakendamine (peale füüsiliste ka organisatsioonilised, näiteks serveriruumi loomine algab asukoha valikust).

Puudused tehnoloogias

- Süsteemide, seadmete tõrked;
- Seadmete paigutus;
- Süsteemide jõudlus;
- Ülepingutatud turvameetmed.

Puudused töötajates

- Teadmatusest või kogenematusest tehakse vigu;
- Eiratakse eeskirju ja nõudeid :
  - pääsuõiguste edasiandmine;
  - töö- ja eraasjad ei ole lahutatud;
- Ollakse liialt uudishimulikud:
  - pääsuõiguste taotlemine sinna, kuhu pole vaja.

Puudused töökorralduses

- Reeglid – puudulikud, ei teata, ei järgita;
- IT korraldus segane – ei tea kellele, millal ja kuidas probleeme teavitada;
- Dokumentatsiooni puudulikkus – süsteemi kirjeldus, kasutusjuhend puudu;
- Liigsed õigused – volitamata tarkvara paigaldamine.

Probleemid

- Ebapiisavad paroolid, paroolidega hooletu ringikäimine;
- Krüpteerimisest loobumine;
- Informatsiooni kaitse puudumine – kaitse vajadust ei teadvustata, reegleid ei jälgita;
- Liigne usaldamine;
- Väliste mäluseadmete või sülearvutite kadu / vargus;
- Kontrollimata tarkvara käivitamine.

Meetmed

- **Füüsilised** – uksed, aknad, seinad, lukud, … RUUMIDELE
- **Organisatsioonilised** – protseduurid, korrad, poliitikad, … INIMESTELE
- **(Info)tehnoloogilised** – pääsuõigused, ID kaart, viirusetõrje, krüpteerimine, varukoopiad, … SÜSTEEMIDELE

Meetmete liigid

- Ennetavad – vajalikud infoturbe intsidentide ärahoidmiseks;
- Avastavad – lähevad käiku, kui intsident on aset leidnud või on kõrgendatud kahtlus;
- Parandavad – taastavad olukorra, mis oli enne intsidenti ja võiksid olla aluseks ennetavate meetmete täiendamisel (et sarnaseid intsidente tulevikus ära hoida).

Enesehindamine

- Kas tööväliselt ajal on ametiasutuse sissepääsude uksed lukustatud?
- Kas ruumides on olemas valvesignalisatsioon?
- Kas ruumid on tööväliselt ajal valvesignalisatsiooni all?
- Kas ruumides on olemas tuletõrjesignalisatsioon?
- Kas tööväliselt ajal valvatakse ruume mehitatult?
- Kas võõrastele on tööpäeval piiratud sissepääs ametiasutuse ruumidesse?
- Kas ametiasutuse kõikide tööruumide uksed on lukustatavad?
- Kas tööruumide uste võtmed/kaardid väljastatakse ainult seal töötavatele töötajatele?
- Kas isikuandmeid või muud olulist informatsiooni sisaldavaid paberkandjal dokumente või töömaterjale hoitakse lukustatavates ruumides nii, et hoida ära volitamata juurdepääsu?
- Kas isikuandmeid või muud olulist informatsiooni sisaldavate paberkandjal dokumentide või töömaterjalide hävitamine toimub nii, et on välistatud nende sattumine kõrvaliste isikute kätte?

Enesehindamine

- Kas hoone valvamiseks töövälisel ajal on sõlmitud leping valvet teostava füüsilise või juriidilise isikuga?
- Kas sissepääsu(de) valvamiseks töö ajal on sõlmitud leping valvet teostava füüsilise või juriidilise isikuga?
- Kas hoonesse/ruumidesse sisenemise kord on haldusaktiga või muul viisil reguleeritud?
- Kas hoonesse/ruumidesse sissepääsul kontrollitakse külastajate isikuid?
- Kas ametiasutuses on määratud tuleohutuse eest vastutav isik?
- Kas ametiasutuses on määratud isikuandmete kaitse eest vastutav isik?
- Kas ametiasutusel on Andmekaitse Inspektsioonis registreeritud delikaatsete isikuandmete töötlemine?
- Kas ametiasutusel on olemas arhiivi ohuplaan?
- Kas tööruumide võtmete/kaartide väljastamine on haldusaktiga või muul viisil reguleeritud?
- Kas tööruumide kasutamise kord on haldusaktiga või muul viisil reguleeritud?
- Kas tööruumide kasutamise korras on nõutud lukustamata ustega tööruumide mitte valveta jätmist?
- Kas uue töötaja töölevõtmisel tehakse isiku nõusolekul kandidaadi taustauuring?
- Kas töötajatele tutvustatakse allkirja vastu:
  - hoonesse/ruumidesse sisenemise korda?
  - tööruumide kasutamise korda?
  - tuleohutusreegleid?
  - tööohutusreegleid vm turvariskide füüsilise vältimise meetmeid?
  - infoturbe põhimõtteid ja organisatsioonilisi meetmeid (näiteks protseduurireeglid, korrad ja eeskirjad turvanõuete täitmiseks)?
  - infotehnoloogiliste vahendite kasutamise reegleid?
- Kas infotehnoloogia vahendid (lauaarvuti, sülearvuti, printer jms) väljastatakse töötajale allkirja vastu?
- Kas töötajate ametijuhendites/töölepingutes on sätestatud konfidentsiaalsusreeglid?
- Kas töösuhte lõppemisel võetakse isikult ära tööruumide võtmed/kaardid ja tühistatakse juurdepääsuõigused infosüsteemidele ja andmekogudele?

Infoturbe organisatsioon

- Tippjuhtkond;
- Infoturbe juht;
- Infoturbe nõukogu;
- Ekspert/spetsialist;
- Töötaja/teenistuja/kasutaja;
- Protsessi omanik;
- Muud võtmeisikud;
- Audiitor;
- Koolitajad ;
- **Organisatsiooni infoturbepoliitika.**

Intsidendid

Me teame, kes tegelevad ja me teame reegleid.
Nüüd, kui intsident aset leiab, siis:

- Jääda rahulikuks, mitte teha läbimõtlemata tegusid
- Viivitamata raporteerida vastavalt eeskirjadele
- Mitte võtta vastumeetmeid enne heakskiitu
- Mitte varjata asjaolusid
- Hinnata kahjusid, tagajärgi, mõjutatud pooli
- Informeerida kolmandaid osapooli vaid siis, kui see on lubatud

Õigusaktid

Riigi tasandil:

- Isikuandmete kaitse seadus
- Avaliku teabe seadus
- Kohaliku omavalitsuse seadus
- Hädaolukorra seadus
- Tuleohutuse üldnõuded
- Registrite seadused
- Karistusseadustik
- Infosüsteemide koosvõime (raamistikud)
- ISKE määrus

Tallinnas:

- Infoturbe põhimõtted
- Asjaajamise kord
- Tallinna linna ametiasutustes kasutatava arvutustehnika riistvara- ja tarkvarastandardid
- IT vahendite kasutamise reeglid
- Infosüsteemide põhimäärused

- Infoturbe suurim oht asub tooli ja arvuti vahel

  Vaata:
  http://www.youtube.com/watch?v=aDKSZuql9xc&NR=1

Tänan!

anne-mari.vunder@tallinnlv.ee