Infoturbe haldus

Hillar Põldmaa

Teemad

- Seire ja logimine
- Intsidendihaldus, forensic, raporteerimine
- Jätkusuutlikkuse haldus
- Vastavus

Seire ja logimine

Seire

Seire kaalutlusi

- Kasutajate privaatsus
  - http://www.aki.ee/et/uudised/pressiteated/andmekaitse-inspektsiooni-10-soovitust-uueks-aastaks
  - 3. Töö juures kaitse ise oma eraelu!
- Käideldavus
- Konfidentsiaalsus
- Terviklus
- Mida ja kui palju - mahud
- Turvalisus

Seire eesmärk

- Informatsioon tegeliku kasutamise kohta
- Informatsioon võimalike probleemide kohta
- Tuvastada võimalikud ründed
- Säilitada tõendeid ründe kohta
- Hilisema uurimise võimalus

Mida seirata

- Võrguliiklus
- Teenust pakkuvad masinad
  - Ressursid (CPU, RAM, HDD)
  - Teenused
- Teenused – kasutaja poolne vaade
- Masinate (eelkõige serverite) vaheliste ühenduste jälgimine (võrk ja võrguseadmed);
- Masinate (eelkõige serverite) logide jälgimine;

Seire eeldused

- Vastavate ressursside olemasolu
- Vajaliku tarkvara paigaldus
  - Võrk
  - Logid (seadmed, rakendused, andmebaasid)
  - Teenuste testid
- Kellaaegade ühtlustamine
- Inimene, kes tegeleb seirega

Seire vahendeid (1/2)

Protokollid

- SSH
- HTTP(S)
- SNMP – simple network management protocol
  - V1, v2c, v3
- SYSLOG
  - Vajadusel konverterid
- NB! Windowsi logi **ei ole** universaalselt käideldav

Seire vahendeid (2/2)

Rakendused

- Nagios ja Zabbix (käideldavus)
- Snort ja Suricata (võrgupaketid)
- MRTG (multi router…
- ELK
  - Elasticsearch, Logtash, Kibana
- …
- Kommertslahendused...

Seire planeerimine

- Üks server tekitab mõnest MB kuni mitu GB logi päevas (kasutajad, teenused)
  - Win/Lin süsteemilogi 2-3 MB,
  - Rakendused 1-4 GB
- Logide töötlemiseks vajalikud ressursid
  - Protsessor ja mälu (arvutusvõimsus)
  - Võrk (edastamine)
  - Kettaruum

Kellaaja ühtlustamine

- Võrgu kõikidel masinatel peab olema üks kellaaeg
- NTP server (näiteks pool.ntp.org)
  - Windows
  - Linux/UNIX
- Arvestamine partneritega

Seire prioritiseerimine

Ei tohi tekkida täiendavaid turvariske

- Põhiprotsessid **peavad** jääma toimima
- Konfidentsiaalsus **peab** olema tagatud
- Põhitegevuse serverid
  - Rakendus ja andmebaasiserverid
  - Eriserverid (nt pildipangad vms)
- Turvaserverid (viirustõrje, snort)
- Abitegevuse serverid (dokumendihaldus, faili- ja siseveebiserver jne)

Nõuded logidele

- Maht võimalikult väike, samas peavad sisaldama vajalikku infot (kes, millal, mida, mille pärast)
- Kirjed peavad olema sarnasel kujul

  $TIMESTAMP $WHO $EVENT $ADDITIONAL-INFO
- Kooditabel peab olema sama (ISO, UTF)
- Failinimi peab olema sarnane
- Põhjendus – regulaaravaldistega otsimise võimalus (RegExp compatible)

Logide kirjutamine

- Süsteemsed
  - Windows
  - UNIX/Linux
- Rakendused
- Andmebaasid

Logide edastamine

- Logide hoidmine keskserveris (autentsuse tagamine)
- Kohalik kõvaketas ja sealt mingi programmiga edasi saata
- Keskserveri kettale (autentsuse probleem)
  - Kirjutamisõigus, seega muutmisõigus
- Hea lahendus – otse mingi süsteemiga (Lin:rsyslog või syslog-ng; Win ossec vms)
- **NB! Võrgu koormus, ketta mahutavus**

Logide korreleerimine

- Mitme eri seadme logide omavaheline võrdlemine
  - Kellaajad
  - Sündmused
- Muster, mis võimaldab
  - Tuvastada kasutajate käitumise
- Näited
  - Lokaalsesse arvutisse logib kasutaja, kes pole tööl
  - Legaalne programm võtab ühendust veebilehega

Termineid

- True Positive
- True Negative
- False Positive
- False Negative
- Korreleerimine võimaldab kahte viimast vähendada

Intsidendihaldus

Eskaleerimine

- Üks ja ühine kontakt

- Sündmus (Event)
- Probleem (Problem)
- Intsident (Incident)
- Avarii (Disaster)

Intsidendihaldus

- Plaanimine
- Tuvastamine
- Kindlaks tegemine
- Hindamine
- Raporteerimine ja kommunikatsioon
  - Erinevad sihtgrupid (juhtkond, töötajad, partnerid, avalikkus, CERT)
- Tagajärgede vähendamine
- Taastamine

Plaanimine

Murphy seadus: kui midagi saab sandisti minna, siis ta ilmtingimata ka läheb

Siis, kui on probleem, pole enam aega

- Eelnevalt plaanid valmis

Plaane tuleb ka testida

- Reaalselt (plaan näppu ja kõik sammud läbi käia)
- TTX (**T**able**T**op E**x**ercise)

TTX – Table Top Exercise

Ründajad annavad ette ründestsenaariume, kaitsjad selgitavad, mida nad ühel või teisel juhul teeksid.

Kasutatakse juhul, kui reaalne testimine pole:

- Tehniliselt võimalik
- Rahaliselt võimalik

Rünnete tuvastamine

Monitooring (seire)

- Logid (serverid, teenused, tööjaamad)
- Võrguliikluse analüsaatorid
- Pahavara tuvastajad
- turvaseadmed

Parimaid tulemusi annab kõikide kombinatsioon ja nende väljundite korreleerimine

Kindlaks tegemine

- Potentsiaalse ründe puhul tuleb kindlaks teha millega on tegemist
- Võimalik, et paanikaks polegi põhjust

Hindamine

- Kui ohtlik on rünne
- Mida saab konkreetse ründe puhul ette võtta
- Mitme erineva samaaegse ründe korral prioritiseerimine
- Sageli peidetakse üks rünne teise sisse
  - Tüüpiline on ründe peitmine DDoS sisse

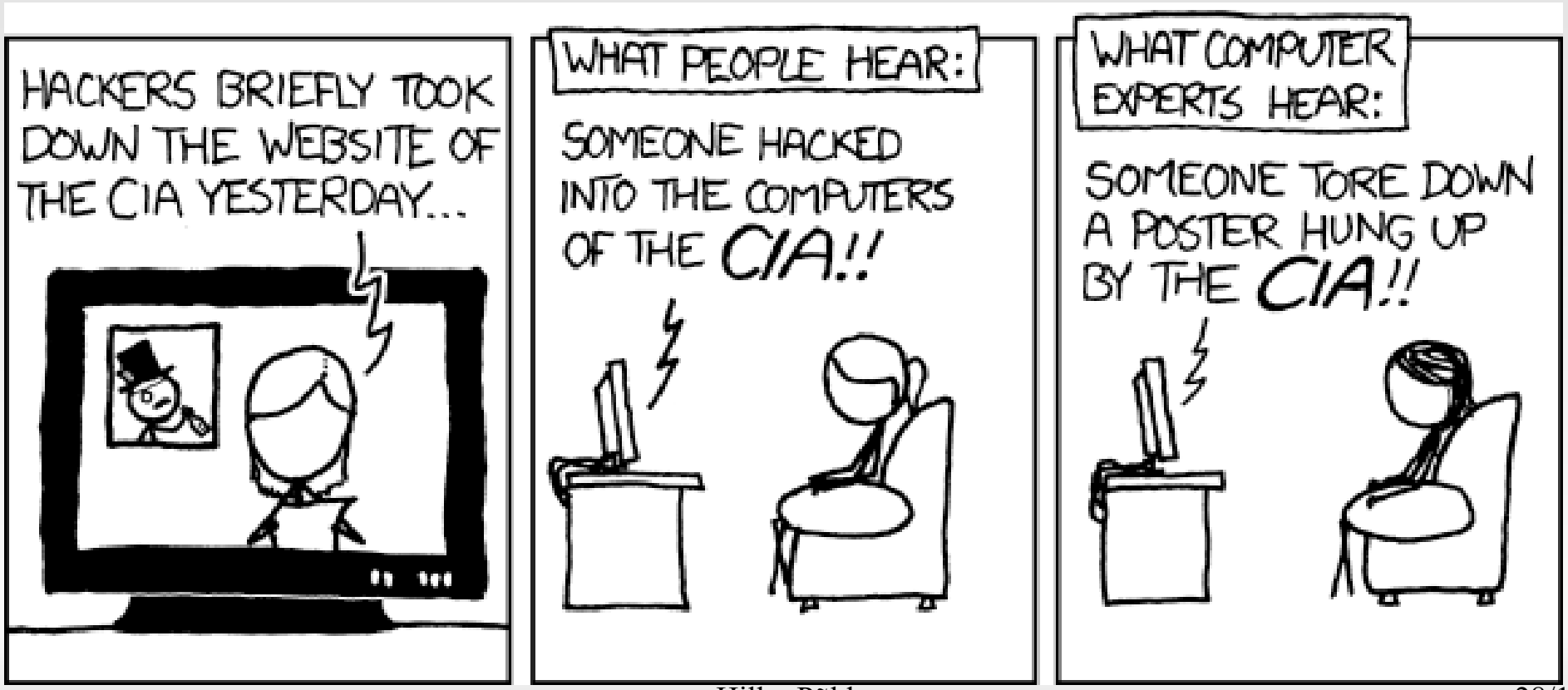
Raporteerimine/kommunikatsioon

Erinevad sihtgrupid

- Juhtkond
- Töötajad
- Partnerid
- Avalikkus
- CERT

Kommunikatsioonireeglid

- Sihtgrupile arusaadav tekst
  - NB! Sõnavara



Kommunikatsioonireeglid

- Nii palju, kui vajalik, nii vähe kui võimalik
- Kui ei tea või pole kindel
  - tunnista ja ütle, et uurid
- Oluline on paanika ning mainekahju vältimine
- Kui probleem on tekkinud enda süül
  - tunnista ja vabanda
- Kiusatus on vassida
  - Helmes ja valimised
- **Kahe tunni reegel ja kuue tunni reegel**

Tagajärgede vähendamine

Ründe lokaliserimine

- Arvuti võrgust eemaldada
- Võrguühenduste blokeerimine
- ...

NB! voolu väljalülitamine ei ole hea idee

- Jäljed võivad hävineda

Jälgede säilitamine edasiseks uurimiseks

Enne taastamist võtta näidised

- Edasine uurimine
- Raport

Intsidendi uurimise (Forensic) ettevalmistavad sammud

- Koopia mälust (kui pole võimalik siis...)
- Koopia kõvakettast (kui pole võimalik siis...)
  - Koopia autentsuse tagamine
- Intsidendi uurimine ja analüüs

Taastamine

- Riistvara taastamine
  - Kõvaketta vahetus
- Võrguühenduste taastamine

Puhas install

- Programmid originaalmeedialt
- Seaded vastavalt taasteplaanile
  - Varukoopia /etc, seadistusfaildest tuleb üle vaadata
- Andmed varukoopiast

Intsidendiraport

- Mis juhtus
- Miks juhtus
- Tagajärjed
- Mis tehti kõrvaldamiseks ja parandamiseks
- Mida teha, et edaspidi ei juhtuks

Intsidendiraporti näidis

Intsidendi tüüp			Intsidendi põhjus			
Käideldavus			Tarkvara viga		Kasutajaõiguste haldus	
Terviklus			Riistvara viga		Välise teenusepakkuja viga	
Konfidentsiaalsus			Administreerimise viga		Disain ja häälestused	
Muu			Andmehalduse viga			

Intsidendi kokkuvõte:	
Intsidendi toimumise aeg, ulatus ja äriline mõju:	
Intsidendi kirjeldus ja kronoloogia:	Taust: ...
Põhjus / Lahendus:	Intsidendi algpõhjus: ... Võimalik lahendus: ...

Soovitus 1:	
Soovitus 2:	

Edasised sammud

Kas on vaja midagi muuta?

- Riistvara
- Konfiguratsioon
- Juhendid ja korrad
- Koolitused

Intsidendi uurimine (Forensics)

Sissejuhatuseks

- Head tõlget terminile „**forensics**“ hetkel ei ole
- Eesti keeles võib kasutada terminit „**intsidendi uurimine**“
- Loengus kasutame inglisekeelseid väljendeid „**Digital Forensics**“ ja „**Computer Forensics**“

Digital Forensics – mis see on?

Protsess intsidendi uurimiseks

- Säilitamine
- Kogumine
- Vaatlus
- Analüüs
- Raport

Peab vastama „5W“ küsimusele

Väljund (tulemus) on raport

5W

Who What Where When Why How

- **Who** gained access?
- **What** did they do?
- **When** did this happen?
- **Where** did they go?
- **Why** did they choose this network?
- **How** did they do this?

Intsidendi haldus vs. digital forensics

Intsidendi haldus

- Valideerib tuvastamise käigus tehtud avastused
- Võtab kasutusele meetmed intsidendi peatamiseks ja mõju vähendamiseks

Digital Forensic

- intsidendi peatamiseks ja mõju vähendamiseks ning selle uurimiseks vajalike tõendite kogumine, säilitamine, analüüsimine ning esitlemine

Computer forensics

Computer Forensics = Teadus + Kunst

- Teadus = tööriistad ja meetodid
- Kunst = tööriistade valik ja kasutamine ning tulemuste interpreteerimine
- Kaks erinevat uurijat võivad samade tõendite pealt jõuda erinevate tulemusteni

2 nägu (mütsi)

- Kunstnik/praktik – kasutada juba loodud tehnikat/teadmisi
- Teadlane – loob uued meetodid (kui vajalik)

Digital Forensics – mida see ei ole?

- Digital Forensics – ei ole mõeldud andmetaasteks
- Digital Forensics – ei ole andmete tootja vaid analüüside ja raportite looja

Spetsialiseerumine

Erinevad suunad – vajalik on spetsialiseerumine

- Pahavara (rootkit, MBR-kit's)
- Andmete peitmine (steganography)
- Sissetungid arvutisse (sisemine/välimine)
- Mobiilseadmete uurimine (kasvav turg)
- Võrgu uurimine (Erineb Computer Forensics)
- Anti-Forensics
- Kombinatsioonid

Muutuv maailm – uued OS, FS, meetodid, tööriistad...

Forensic protsessina

Kolm suuremat plokki

- Tõendite kogumine
- Tõendite analüüs
- Raporteerimine

Kasutusel on mitmeid erinevaid mudeleid ja töövooge

- Väga suuri põhimõttelisi erinevusi pole

Forensic process

- Verifitseerimine — **Intsidendi haldus**
- Süsteemi kirjeldamine
- Tõendite hankimine

- Ajalise järjestuse analüüs — **Forensics**
- Meediumi analüüs
- Sõnede (string) otsing ja biti otsing

- Andmete taastamine
- Raporteerimine

Verifitseerimine

Kas siin on toimunud intsident?

- Forensics on kallis – kas me peaksime sellega tegelema?

Ettevaatust, et tõendeid mitte ära rikkuda

- Töökindlad riistad

Põhjalikult, et mitte lasta end lollitada (vale-negatiivse oht)

- Tööriistu on võimalik lollitada
- Pahavara ja VMware

Süsteemi kirjeldamine

Analüüsitava süsteemi kirjeldamine

- Kuskohast saadud
- Milleks seda kasutati
- Kuidas konfigureeritud (OS, võrk, välisseadmed)
- Muu asjakohane info

Tõendite kogumine

Väga palju kohti, kuhu peab vaatama

- Kohalik
- LAN
- WEB

Püsivad ja mittepüsivad

Tõendid ei tohi muutunud/muudetud

- Tõendite kogumise kiirus
- Võimalikult vähe „puudutades“

Ajalise järjestuse analüüs

- Iga uurimise põhiline tööriist
- Sündmuste ajaline järjekord
- Installeerimine
- Uuendused
- Buutimised
- Taaskäivitused
- Failide avamised ja muutmised
- jne...

Meediumi analüüs

Juhtumipõhiste tõendite otsimine

Uurimise-spetsiifilised

- Kustutatud failid
- Pildid
- E-kirjad
- Pahavara

Sõnede otsimine

- Arvuteid kasutatakse enamasti tekstitöötluseks
- Inimeste loodud sisu
- Leida kõik sõned
- Tekitada „pahade väljendite“ nimekiri
- Otsida
- Spetsiifilised mustrid – bitiotsing

Andmete taastamine

Pahalased püüavad oma jälgi peita

- Kustutatud failid
- Failide osad

Raporteerimine

Kõige olulisem osa – see on tulem

> 50% kulutatud ajast

Raport peab vastama paljudele küsimustele

- Miks uurimine läbi viidi?
- Mida konkreetselt uuriti, milliseid tõendeid leiti?
- Kuidas tagati tõendite ahel (chain of custody)?
- Mida leiti?
- ...

Raporteerimine

Aruande eesmärk on anda lugejale:

- Kogu vajalik informatsioon
- Selgelt
- Lühidalt

Sihtgrupispetsiifiline sõnavara/tekst

Ei tohi olla isiklikke arvamusi või seisukoht

Töövoog

Iteratiivne protsess

Parim meetod

Parimad tööriistad

Leitud tulemuste analüüs

Samad meetodi, kuid erinevad tööriistad

- Platvorm (riistvara)
- Operatsioonisüsteem
- Failisüsteem

Märkmete tegemine

- Jätkuv
- Süsteemne
- Piisavalt detailne, et tulemus oleks korratav
- Digitaalne ja paberkandjal

Märkmete tegemine - tähtsus

Tõendite ahel (chain of custody)

Dokumenteerida tõendi seisukord:

- Kettatõmmise kontrollsumma/räsi (md5, sha1, sha512, ...)
- Süsteemsete komponentide (riistvara) räsi
- Korrata, kui tõendid võivad olla muutunud
- Dokumenteerida paberil
- Dokumenteerida tõendil
- Toetavad dokumendid

Märkmete tegemine – tõendil

Seadme tähistamine

- Korpuse number ja seerianumber
- Tähistamise süntaks (näit. juhtum#-DD-MM-YY –S/N)

Tõendite loend

- Kirjeldus
- S/N
- Kontrollsumma
- Meediumi suurus

Korratavus:

- Salvestustöörist ja versioon; käsurea logi vms

Märkmete tegemine

Käigu pealt dokumenteerimine

- Kasutatud tööriist
- Versioon
- Suvandid (options), võtmed (switches), käsud

Peab olema piisav tulemuse taaskordamiseks

Juhtumi uurimine võib kesta aastaid (kohus) – nii pika aja jooksul ei saa enam mälu usaldada

Tagasi intsidendi halduse juurde

Jälgede säilitamine edasiseks uurimiseks

Enne taastamist võtta näidised

- Edasine uurimine
- Raport

Uurimise (Forensic) sammud

- Koopia mälust (kui pole võimalik siis...)
- Koopia kõvakettast (kui pole võimalik siis...)
  - Koopia autentsuse tagamine
- Pahavara analüüs

Allikad

- Seire logid
- Arvuti(d) ise
- Seletuskirjad

Jätkusuutlikkuse haldus

Jätkusuutlikkuse tagamine:

- Protsesside talitluspidevuse nõuded
- Talitluspidevuse planeerimine
- Taaste planeerimine
- Talitluspidevuse testimine

Protsesside talitluspidevuse nõuded

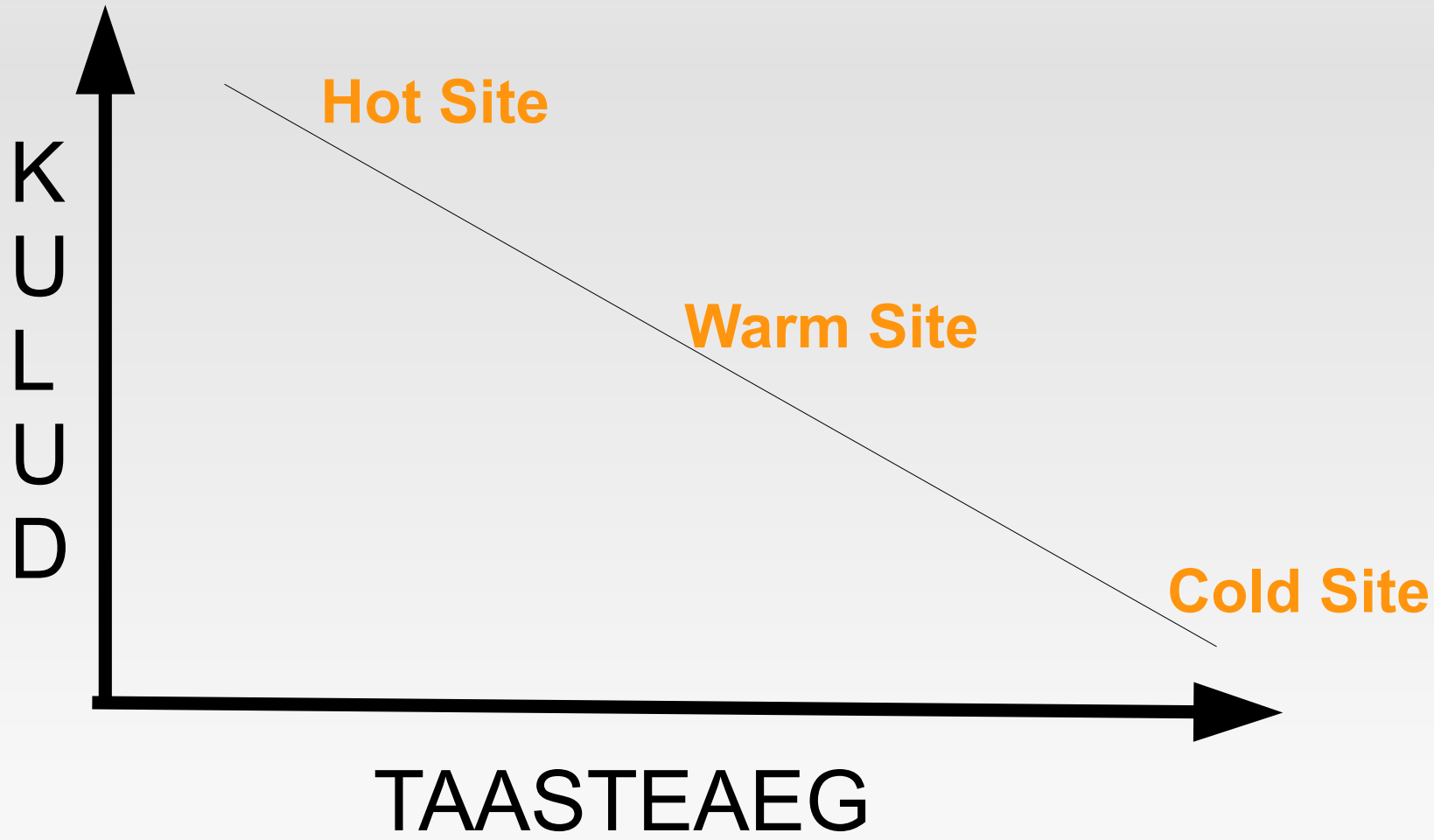
- Kui kaua võib protsess mitte toimida, enne kui see mõju avaldab?
  - Päevades
  - Tundides
  - Sekundites
- Kas on lubatav teenuse ajutine halvenemine
  - Reaktsiooniaeg millisekundid vs sekundid
  - Mõningane funktisonaalsuse kadu
- Vastavalt hakkame planeerima talitluspidevust

Talitluspidevuse planeerimine

Sõltub äriprotsessi nõuetest

- Kui on lubatud teenuse halvenemine
  - Näide: 2007 ajalehed ja riigi veebid
- Taastamise kiirus
  - Hot Site
  - Warm site
  - Cold site
- Varukopeerimise nõuded

Jätkusuutlikkuse haldus (3/4)



Varukopeerimise nõuded

- Lubatud andmekadu
  - Kui palju on äripool valmis „käsitsi“ uuesti tegema
- Varukoopia plaan
  - Päev
  - Nädal
  - Kuu
  - Kvartal
  - Aasta
- Arhiivikoopia

Taaste planeerimine

- Tegevuse katkematuse strateegia tähtis osa on plaan kriitiliste tegevuste jätkamiseks katkestuse korral.
- Avariijärgne taasteplaan visandab rollid ja kohustused sellisteks tingimusteks.
- Kõigi infosüsteemi olulisemate elementide ja andmekogude kohta peab olema koostatud avariijärgse taasteplaan ning on määratud vastutav teostaja

Taasteplaan (1/2)

Avariijärgne taaste plaan peab sisaldama:

- kriitilisteks loetavate tegevuste loetelu, eelistatavalt koos prioriteediklassidega ja koos ärikohustuste täitmiseks adekvaatsete ajaliste piiridega;
- avarii liike, mille eest tuleb kaitsta;
- kriitilisi tegevusi toetavate töötlusressursside ja asukohtade asendamiseks vajalike vabade ressursside ja kohtade loetelu;

Taasteplaan (2/2)

- töötlusressursside käituseks või puuduvate töötajate asendamiseks kasutada olemasolevate töötajate loetelu;
- varundamisele kuuluva informatsiooni ja selle talletuskoha määrangu koos nõudega sooritada varundussalvestused määratud vastavalt varukoopiate tegemise korrale;
- lepinguid teenusetarnijatega teenuste prioriteetseks taasalustamiseks, kus on võimalik.

Talitluspidevuse testimine

- Avariijärgse taasteplaani tuleb testida nii tihti, kui on vaja probleemide avastamiseks ja töötajate tegutsemisvalmiduse säilitamiseks.
- Taasteplaane tuleb regulaarselt uuesti hinnata, et veenduda nende eesmärgipärasuse toimivuses.
- Testimine reaalselt
  - **Varukoopiad!**
- Testimine „laual“ - TTX

Vastavus

Turbenõuete vastavus:

- Vastavus õigusaktide nõuetele;
- Vastavus infoturbepoliitikale;
- Infosüsteemide auditeerimisvajadus;
- Infoturbe dokumentide auditeerimine;
- Infoturbe korralduse auditeerimine.

Seadused

Disclaimer

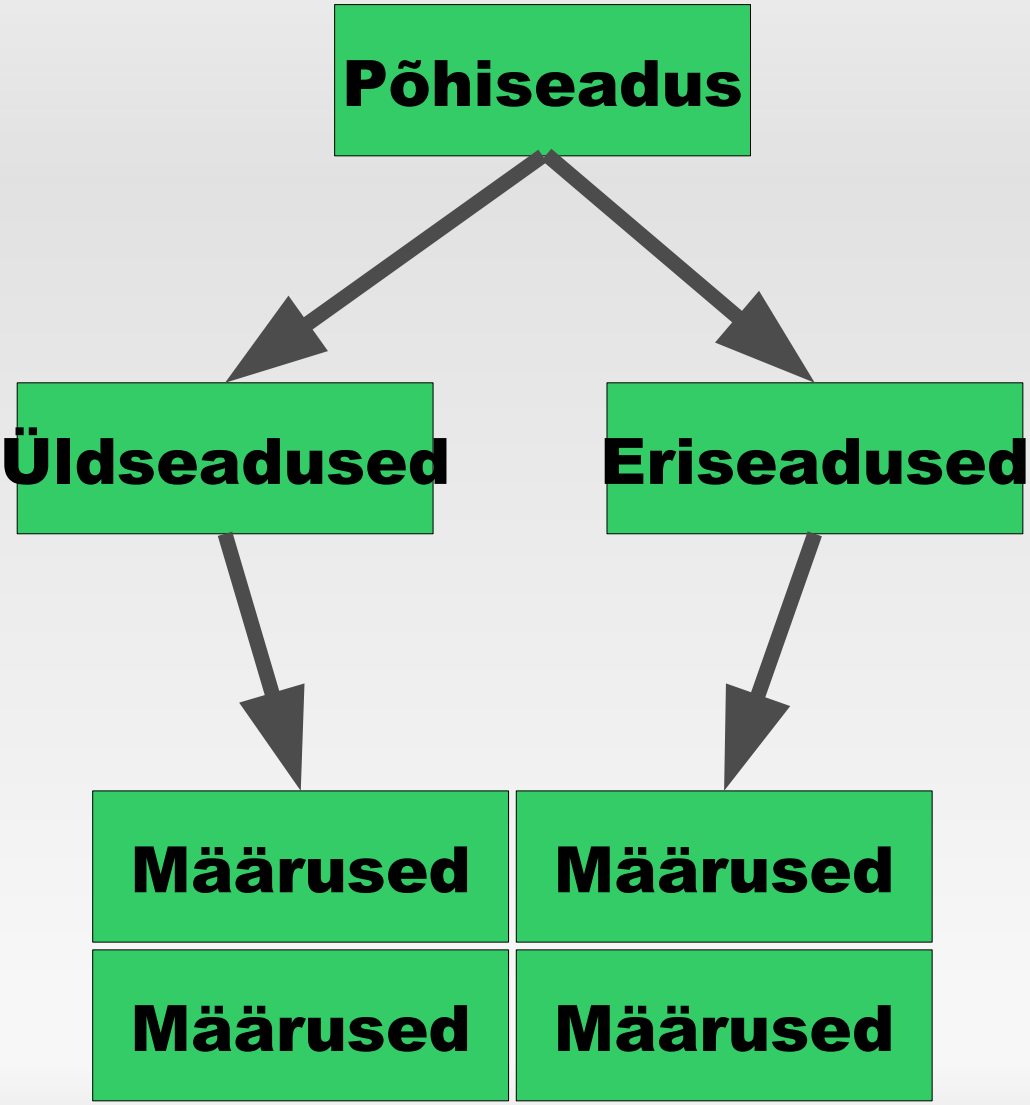
- Järgnev on IT inimese vaade
- Juristidel võb olla hoopis erinev arusaam
- Naljaga pooleks:

  Kui toas on kolm juristi, siis on seal neli arvamust

Üldine loogika

Põhiseadus

- **Üldseadused** – kehtestavad üldised reeglid
- **Eriseadused** – kehtestavad konkreetsed reeglid konkreetsetel tingimustel
- **Määrused** – täpsustavad seaduse mingit punkti



Avalik ja eraõigus

- Avalik õigus – kõik, mis pole lubatud, on keelatud
  - Kui seaduses pole öeldud, siis seda teha ei tohi
  - Õnneks on väike ruum kaalutlusõiguse puhul
- Eraõigus – kõik, mis pole keelatud, on lubatud
  - Liigne liberaalsus sünnitab üsna kummalist käitumist

Andmete töötlusega seonduvad õigusaktid

- Üldjuhul andmete töötlusega seonuvad
- Kokku üle saja erineva
  - Valdkonnaspetsiifilised õigusaktid (eriseadused) - statistikud, pangad jne
- Põhilised (üldseadused)
  - Isikuandmete kaitse seadus (IaKS)
  - Autoriõiguse seadus (AutÕS)
  - Võlaõigusseadus (VõS) üldine lepinguid käsitlev

Küberturbega seotud seadused

- Avaliku teabe seadus (AvTS);
- Elektroonilise side seadus (ESS);
- Hädaolukorra seadus (HOS); (hetkel on kooskõlastamisel seaduse uus versioon)
- Korrakaitseseadus (KoRS);
- Karistusseadustik (§-id 206, 207, 213, 216[1], 217, 218)
- Riigisaladuse ja salastatud välisteabe kaitse seadus.

Küberturbega seotud määrused

- Vabariigi Valitsuse 14.03.2013 määrus nr 43 „Elutähtsa teenuse infosüsteemide ning nendega seotud infovarade turvameetmed“
- Vabariigi Valitsuse 20.12.2007 määrus nr 252 „Infosüsteemide turvameetmete süsteem“
- Vabariigi Valitsuse 15.03.2012 määrus nr 26 „Infoturbe juhtimise süsteem“
- Vabariigi Valitsuse 03.07.2014 määrus nr 108 „Kaitseliidu kaasamise tingimused ja kord küberturvalisuse tagamisel“
- **Oluline dokument** „Küberjulgeoleku Strateegia 2014-2017“.

Avaliku teabe seadus

Avaliku teabe seadus

Peatükk 5^1 - andmekogud (§§ 43^1...43^9)

- Tekkis peale Andmekogude Seaduse liitmist 2007
- Ütleb, et andmekogud on ainult riigil
- Ei käsitle arvutist väljaspool olevaid andmekogusid

Andmekogu

- Andmekogu on riigi, kohaliku omavalitsuse või muu avalik-õigusliku isiku või avalikke ülesandeid täitva eraõigusliku isiku infosüsteemis töödeldavate korrastatud andmete kogum, mis asutatakse ja mida kasutatakse seaduses, selle alusel antud õigusaktis või rahvusvahelises lepingus sätestatud ülesannete täitmiseks.

Riigi infosüsteem

- Riigi infosüsteemi kuuluvad andmekogud, mis on riigi infosüsteemi andmevahetuskihiga liidestatud ja riigi infosüsteemi haldussüsteemis registreeritud, ning andmekogude pidamist kindlustavad süsteemid.

Riigi infosüsteemi kindlustavad süsteemid

- klassifikaatorite süsteem;
- geodeetiline süsteem;
- aadressiandmete süsteem;
- infosüsteemide turvameetmete süsteem;
- infosüsteemide andmevahetuskiht;
- riigi infosüsteemi haldussüsteem.

Andmekogu asutamine

- Andmekogu asutatakse seadusega või selle alusel antud õigusaktiga
- Keelatud on asutada ühtede ja samade andmete kogumiseks eraldi andmekogusid.
- Enne andmekogu asutamist, andmekogus kogutavate andmete koosseisu muutmist, andmekogu kasutusele võtmist või andmekogu lõpetamist kooskõlastatakse andmekogu tehniline dokumentatsioon Majandus- ja Kommunikatsiooniministeeriumiga, Andmekaitse Inspektsiooniga ja Statistikaametiga.
- Ainult organisatsiooni sisemise töökorralduse vajadusteks või asutustevaheliseks dokumentide menetlemiseks peetavat ja riigi infosüsteemi mittekuuluvat andmekogu ei pea käesoleva paragrahvi lõikes 3 sätestatud korras kooskõlastama.

Vastutav ja volitatud töötleja

- Andmekogu **vastutav töötleja** (haldaja) on riigi- või kohaliku omavalitsuse asutus, muu avalik-õiguslik juriidiline isik või avalikke ülesandeid täitev eraõiguslik isik, kes korraldab andmekogu kasutusele võtmist, teenuste ja andmete haldamist. **Andmekogu vastutav töötleja vastutab andmekogu haldamise seaduslikkuse ja andmekogu arendamise eest.**
- Andmekogu vastutav töötleja **võib volitada** andmete töötlemise ja andmekogu majutamise teisele riigi- või kohaliku omavalitsuse asutusele, avalik-õiguslikule juriidilisele isikule või hanke- või halduslepingu alusel eraõiguslikule isikule vastutava töötleja poolt ettenähtud ulatuses.

Vastutav ja volitatud töötleja

- **Volitatud töötleja** on kohustatud täitma vastutava töötleja juhiseid andmete töötlemisel ja andmekogu majutamisel ning tagama andmekogu turvalisuse.
- Andmekogu vastutav töötleja korraldab riigi poolt kohalikule omavalitsusele pandud või delegeeritud ülesannete täitmiseks asutatud andmekogu keskse tehnoloogilise keskkonna loomise ja haldamise.

NB! vastutava ja volitatud töötleja mõistet kasutatakse ka eraettevõtluses

- Paljude riiklike andmekogude volitatud töötlejaks on eraettevõtted

Andmekogu põhimäärus

- Andmekogu põhimääruses sätestatakse andmekogu pidamise kord, sealhulgas andmekogu vastutav töötleja (haldaja), andmekogusse kogutavate andmete koosseis, andmeandjad ja vajaduse korral muud andmekogu pidamisega seotud korralduslikud küsimused.
- Andmeandjaks on riigi- või kohaliku omavalitsuse asutused või muud avalik-õiguslikud või eraõiguslikud isikud, kui neil on seadusega või selle alusel antud õigusaktiga sätestatud kohustus andmekogusse andmeid esitada või kui nad teevad seda vabatahtlikult.

Andmekogu registreerimine

- Enne andmekogu kasutusele võtmist tuleb see registreerida riigi infosüsteemi haldussüsteemis. Andmekogu registreerimise kord sätestatakse käesoleva seaduse § 43^9 lõike 1 punktis 6 nimetatud kindlustavat süsteemi kehtestavas määruses.
- Enne riigi infosüsteemi kuuluva andmekogu registreerimist kontrollib ja kooskõlastab vastavat pädevust omav majandus- ja kommunikatsiooniministri volitatud teenistuja või ministeeriumi valitsemisalasse kuuluva asutuse töötaja andmekogu tehnilise vastavuse ning kogutavate andmete koosseisu ja allikate vastavuse seaduse või selle alusel antud õigusaktiga kehtestatud nõuetele.

Andmekogu avalikkus

- Andmekogus töödeldavad andmed peavad olema avalikult kättesaadavad, kui neile ei ole seadusega või selle alusel kehtestatud juurdepääsupiirangut.
- Andmekogus ei avalikustata isikuandmeid, kui avaldamise kohustus ei tulene seadusest.
- Julgeolekuasutust puudutavate andmete kajastamisel riigi andmekogudes võib julgeolekuasutuse juhi salajase käskkirja alusel kasutada variandmeid.

Riigi infosüsteemi kindlustavad süsteemid

- klassifikaatorite süsteem;
- geodeetiline süsteem;
- aadressiandmete süsteem;
- **infosüsteemide turvameetmete süsteem (ISKE);**
- infosüsteemide andmevahetuskiht;
- riigi infosüsteemi haldussüsteem.

Andmevahetus riigi infosüsteemi kuuluvate andmekogudega ja riigi infosüsteemi kuuluvate andmekogude vahel toimub läbi riigi infosüsteemi andmevahetuskihi.

Elektroonilise side seadus

Reguleerimisala

- Elektroonilise side võrgud ja teenused
- Raadiosagedused (raadioside, mobiil, wifi jne)
- Numbrijaotus
- Nõuded teenuse pakkujatele, nende õigused ja kohustused

Andmete säilitamise kohustus § 111[1]

- Sideettevõtja on kohustatud säilitama andmed, et oleks võimalik teha järgmisi toiminguid:
  - 1) sideallika seiramine ja tuvastamine;
  - 2) side sihtpunkti tuvastamine;
  - 3) side kuupäeva, kellaaja ja kestuse kindlaksmääramine;
  - 4) sideteenuse liigi kindlaksmääramine;
  - 5) sideteenuse kasutaja terminalseadme või oletatava terminalseadme kindlaksmääramine;
  - 6) terminalseadme asukoha kindlaksmääramine.

Andmete säilitamise kohustus § 111[1]

- (2) Telefoni- ja mobiiltelefoniteenuse ning telefonivõrgu ja mobiiltelefonivõrgu teenuse osutaja
- (3) Interneti-ühenduse, elektronposti ja Interneti-telefoni teenuse osutaja

Kogu info va. sisu

- Säilitatakse 1 aasta

Kohtule andmise kohustus (§114[1])

- Sideettevõtja on kohustatud esitama §111[1] lg 2 ja 3 näidatud info
- NB! uurimisorganite õigused on mööda seadust laiali

Hädaolukorra seadus

Reguleerimisala

- Sätestab kriisireguleerimise õiguslikud alused
  - hädaolukorraks valmistumise
  - hädaolukorra lahendamise
  - elutähtsate teenuste toimepidevuse tagamise
- Reguleerib ka eriolukorra väljakuulutamist, lahendamist ja lõpetamist ning Kaitseväe ja Kaitseliidu kaasamist hädaolukorra lahendamisse.
- Ei reguleeri sõjalisest ohust tingitud hädaolukorraks valmistumist ja hädaolukorra lahendamist

Elutähtsad teenused

Kokku 43 nimetust. Põhilised valdkonnad

- Trantsport ja side
- Pääste ja arstiabi (erakorraline meditsiin)
- Elekter ja kütus
- Toit ja vesi
- Kanalisatsioon ja prügi
- Pangateenused (maksed ja sularaha)
- Vanglad

Seaduse juures olevad määrused

- Hädaolukorra riskianalüüsi koostamise juhend
- Hädaolukorra lahendamise plaani koostamise juhend
- Toimepidevuse riskianalüüsi koostamise juhend
- Toimepidevuse plaani koostamise juhend
- Elutähtsa teenuse infosüsteemide ning nendega seotud infovarade turvameetmed

Hädaolukorra seadus

- Riskianalüüsi, tegutsemisplaani ja õppuste nõue

Võib olla abiks, kui on vaja

- Põhjendada mingeid (rangemaid) erinõudeid
- Põhjendada riskianalüüsi metoodikat

Korrakaitseseadus

Reguleerimisala

- Avaliku korra kaitse
- Korrakaitse on avalikku korda ähvardava ohu ennetamine, ohukahtluse korral ohu väljaselgitamine, ohu tõrjumine ja avaliku korra rikkumise kõrvaldamine
- **Internet on avalik ruum (nt. kommentaarium)**
- ei kohaldata julgeolekuasutuste tegevusele
- ei kohaldata Kaitseväe tegevusele riigi sõjalisel kaitsmisel
- ei kohaldata vanglateenistuse tegevusele kinnipeetava ja vahistatu suhte

Andmete saamine sideettevõtjalt (§ 35)

- (1) Politsei või seaduses sätestatud juhul muu korrakaitseorgan võib töödelda isikuandmeid, tehes kirjaliku või elektroonilise päringu elektroonilise side seaduse § 111^1 lõigetes 2 ja 3 ning § 112 lõikes 3 nimetatud mobiiltelefonivõrgus kasutatavate terminalseadmete asukoha tuvastamist reaalajas võimaldavate andmete saamiseks isiku kohta, kelle puhul see on vajalik kõrgendatud ohu väljaselgitamiseks või tõrjumiseks.

Karistusseadustik

Arvutiandmetesse sekkumine § 206

(1) Arvutisüsteemis olevate andmete ebaseadusliku muutmise, kustutamise, rikkumise või sulustamise eest

(2) Sama teo eest, kui:

1) see on toime pandud paljudes arvutisüsteemides olevate andmete vastu ja selle toimepanemisel kasutati käesoleva seadustiku §-s 216^1 nimetatud seadet või arvutiprogrammi;

2) see on toime pandud grupi poolt;

3) see on toime pandud elutähtsa valdkonna arvutisüsteemis olevate andmete vastu või

4) sellega on tekitatud oluline kahju,

Arvutisüsteemi toimimise takistamine § 207

(1) Arvutisüsteemi toimimise ebaseadusliku häirimise või takistamise eest andmete sisestamise, edastamise, kustutamise, rikkumise, muutmise või sulustamise teel

(2) Sama teo eest, kui:

1) see on toime pandud paljude arvutisüsteemide vastu ja kui selle toimepanemisel kasutati käesoleva seadustiku §-s 216^1 nimetatud seadet või arvutiprogrammi;

2) see on toime pandud grupi poolt;

3) sellega häiritakse või takistatakse elutähtsa valdkonna arvutisüsteemi toimimist või avalike teenuste osutamist või

4) kui sellega on tekitatud oluline kahju,

Arvutikelmus § 213

(1) Teisele isikule varalise kahju tekitamise eest arvutiprogrammi või andmete ebaseadusliku sisestamise, muutmise, kustutamise, rikkumise, sulustamise või muul viisil andmetöötlusprotsessi ebaseadusliku sekkumise teel varalise kasu saamise eesmärgil –

karistatakse rahalise karistuse või kuni kolmeaastase vangistusega.

(2) Sama teo eest, kui see on toime pandud:

1) isiku poolt, kes on varem toime pannud varguse, röövimise, omastamise, süüteo toimepanemise tulemusena saadud vara omandamise, hoidmise või turustamise, asja tahtliku rikkumise või hävitamise, kelmuse või väljapressimise;

2) ametiisiku poolt;

3) suures ulatuses või

4) grupi poolt,

Arvutikuriteo ettevalmistamine § 216[1]

(1) Seadme või arvutiprogrammi, mis on loodud või kohandatud eelkõige käesoleva seadustiku §-s 206, 207, 213 või 217 sätestatud kuritegude toimepanemiseks, või kaitsevahendi, mille abil on võimalik hankida juurdepääs arvutisüsteemile, hankimise, valmistamise, valdamise, levitamise või muul viisil kättesaadavaks tegemise eest, et panna ise või võimaldada kolmandal isikul panna toime käesoleva seadustiku §-s 206, 207, 213 või 217 sätestatud kuritegu

Saksamaa näide

Arvutisüsteemile ebaseaduslikult juurdepääsu hankimine § 217

(1) Arvutisüsteemile ebaseaduslikult juurdepääsu hankimise eest kaitsevahendi kõrvaldamise või vältimise teel

(2) Sama teo eest:

1) kui sellega on tekitatud oluline kahju või

2) kui juurdepääs on hangitud riigisaladust, salastatud välisteavet või ainult ametialaseks kasutamiseks ettenähtud andmeid sisaldavale arvutisüsteemile või

3) kui juurdepääs on hangitud elutähtsa valdkonna arvutisüsteemile

Riigisaladuse ja salastatud välisteabe kaitse seadus

Reguleerimisala

- sätestab riigisaladuseks oleva teabe, riigisaladuse ja salastatud välisteabe salastatuse kustumise ning salastamisaluse ja -tähtaja muutmise, samuti riigisaladuse, salastatud välisteabe ja salastatud teabekandjate kaitse korra alused ning vastutuse käesoleva seaduse rikkumise eest
- Juurde kuuluv määrus räägib ka IT-vahenditest

Vabariigi Valitsuse 20.12.2007 määrus nr 252 „Infosüsteemide turvameetmete süsteem“

Reguleerimisala

(1) Määrusega kehtestatakse riigi ja kohaliku omavalitsuse andmekogudes sisalduvate andmekoosseisude töötlemiseks kasutatavate infosüsteemide ning nendega seotud infovarade turvameetmete süsteem.

(2) Turvameetmete süsteem koosneb turvanõuete spetsifitseerimise korrast ning andmete organisatsioonilistе, füüsiliste ja infotehniliste turvameetmete kirjeldustest.

(3) Määrust ei kohaldata riigisaladust töötlevate infosüsteemide turbeks.

Reguleerimisala laiendusi

- Riigiasutused võivad nõuda ka oma partnerite käest
- Kui eraettevõtja töötleb riigi andmeid, on kohustuslik
- x-teega ühendatud süsteemide puhul on kohustuslik

Vabariigi Valitsuse 15.03.2012 määrus nr 26 „Infoturbe juhtimise süsteem“

Reguleerimisala

- (1) Määrusega kehtestatakse valitsusasutuse (edaspidi asutus) infoturbe juhtimise süsteem ning ministeeriumi kantsleri ja asutuse juhi (edaspidi asutuse juht) ja infoturbejuhi ülesanded.
- (2) Asutuse juht ja infoturbejuht juhinduvad oma tööülesannete täitmisel käesolevast määrusest, Vabariigi Valitsuse 20. detsembri 2007. a määrusest nr 252 „Infosüsteemide turvameetmete süsteem", rahvusvahelistest infoturbe halduse standarditest ja parimast praktikast.
- (3) Asutuse juht korraldab infoturbe juhtimise süsteemi rakendamise ka oma asutuse hallatavas riigiasutuses.

Isikuandmete kaitse seadus

Isikuandmete kaitse seadus

- Isikuandmed on mis tahes andmed tuvastatud või tuvastatava füüsilise isiku kohta, sõltumata sellest, millisel kujul või millises vormis need andmed on.
- Isikuandmete töötlemine on lubatud üksnes andmesubjekti nõusolekul, kui seadus ei sätesta teisiti

Delikaatsed isikuandmed (1)

- poliitilisi vaateid, usulisi ja maailmavaatelisi veendumusi kirjeldavad andmed, välja arvatud andmed seadusega ettenähtud korras registreeritud eraõiguslike juriidiliste isikute liikmeks olemise kohta;
- etnilist päritolu ja rassilist kuuluvust kirjeldavad andmed;
- andmed terviseseisundi või puude kohta;
- andmed pärilikkuse informatsiooni kohta;
- biomeetrilised andmed (eelkõige sõrmejälje-, peopesajälje- ja silmaiirisekujutis ning geeniandmed);
- andmed seksuaalelu kohta;

Delikaatsed isikuandmed (2)

- andmed ametiühingu liikmelisuse kohta;
- andmed süüteo toimepanemise või selle ohvriks langemise kohta enne avalikku kohtuistungit või õigusrikkumise asjas otsuse langetamist või asja menetluse lõpetamist.

Delikaatsed isikuandmed (3)

- Füüsilise isiku kohta kogutud statistilised andmed ei ole isikuandmed, kui puudub võimalus isikut, kelle kohta need andmed on kogutud, üheselt tuvastada.
- Delikaatsete isikuandmete töötlemine on ilma andmesubjekti nõusolekuta lubatud:
  - seaduse või välislepinguga ettenähtud ülesande täitmiseks
  - andmesubjekti või muu isiku elu, tervise ja vabaduse kaitseks

Isikuandmete töötlemise põhimõtted

- **seaduslikkuse põhimõte** – isikuandmeid võib koguda vaid ausal ja seaduslikul teel;
- **eesmärgikohasuse põhimõte** – isikuandmeid võib koguda üksnes määratletud ja õiguspäraste eesmärkide saavutamiseks ning neid ei või töödelda viisil, mis ei ole andmetöötluse eesmärkidega kooskõlas;
- **minimaalsuse põhimõte** – isikuandmeid võib koguda vaid ulatuses, mis on vajalik määratletud eesmärkide saavutamiseks;
- **kasutuse piiramise põhimõte** – isikuandmeid võib muudel eesmärkidel kasutada üksnes andmesubjekti nõusolekul või selleks pädeva organi loal;

Isikuandmete töötlemise põhimõtted

- **andmete kvaliteedi põhimõte** – isikuandmed peavad olema ajakohased, täielikud ning vajalikud seatud andmetöötluse eesmärgi saavutamiseks;
- **turvalisuse põhimõte** – isikuandmete kaitseks tuleb rakendada turvameetmeid, et kaitsta neid tahtmatu või volitamata töötlemise, avalikuks tuleku või hävimise eest;
- **individuaalse osaluse põhimõte** – andmesubjekti tuleb teavitada tema kohta kogutavatest andmetest, talle tuleb võimaldada juurdepääs tema kohta käivatele andmetele ja tal on õigus nõuda ebatäpsete või eksitavate andmete parandamist.

Isikuandmete kaitse meetmed

- Isikuandmete töötleja on kohustatud kasutusele võtma organisatsioonilised, füüsilised ja infotehnilised turvameetmed isikuandmete kaitseks:
- **andmete tervikluse osas** – juhusliku või tahtliku volitamata muutmise eest;
- **andmete käideldavuse osas** – juhusliku hävimise ja tahtliku hävitamise eest ning õigustatud isikule andmete kättesaadavuse takistamise eest;
- **andmete konfidentsiaalsuse osas** – volitamata töötlemise eest.

Meetmete valdkonnad (K,T,S)

Isikuandmete töötleja kohused:

- vältima kõrvaliste isikute ligipääsu isikuandmete töötlemiseks kasutatavatele seadmetele;
- ära hoidma andmete omavolilist lugemist, kopeerimist ja muutmist andmetöötlussüsteemis, samuti andmekandjate omavolilist teisaldamist;
- ära hoidma isikuandmete omavolilist salvestamist, muutmist ja kustutamist ning tagama, et tagantjärele oleks võimalik kindlaks teha, millal, kelle poolt ja milliseid isikuandmeid salvestati, muudeti või kustutati või millal, kelle poolt ja millistele isikuandmetele andmetöötlussüsteemis juurdepääs saadi;

Meetmete valdkonnad (OFIT)

Isikuandmete töötleja kohused:

- tagama, et igal andmetöötlussüsteemi kasutajal oleks juurdepääs ainult temale töötlemiseks lubatud isikuandmetele ja temale lubatud andmetöötluseks;
- tagama andmete olemasolu isikuandmete edastamise kohta: millal, kellele ja millised isikuandmed edastati, samuti selliste andmete muutusteta säilimise;
- tagama, et isikuandmete edastamisel andmesidevahenditega ja andmekandjate transportimisel ei toimuks isikuandmete omavolilist lugemist, kopeerimist, muutmist või kustutamist;
- kujundama ettevõtte, asutuse või ühenduse töökorralduse niisuguseks, et see võimaldaks täita andmekaitse nõudeid.

OFIT

- **O** rganisatsioonilised
- **F** üüsilised
- **I** nfotehnoloogilised
- **T** urvameetmed

Autoriõiguse seadus

Autoriõiguse seadus

- Kaitstakse teoseid (palju liike);
- teosteks pole näiteks ideed, päevauudised, faktid ja andmed
- Autori varalised õigused on võõrandatavad, isiklikud mitte
- Autor otsustab, kellel ja mis tingimustel ta oma teoseid kasutada lubab
- Autoriõigus tekib teose loomisega (vajalik tajutav väljendus) automaatselt

Autoriõiguse seadus

- Copyright, leping
- Teoste edasi levitamine, välja rentimine, avalik esitus jms on enamasti autori või levitaja poolt lepinguga piiratud
- Isiklikuks tarbeks (mitteäriliselt) tohib kopeerida (ka võrgust "tõmmata") ja sõpradega koos vaadata

- Patent **ei ole** autoriõiguste seaduses

Autoriõiguse seadus

Arvutiprogrammide erinõuded

- Ei tohi enda tarbeks kopeerida („alla tõmmata“)
- Tohib teha varukoopia

- Tohib kopeerida, tõlkida, kohandada jms programmi tööle saamiseks ja vigade parandamiseks

Autoriõiguse seadus

Arvutiprogrammide erinõuded

- Õiguspärane kasutaja tohib arvutiprogramme pöördkodeerida (reverse engineering) ühilduvuse saavutamiseks, kui vajalikku infot muidu ei saa ja pöördkodeeritakse ainult vajalikke osi
- Pöördkodeerimisel saadud infot ei tohi kasutada muuks otstarbeks kui sõltumatult loodud programmi ühilduvuse tagamiseks, üle anda teistele isikutele (v.a. ühilduvuse tagamiseks) ega kasutada konkureeriva programmi tegemiseks

Auditid

Teemad

- auditi tüübid
- auditi tegevused
- ISKE audit
- ISO 27001 audit
- OWASP
- läbistustestimine (penetration testing)
- Kuidas olla auditeeritav ja auditeerija

Miks audit?

- Audit on IT juhtimises oluliseks instrumendiks:
- Mittevastavuste õigeaegne avastamine võimaldab korrigeerivate ja preventiivsete toimingute abil leevendada IT riske

Auditi vajadus

- Preventiivne toiming, leida probleemid varakult
- Juhtkonnale vajalik kontrollimehhanism
- Tagada süsteemide töö nõuetele vastavalt
- Organisatsiooni parendamise mehhanism

Auditi eesmärk

- Auditi eesmärgiks on objektiivsete andmete kogumine selleks, et anda põhjendatud hinnang auditeeritavate süsteemide seisundile

- Auditi eesmärk sätestatakse lepingus

Audit peab olema

- Avatud
- Aus
- Konstruktiivne

- Auditeeritavale on audit alati kasulik

Definitsioonid: “kes”

- **audiitor** – isik, kellel on vajalik kvalifikatsioon ja kes viib läbi auditi
- **klient** – auditit telliv isik või organisatsioon; siseauditi puhul – ettevõtte juhtkond
- **auditeeritav** – organisatsioon, süsteem, toode või isik, mida/keda auditeeritakse

Kliendid vastutavad

- Määratlevad auditi eesmärgid ja vajadused ning algatavad auditeerimisprotsessi
- Määratlevad auditeeriva organisatsiooni
- Määratlevad auditi üldskoobi
- Saavad auditi raporti
- Määratlevad korrigeerivad toimingud (vajaduse korral)

Auditorid vastutavad

- Vastavus auditi nõuetega
- Auditi plaan
- Leidude dokumenteerimine
- Auditi tulemuste raport (aruanne)
- Korrigeerivate toimingute tõhususe verifitseerimine

Auditeeritavad vastutavad

- Töötajate informeerimine auditi eesmärkidest ja skoobist
- Vastutavate isikute määramine audiitoritega kohtumiseks
- Ressursside eraldamine audiitoritele nende töö toimivuse ja tõhususe tagamiseks
- Tagada audiitorite ligipääs kõigile vajalikele materjalidele ja isikutele
- Koostöö audiitoritega auditi eesmärkide saavutamiseks
- Korrigeerivate toimingute määratlemine ja algatamine

Auditi tüübid 1

Vastavusaudit

- Vastavusaudit kontrollib ettevõtte süsteemide vastavust auditi aluseks olevale standardile
- Üldiselt on kõik auditid suuremal või vähemal määral vastavusauditid

Auditi tüübid 2

Tulemusaudit

- Tulemusauditite põhieesmärgiks on anda hinnang auditeeritava tegevuse tulemuslikkusele.
- Tulemuslikkuse hindamine hõlmab eelkõige auditeeritava tegevuse säästlikkuse, tõhususe ja mõjususe hindamist (kas kõike koos või mõnda aspekti eraldi).
- Vajaduse korral hinnatakse ka auditeeritava tegevuse kooskõla asjakohaste õigusaktidega.

Auditi tüübid 3

- Protsessi audit (vastavusauditi ja tulemusauditi kombinatsioon)
- Finantsaudit (vastavusauditi ja tulemusauditi kombinatsioon)

auditi tegevused

- Sissejuhatav kohtumine
- Info kogumine
- Mittevastavuste registreerimine
- Mittevastavuste hindamine
- Nõuetele vastavuse määratlemine
- Tähelepanekute fikseerimine
- Kokkuvõttev/lõpetav kohtumine

Sissejuhatav kohtumine

Kohtumisel peaks osalema

- Auditi tellija (asutuse juht)
- Kõik olulisemad osapooled

Kohtumisel räägitakse läbi

- Auditi skoop ja ulatus
- Kes on partnerid
- Ajagraafik ning lepitakse kokku kohtumised
- Juhul kui, siis ka tööajad ja töökohad

Info kogumine

Kaks (teine-teist täiendavat) metoodikat

- Vaatlus („hands on“)
  - Seadmed
  - Konfiguratsioon
  - Töötlusprotsessid
- Intervjuu
  - „Kas“ küsimused
  - „Kuidas“ küsimused

Mittevastavuste registreerimine

- Sisuliselt võrdlemine auditi aluseks oleva standardiga
- Vastavalt auditi juhendile
- Vaatluse ja intervjuu põhjal otsustatakse
  - Kas standardi punkt on täidetud
  - Kuidas standardi punkt on täidetud

Mittevastavuste hindamine

- Kui leitakse mittevastavused, siis antakse hinnang, kui tõsine see mittevastavus on

Mittevastavuse gradiatsioon

- Olulised (major)
  - Standardi mingit osa on ignoreeritud
  - Võib põhjustada mittevastava toote/teenuse väljastamise
  - Protseduur, mida regulaarselt on ignoreeritud
- Väheolulised, sekundaarsed (minor)
  - **3 kuni 5** VÄHEOLULIST ühes süsteemis/protsessis võib anda OLULISE mittevastavuse

Mittevastavuse gradiatsioon

- Leiud (findings)
  - Väheoluline probleem, üksik intsident
  - Leiule peab auditeeritav reageerima
- Tähelepanek (observation)
  - Võimalus süsteemi/protsessi parendada

Tähelepanekute fikseerimine

- Kui audiitor leiab probleemi, siis ta teavitab sellest koheselt – mitteteavitamine on välistatud.
  - Leiu kohta võetakse asjasse puutuvalt töötajalt allkiri.
  - Allkiri ei tähenda probleemi tunnustamist, vaid ainult fakti kinnitust
- Kas probleem on või polnud, selgitatakse päevalõpu kohtumistel või lõppkohtumisel (final meeting)

Tähelepanekute fikseerimine

- Kui audiitor ei teavita töötajat leiust, siis leidu polnud.
- Audiitorid ei teavita juhtkonda probleemist ilma seda eelnevalt probleemiga seotud töötajatega arutamast – “fair play” põhimõttest peetakse alati kinni.

Kokkuvõttev/lõpetav kohtumine

- Vaadatakse läbi kõik leiud
- Vaadatakse läbi kõik mittevastavused
- Antakse auditeeritavale võimalus selgitada
- Selgitused dokumenteeritakse

Audit väljund

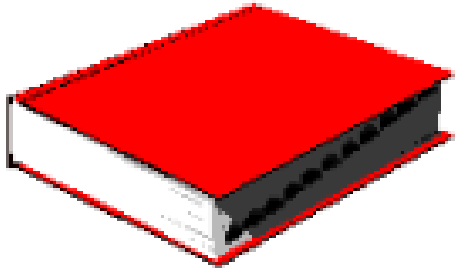
Auditi raport

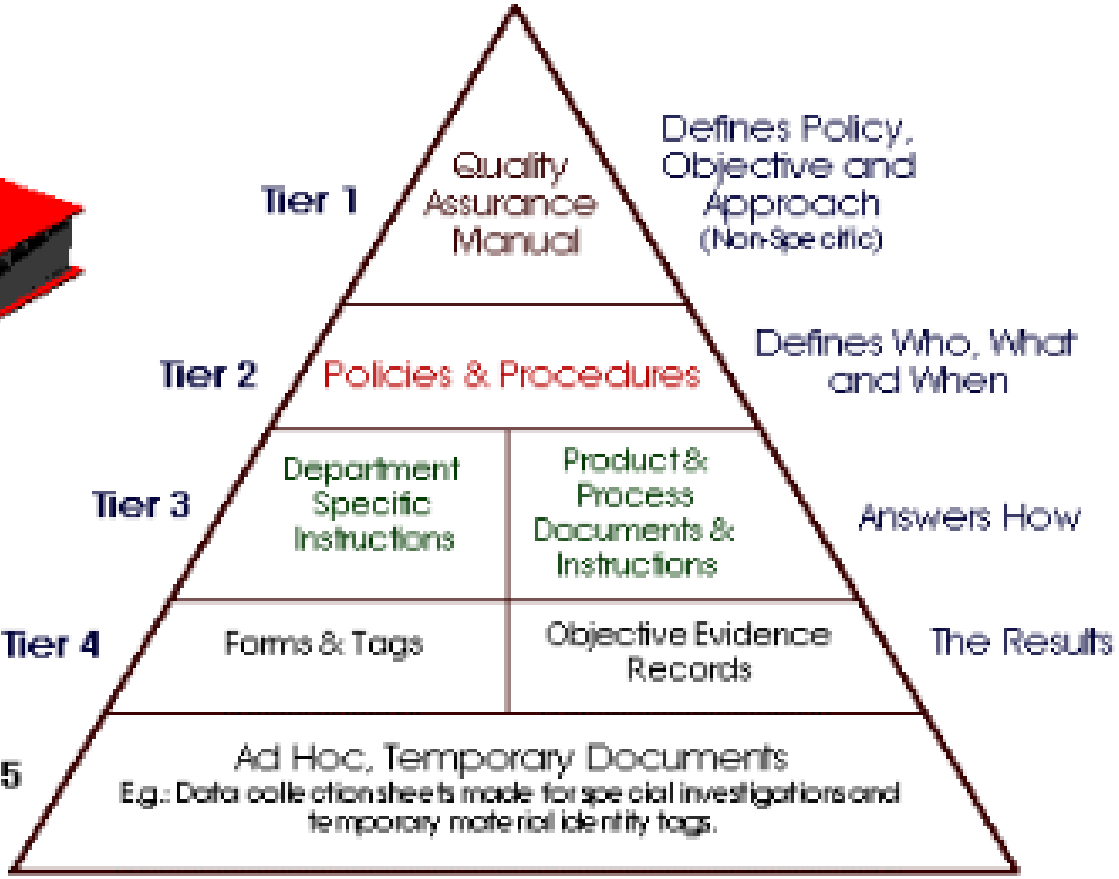
- Kes tegi
- Millal tegi
- Kuidas tegi (metoodikad)
- Mis tulemus oli
- Mida edasi teha (korrigeerivad toimingud)

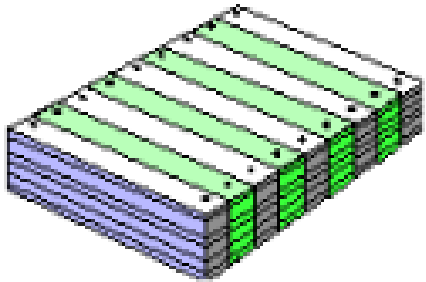
Audiitorid ei ole

- Ebaausad
- Üliaktiivsed
- Urgitsejad
- Inkvisiitorid
- Politsei
- Karistus meie pattude eest
- Auditeeritav: Ära lase ennast tabada “püksid rebadel”
- Auditeeritaval on auditist kasu – KUI AUDIT ON TEHTUD KORREKTSELT

Auditi püramiid







Erinevaid auditeid

ISKE audit

- Tüüpiline vastavusaudit
- Auditi protsessi käigus kontrollitakse kas kõik 11 sammu on korrektselt rakendatud
- Kontrollitakse kas kõik vajalikud meetmed on rakendatud
- Reaalne meetmete kontroll vastavalt audiitori valikule

ISO 27001 audit

- Vastavusaudit
- Kontrollitakse kas kõik meetmed on rakendatud
- Kontrollib, kas kehtestatud protsessid toimivad

Lisamaterjal: ISO-27001-compliance-checklist.pdf

Läbistustestimine (penetration testing)

- Võib olla ilma konkreetse metoodikata
- Põhineb testijate kogemusel
  - Käsitestid
  - Automaattestid

- NB! leping

OWASP ASVS

- OWASP – Open Web Application Security Project
- ASVS – Application Security Verification Standard (hetkel v 3.0)
- Tasemed
  - ASVS Level 1: Opportunistic
  - ASVS Level 2: Standard
  - ASVS Level 3: Advanced

OWASP ASVS Level 1

- Võimalik kontrollida automaat-testidega
- Kontrollitakse vastu OWASP Top 10 (vms)
- „Lihtne leida“ nõrkused
- Tulemuseks vastavus baastasemele

OWASP ASVS Level 2

- Lisaks automaat-testidele ka „käsitsi“ kontroll
- Vastavus tasemele 2 tähendab, et rakendatud turvameetmed on:
  - Riskidele vastavad
  - Piisavad
- Level 2 on enamikel juhtudel piisav tase

OWASP ASVS Level 3

- Väga põhjalik kontroll
- Sobib kõrge turvaastmega rakenduste puhul
  - Tervishoid
  - Pangad
  - ETO-d

ISKE audit

Auditi käigus tehtavad tööd

- kontrollida teostatud infovarade inventuuri vastavust ISKE rakendusjuhendis esitatud nõuetele;
- kontrollida turvaklasside ja turbeastmete määramist s.t. kas andmekogule on turvaklassid/turbeaste määratud asjakohaselt;
- kontrollida rakendamisele kuuluvate turvameetmete valimist s.t. kas turvameetme valik on tehtud vastavalt ISKE rakendusjuhendis esitatud nõuetest lähtuvalt;
- kontrollida kõigi rakendamisele kuuluvate turvameetmete rakendamist

Auditi käik

- Eelnevalt tutvub audiitor asutuse infoturbealase dokumentatsiooniga ning hindab, kas asutusel on olemas esmased eeldused ISKE auditi edukaks läbimiseks.
- Kui dokumentatsiooniga tutvumisel selgub, et auditi edukaks läbimiseks puuduvad vajalikud eeldused, siis soovitab audiitor ISKE auditi projektiga mitte jätkata ning anda asutusel võimalus esmased puudused kõrvaldada ning alles seejärel tellida ISKE audit;

Dokumentatsiooni läbivaatus

- Ajakohastatud infovarade inventuur
- Andmekogude kaardistamine ja neile peakasutajate määramine
- Andmekogudele turvaklasside ja turbeastmete määramine
- Muudele infovaradele turbeastmete määramine
- Rakendamisele kuuluvate tüüpmoodulite ja turvameetmete loetelude koostamine ja turvameetmete rakendamine

Turvameetmete kontroll

Kontrollitakse

- Kõiki mooduli B 1.0 meetmeid =
  - Kontrollitakse, kas kõik poliitikad on olemas, kui ei ole, siis küsitakse põhjendust
  - Kas poliitikates on kajastatud kõik meetmed, kui ei ole, siis küsitakse põhjendust
- Juhuvalimiga igast mooduligrupist kaks moodulit (kokku 10 moodulit)
- Audiitori hinnangul kaalukamad moodulid (kokku 5 moodulit)

Küsimused?