

# Riskianalüüs

Riskianalüüsi teema on tihedalt seotud andmeturbega – ka selles aines käsitletakse riskianalüüsi (laiemalt riskihaldust). Süsteemihalduse kursuses vaadeldakse riskianalüüsi lihtsalt kui üht protsessi, mida tuleb süsteemi elu mitmetel etappidel läbi viia. Ära tuuakse riskianalüüsi põhimõisted ja meetodika kirjeldus, lisaks soovitusel. Ohtude, nõrkuste ja turvameetmete detailidesse ei laskuta.

## Mis on risk?

Olenevalt alast ja olukorrast, kus terminit „risk“ kasutatakse, defineeritakse see üsna erinevalt. Enamasti on tegu mingi suurusega, mis sõltub ohu (nõrkuste tõttu ja turvameetmete kiuste) realiseerumise tõenäosusest ja tekitatud kahjust ehk toimest. Kahju/toime omakorda sõltub juhtumist puudutatud varade väärtusest. Juhul, kui neid suuruseid saab arvuliselt väljendada, siis on risk ohu realiseerumise tõenäosuse ja seeläbi tekitatud võimaliku kahju korrutis. Paraku ei saa kõike alati arvudele taandada.

## Mis on riskianalüüs?

Riskianalüüs on riskihalduse osa – see on protsess, kus hinnatakse ja kirjeldatakse süsteemi(s) varitsevaid ohte, süsteemi nõrkusi, varasid, millest süsteem koosneb, mida süsteem töötleb ja millele süsteem ligipääsu võimaldab, süsteemis rakendatud turvameetmeid, ning kõige selle läbi tuuakse (arvutatakse) välja süsteemiga seotud olulisemad riskid. Riskianalüüsi väljundit kasutatakse selleks, et neid (olulisemaid) riske sobivaid turvameetmeid rakendades vähendada nii, et nad jääksid meile sobivatesse (lubatud, etteantud) piiridesse. Tihti seatakse tehtavate kulutuste piir nii, et see oleks enam-vähem võrdne võimaliku maksimaalse kahjuga pärast nende turbekulutuste tegemist. Riskide vähendamine võib tähendada süsteemi muutmist, kasutajate teavitamist, teatud varade eraldamist süsteemist jne. Riskianalüüsi hinnangud peavad olema võimalikult täpsed ja soovitatavalt rahasummades väljendatud, vastasel juhul ei ole sellele järgnevad sammud kuigi efektiivsed.

## Riskianalüüs süsteemihalduses

Riskihaldusega seotud terminid – ohud, nõrkused, varad, turvameetmed võib süsteemihalduse seisukohalt lahti kirjutada järgnevalt:

### Ohud

Oht on süsteemi kahjustada võiva soovimatu sündmuse (turvaintsidendi) potentsiaalne põhjus. Ohtusid võib jaotada erinevate kriteeriumite alusel. Tahtluse järgi jaotuvad ohud juhuslikeks ja tahtlikeks. Kuigi enamasti nähakse ja prognoositakse lihtsamini tahtlikke ohte, näitab ajalugu, et juhuslikke ohtude põhjustatud intsidente on rohkem. Tõsi, tahtliku ohu põhjustatud sündmuse toime on tavaliselt suurema ulatusega, aga see ei ole reeglilik.

Aktiivsuse järgi saab ohud jagada passiivseteks ja aktiivseteks. Passiivse ohu põhjustatud juhtum ei muuda süsteemi ja temas paiknevaid varasid, küll aga võib mingil moel nende varade väärtust kahandada, tekitada uusi ohtusid või tuua organisatsioonile muul moel kahjusid. Aktiivse ohu põhjustatud juhtum muudab süsteemi ja/või temas paiknevaid varasid.

Ohu lähtumise alusel saab ohud jagada välisteks ja sisemisteks ohtudeks. Väline oht lähtub väljastpoolt süsteemi ja sisemine oht süsteemi seest. Jällegi pööratakse paljudel juhtumitel rohkem tähelepanu välistele ohtudele, samas kui tegelikult on sisemiste ohtude põhjustatud juhtumeid teada palju rohkem.

## **Nõrkused**

Nõrkusteks nimetatakse süsteemi ja süsteemi ümbritsevate objektide omadusi, mille kaudu saab võimalikuks ohtude realiseerumine. On oluline mõista, et nõrkused üksi ei põhjusta veel kahjusid.

Laias laastus võib tuua kahte sorti nõrkuseid: tehnoloogilised ja organisatsioonilised. Kumbagi neist võib veel edasi jaotada. Tehnoloogilised nõrkused on näiteks puudused süsteemi struktuuris või komponentides (riistvaravead, tarkvaravead), puudused süsteemi füüsilises asukohas. Organisatsioonilised nõrkused on näiteks töötajate-kasutajatega seotud nõrkused (teadmatus, vähene koolitus) ja ettevõtte korralduslikud nõrkused (mittesobiv asjaajamiseeskiri, nõrk käsuliin...).

## **Varad**

Vara on kõik see, mis omab ettevõtte ja tema klientide jaoks mingit väärtust. Süsteemihalduse jaoks on olulised varad süsteem ise (riistvara+tarkvara) ja süsteemis salvestatud ning süsteemi poolt käideldavad andmed, süsteemiväline (kuid süsteemiga seotud) andmesideressurs, süsteemi töövoime. Süsteemihalduse varadeks võib vahel lugeda ka süsteemiadministraatoreid. (Inimressursse loetakse pea alati riskianalüüsis üheks vara liigiks).

IT varade eriomadusteks on füüsilise kontakti vältimise võimalus ja andmete portatiivsus.

Ühe eripärana võib välja tuua ka seda, et tavaliselt peetakse organisatsioonides täpset arvet füüsiliste varade üle, varadele määratakse vastutavad isikud, kuid mittefüüsilised varad jäävad täiesti reguleerimata. Märkamatu võib nende mittefüüsiliste varade väärtus ületada füüsiliste varade väärtuse ja siis võib selge ülevaate ja regulatsioonide puudus valusalt kätte maksta.

## **Turvameetmed**

Turvameetmed on teguviisid, protseduurid või mehhanismid, mis võivad kaitsta ohu eest, kahandada mingit nõrkust, vähendada turvaintsidendi tekitatud kahjusid, avastada turvaintsidende ja soodustada intsidendijärgset taastamist.

Turvameetmete levinud jaotus on meetmete rakendamisvaldkonna alusel: organisatsiooniline, tehnoloogiline, füüsiline. Süsteemihaldaja peab kindlasti rohkem tähelepanu pöörama tehnoloogilistele turvameetmetele, kuna need on reeglina täielikult tema vastutusalas. Ka füüsilistest meetmetest (serveriruumi turvauksed, tulekindlus, jahutus, „Kensington“ lukud) on ettevõttesiseselt tavaliselt kõige parem ülevaade süsteemiadministraatoritel, kuid siin on vaja kaasata oma ala spetsialiste väljastpoolt. Organisatsioonilised meetmed kehtestab ettevõtte juhtkond. Kindlasti tehakse seda hästi töötavas ettevõttes kooskõlas administraatori arvamusega, aga mingil juhul ei tohi olla süsteemiadministraator see, kes omal käel organisatsioonilisi meetmeid kehtestab.

Teine, süsteemihalduri vaatepunktist loomulik jaotus, on selle järgi, millisel turvaintsidendi etapil vastavaid turvameetmeid rakendatakse: ennetavad meetmed kaitsevad ohu eest ja kahandavad nõrkusi, avastavad meetmed avastavad intsendid toimumise ajal või tagantjärele ning annavad nende kohta võimalikult täpset informatsiooni, taastavad meetmed leevendavad kahjusid ja aitavad süsteemi juhtumieelset seisu- ja töökorda taastada.

## **Riskianalüüsi meetodid**

Süsteemihalduse alases riskianalüüsis kasutatakse praegu rohkem kogemustel baseeruvaid, isekujunenud meetodeid, mida on siis erinevatesse standarditesse-juhenditesse kirjutatud ja seeläbi korrastatud. Ühtne ja selgepiiriline metoodika tihti puudub, on palju erinevaid lähenemisi, millede seast sobiva valimine raske. Samuti on vähegi suuremate süsteemide riskianalüüs väga töömahukas, ohud muutuvad ja täienevad, uusi nõrkusi ja turvameetmeid lisandub pidevalt – kõigi nendega peab kaasas käima. Siiski on märgata ka formaalsete meetodite järk-järgulist kasutuselevõttu ja riskianalüüsiga tegelevate teenusepakkujate tekkimist.

Järgnevalt on kirjeldatud erinevaid lähenemisi arvutisüsteemide riskianalüüsile. Riskihalduse üks alamülesandeid ongi sobiva meetodi valik ja oma vajadustele kohandamine. Liiga suurt täpsust taotledes kulub palju ressursse ja töö ei pruugigi valmis saada, samas aegub täpne riskianalüüs kiiresti. Liiga üldine analüüs aga ei oma märkimisväärset rakendusväärtust. Seega on meetodi valik oluline. Järgnevad meetodid ei ole alati üksteist välistavad, neid saab tihtipeale edukalt kombineerida (enamasti nii tehaksegi).

Standarditest on sobiv tutvuda EVS-ISO/IEC TR 13335 ja ISO/IEC 17799' (uue nimega ISO 27002)

## **Kvalitatiivne ja kvantitatiivne analüüs**

Kvalitatiivse riskianalüüsi puhul kasutatakse kõikide analüüsi kaasatud suuruste ja väärtuste väljendamiseks hinnangulisi tasemeid (reeglina 3-4 taset iga suuruse mõõtmiseks), nende alusel siis leitakse suurimad süsteemiga seotud riskid. Meetodi plussideks on, et lihtsam on kajastada mitterahalisi väärtuseid, protsess on väiksema mahuga ja seega kiirem (hea korduvanalüüsideks!). Miinustena võib tuua võimaliku ebatäpsuse, samuti ei ole kvalitatiivse riskianalüüsi tulemus lihtsasti rahasummadeks konverteeritav, juhtkond aga tahab tihtipeale dokumentides näha konkreetseid rahanumbreid.

Kvantitatiivse analüüsi puhul kirjeldatakse kõiki suuruseid ja väärtuseid ühtsete ühikutega skaalal, tihtipeale rahalisel skaalal. See tähendab, et ka mittemateriaalsed, mitterahalised väärtused teisendatakse mingil moel skaalale sobivateks suurusteks. Ohu realiseerumise tõenäosus tuleb arvuliselt väljendada. Selleks võib kasutada nii ettevõtte vastavat ajalugu, kui ka üldiseid, keskmisi näitajaid maailmas. Meetodi plussideks on suurem detailsus ja konkreetsete summad väljundina, miinusteks on suur töömaht ja mitterahaliste väärtuste valedhindamise oht – eriti ohtude realiseerumise tõenäosuste puhul.

## **Eeskujul baseeruv riskianalüüs (etalonturve)**

Eeskujul baseeruv riskianalüüs kasutab ära sarnaste süsteemide peal eelnevalt läbi viidud riskianalüüside tulemusi. Kasutatakse ära seda, et on palju üksteisega väga sarnaseid süsteeme: ühte neist hinnatakse detailselt ja teiste puhul saab piirduda erinevuste leidmise ja hindamisega.

Kasulik on analüüsi moodulhaaval läbi viimine: nii saab mooduleid omavahel kombineerides katta ka süsteeme, mis etalonsüsteemist üsna palju erinevad. Tüüpiline etalonmoodul koosneb mooduli tüübist, kirjeldusest, sisend- ja väljundparameetritest, tabelitest riskitasemete hindamiseks ja juhenditest, kuidas see moodul ja tema väljundid sobitada teistega. Vastavalt leitud riskitasemetele on tavaliselt antud ka turvameetmete komplektid, mida rakendama peaks.

Etalonturve kõlbab „tüüpiliste“ süsteemide analüüsimiseks, mida rohkem on analüüsitavas süsteemis unikaalseid alamosi, seda riskantsem etalonturbe tuim rakendamine on. Eesti riigiasutuste jaoks on välja töötatud infosüsteemide kolmeastmeline etalonturbe skeem ISKE, mida jõudumööda ka rakendatakse.

## **Kogemustel baseeruv riskianalüüs**

Kogemustel baseeruv riskianalüüs on kiire ja vähese vaevaga läbi viidav. Sedasorti analüüs ei baseeru mitte niivõrd ressursside ja riskide objektiivsel hindamisel, vaid administraatorite ja analüütikute kogemusel. Seega on kogemustel baseeruva riskianalüüsi õnnestumiseks vaja kogemustega läbiviijaid. Paraku on sellisel lähenemisel palju varjukülgi. Kergesti tekib piiratud maailmavaate või silmaklappide efekt: nähakse vaid seda tüüpi riske, millega ollakse seni tuttav. Saavutamata võib jääda üks riskianalüüsi põhieesmärke: selgitada välja ka administraatorile seni tundmata ohud/riskid. Samuti ei ole selline analüüs väga paindlik muutuvates oludes, kus ressursside väärtus ja riskid kiiresti muutuvad.

## **Katastroofiplaneerimine**

Katastroofiplaneerimine on teema, mis kipub süsteemide loomisel ja hooldamisel sageli ununema või kõrvale jääma. Kuni katastroof käes pole, on alati midagi „olulisemat“ teha ning selline „tühine“ teema kipub kõrvale jääma. Kuid katastroofide võimalusega arvestamata jätmine on üks suuremaid vigu, mida süsteemiadministraator teha saab.

Kuigi katastroofist rääkides mõtlevad inimesed sageli maavärinaid või üleujutusi ning Eestis neid sageli ei ole, võivad infosüsteemile katastroofiliseks osutuda palju proosalisemad sündmused: kaevetööd läbi kaablite või toruavarii serveriruumis. Seega süsteemihalduse koha pealt võiks katastroofi defineerida sündmusena, mis planeerimatult peatab või oluliselt takistab hallatava süsteemi tööd.

Kuna on võimatu üles lugeda kõiki võimalikke katastroofe, siis vaatame neid, mis mõjutavad süsteeme ning ei takista kogu organisatsiooni tööd, ehk siis jätame kõrvale hiidlained ja vulkaanipursked ning keskendume infosüsteeme mõjutavatele probleemidele.

### **Katastroofide tüübid**

Üldiselt on nelja sorti probleeme, mis võivad põhjustada infosüsteemis katastroofe:

- Riistvaratõrked
- Tarkvaratõrked
- Mitmesugused riistvara asukohast tulenevad õnnetused (toitehäired, kliima- ja keskkonnahäired)
- Inimeste eksimused

### **Riistvaratõrked**

Riistvaratõrgetest on lihtne aru saada: riistvara läheb rikki ja arvuti ei tee enam tööd. Keerulisem on aga välja selgitada see, kuivõrd ohustatud teie süsteem on, ning mida teha sellise ohu vähendamiseks ja neutraliseerimiseks.

Lihtsaim, mida teha saab, on hoida enda käepärases kohas varuriistvara. Ei maksa unustada, et see meetod toimib vaid siis, kui:

- on olemas keegi, kes oskab leida vigase riistvaratüki ning selle ära vahetada;
- käepärast on asendused just rikki läinud riistvarale.

Olenevalt kasutatavast riistvarast ja inimeste kogemustest ei pruugi vajalikud tööoskused probleemiks olla. Paljud on ise lahti võtnud oma PC-d ja seal juppe vahetanud, ning mõningate lihtsate probleemidega (näiteks PC-serveri kõvaketta tõrge) saab pea igaüks hakkama. Teadmised arvutite riistvarast tulevad alati süsteemihalduse spetsialistile kasuks, seega tasub sellised teadmised kindlasti omandada. Ühest küljest ei ole PC parandamine „raketiteadus“, ent on omad nüansid, (näiteks staatiline elekter) mille mõju teadmata võib lihtsalt seadmeid rikkuda.

Tuleb silmas pidada, et kui seadmel on garantii, või on seadmele ostetud mingi hooldusleping, siis tuleks kindlasti hoolega vaadata, mida vastavad paberid ütlevad komponentide ise vahetamise kohta.

Riistvaravarude hoidmine võib aga olla üpriski tõhus ka siis, kui te ei ole riistvaraspetsialist. Kõige olulisem on see, millist riistvara teil varutud on.

### **Mida varuda ?**

Siin ilmneb katastroofiplaneerimise sõltuvus konkreetsest keskkonnast. Kui valite, millist riistvara varuda, tuleks jälgida järgmisi punkte:

- Kui kaua tohib süsteem seista ?
- Kas on oskused vastavateks parandustöödeks ?
- Kui palju on raha varuseadmete jaoks ?
- Kui palju ruumi varutud asjad võtavad ?
- Kas samu varukomponente saab ka mujal kasutada ?

Iga vastus omab mõju sellele, mida te saate varuda. Näiteks täisvarustuses varuarvutite omamine vähendab kindlasti süsteemi seisuaega, ent on kallim, kui mälumoodulite või kõvaketaste riulis hoidmine. Teisest küljest võib selline kulu end õigustada, kui tõepoolest on tegemist väga olulise süsteemiga, mille seisuaeg toob piisavalt kahju. Kui teie asutuses on seadmed sarnase riistvaraga, on varukomponentide hoidmine kindlasti lihtsam: nii saab väheste hulga komponentidega katta suurema vajaduste spektri.

### **Kui palju varuda ?**

See, kui palju varuda, on samuti keeruline probleem, mis sõltub mitmetest küsimustest:

- Kui kaua tohib süsteem seista ?
- Kui sageli komponendid tõrguvad ?
- Kui kaua võtab aega varude uuendamine ?
- Kui palju on raha komponentide varumiseks ?
- Millised süsteemid veel kasutavad samu komponente ?

Ühest küljest, kui süsteem võib seista kuni 2 päeva, ja varuosa, mida võiks tarvis minna umbes korra aastas, on saadaval ka poest 24 tunni jooksul, siis seda varuosa ei tasu üle ühe eksemplari hoida, ning kui 24 tunni jooksul on kättesaadavus kindlustatud, siis ei maksa ehk üldse hoida.

Teisest küljest, kui süsteem ei tohi seista rohkem kui mõni minut, varuosasid läheb reeglina tarvis korra kuus, ja varude täiendamine on pikk protsess (nädalaid, vahest isegi kuid), siis tasub selliseid seadmeid varuda rohkem, näiteks kümne ringis.

## **Varuosad, mis ei ole varuosad**

Kui riistvara on kasutusel mõne madala prioriteetiga ülesannet täitvas süsteemis, võib seda vaadelda ka kui mõne tähtsama süsteemi varuosa. Ühest küljest on sellisel lähenemisel omad head:

- Varuosadele kulub vähem raha
- Riistvara töökindlus on teises süsteemis kontrollitud

Teisalt muidugi on ka omad vead:

- Vähemtähtsama süsteemi töö on häiritud
- On võimalus, et vähemtähtsama süsteemi riistvara tõrge ja tähtsama süsteemi tõrge võivad sattuda samale ajale.

Seega sellise lähenemise korral tuleb väga hoolikalt vaadata, et „vähemtähtis“ süsteem oleks ikka piisavalt väheoluline – reeglina mitteolulisi süsteeme üldse ei peetagi.

## **Hoolduslepingud ja garantiilepingud**

Hoolduslepingud muudavad riistvaratõrked kellegi teise probleemiks. Süsteemihaldur peab lihtsalt teavitama hooldajat tekkinud probleemist, ning edasi on juba nende asi probleem lahendada. On olemas ka süsteeme, mis oma tõrgetest ise hooldust teavitavad.

Tundub olevat väga lihtne, ent tegelikult on ka siin väga olulised nüansid, mis võivad teie lepingu teile lisaprobleemiks muuta.

Esimesed küsimused hoolduslepingu tegemisel on järgmised:

- Tööaeg, kellaajad päevad millal lepingut täidetakse
- Reaktsiooniaeg
- Varuosade kättesaadavus
- Maksumus
- Millist riistvara hooldatakse
- Vastutuse jaotamine

Erinevad lepingud on mõeldud erinevat sorti klientidele, ning üks oluline muutuja erinevate lepingutasemetes juures on tööaeg. Kui te just väga palju ei maksa, ei tasu ka loota, et spetsialist saabub sama kiiresti, kui kiirabi ning lahendab kõik probleemid.

Olenevalt lepingust võite avastada, et te ei saa isegi igal ajal probleemist teavitada, ning peale probleemist teavitamist tegeletakse teiega siis kui „aega on“.

Harilikud tööajad lepingutele on sellised:

- Tööpäevadel 9.00-17.00, ehk siis tavaliselt tööajal üheksast viieni.
- Tööpäevadel, aga laiendatud tööajaga (näiteks 12 või 18 tundi)
- 24/7 ehk iga päev ja igal ajal.

Mida suurem on tööaeg, seda kallim on leping.

Tuleb silmas pidada, et kui on tarvilik kliendipoolne sekkumine(probleemidest teavitamine, samuti ligipääs seadmetele) peab see kliendipoolne sekkumine olema tagatud lepingu tööajal, muidu on laiendatud tööaja kasutamine suhteliselt mõttetu. Näiteks, kui ostate 24/7 tööaja, aga serveriruumi pääsevad ainult valitud spetsialistid, kelle tööaeg on 9.00-17.00, siis on selge, et 24/7 leping jääb täitmata kliendi suutmatuse tõttu.

Peale tööaja on veel väga oluline muutuja reaktsiooniaeg, ehk aeg millal teie probleemiga tegelema hakatakse, ning mis ajaks probleem lahendatud peab olema. Mida lühem on reaktsiooniaeg, seda kallim on ka leping.

Lisaks hinnale seavad ka looduseadused reaktsiooniajale omad piirid. Näiteks Tartus on raske saada Tallinnast osutatavale riistvara hooldusteenusele alla 4-tunnist reaktsioonaja-lisa. Tavaliselt on selline kauguse punkt ka juba lepingus sees, ühest küljest võib see hinda tõsta (on mingi kilomeetritasu) ning teisest küljest pikendada reaktsiooniaega. 4-tunnised reaktsiooniajad on praeguses praktikas juba suhteliselt kiired ning tavalised on hoolduslepingud, kus reageerima peab järgmisel tööpäeval.

Lisaks tuleb silmas pidada seda, mida reaktsiooniaeg konkreetses lepingus tähendab: kas probleemiga hakatakse tegelema, ning teie probleemile tuleb vastus siis, kui tuleb, või tähendab see tõepoolest seda, et selle aja jooksul on teile komponent kohale toodud ning ka ära vahetatud.

Üldiselt on raha see, mis määrab ära, millise hoolduslepingu saate sõlmida. Piirid, millises mahus või millise raha eest on hooldust mõistlik osta, määrab riskianalüüs.

Hooldatava riistvara täpne valik aitab kõige enam hoolduskulusid vähendada. Ühest küljest tuleb kindlasti realistlikult hinnata, millisele seadmele on millist hooldust tarvis, mis temast sõltub ning kui oluline on see sõltuv süsteem. Teisest küljest tuleb silmas pidada, et kogu tööks vajalik riistvara oleks kaetud: mida keerulisem on süsteem, seda lihtsam on sellel alal eksida.

## **Tarkvaratõrked**

Tarkvaratõrked võivad samuti teie süsteemi jaoks tõsiseks probleemiks osutuda. Ilmselt on kõik arvutikasutajad kokku puutunud probleemiga, et kas arvuti „kiilub kinni“ või rakendus paneb ennast ise kinni. Selliseid probleeme võib juhtuda ka teie süsteemiga, ning olenevalt olukorrast võivad need tõrked olla väga tõsiste tagajärgedega.

Tarkvaratõrked võib jagada põhiliselt kaheks:

- Operatsioonisüsteemi tõrked
- Rakendustarkvara tõrked

Nendel tõrkeliikidel on erinev mõju ja ka erinevad lähenemisviisid probleemide lahendamisele.

### **Operatsioonisüsteemi tõrked**

Operatsioonisüsteemi tõrked mõjutavad tavaliselt kõiki arvutis rikke ajal töötavaid programme ning võivad varieeruda mingi riistvara töö katkemisest totaalse seisakuni, vead operatsioonisüsteemis võivad kaasa tuua ka andmekadu. Probleemid võivad olla põhjustatud nii valedest seadistustest kui ka konkreetsest veast tarkvaras.

Operatsioonisüsteemi vigu on keeruline lahendada, kuna tegemist on ikkagi väga spetsiifilise alaga. Tavaliselt aitab vea vastu tarkvaraparandus, aga kui teie tarkvaratootja seda ei tee, või läheb selle tegemisega aega, siis tuleb kasutada teisi lahendusi.

Nii näiteks on võimalik, et probleem on mingi kindla riistvakomponendi juhtprogrammis, sel juhul võib proovida (ajutist) riistvara vahetust.

Samuti on võimalik, et mingite operatsioonisüsteemi parameetrite muutmisega viga teie puhul ei avaldu (mingid puhvid ei saa täis vms). Muidugi, selliseid parameetreid seades peate kindlasti teadma, mida te teete, muidu võib situatsioon halvemaks minna.

### **Rakendustarkvara tõrked**

Siin on tegemist juba konkreetse programmi enda vigadega, ka siin võivad vead varieeruda töö (osalisest või täielikust) katkemisest kuni andmete rikkumiseni. Samuti võivad probleemid olla tingitud nii tarkvara vales seadistusest, väärkasutusest kui ka tarkvara vigadest. Kui operatsioonisüsteemi viga halvab kogu süsteemi töö, siis rakendustarkvara tõrke puhul võib osa süsteemi funktsionaalsusest ka säilida.

Parandamiseks on tarvilik jällegi parandus tarkvaratootjalt, ent võimalik on ka mitmesuguste nn. kõrvalteede kasutamine: mitte kasutada mingit kindlat funktsionaalsust, või saavutada seda teistmoodi.

### ***Toide, ruumid, kliima, välised tegurid***

Peale infosüsteemi otseste komponentide (riistvara, tarkvara) võivad probleeme tekitada ka välised tegurid. Kui tarkvara ja riistvara töötavad suurepäraselt, võib probleem tulla hoopis mujalt: seadmete asukohast.

Seadmete asukohas on seadmetele neli põhilisemat ohutegurit:

- ruumide olukord
- elekter
- kliima
- ilm ja muud välised tegurid

### **Ruumide olukord**

Reeglina on ka serveriruumid või arvutiruumid tavalised toad majas ning raske on ette kujutada seal mingit tõsist probleemi, kuna Eestis reeglina maavärinaid pole ja seinad seisavad kindlalt. Siiski, kuna arvutustehnika on oma spetsiifiliste nõudmisega ka ruumile, võivad sellised seadmed kahjustuda tunduvalt pisematest probleemidest.

Nii näiteks võib suur tolmu- ja saepulvisaldus õhus rikkuda seadmeid, näiteks lindiseadmete ja ka ventilaatorite tööga lühendab suur tolmu- ja saepulvisaldus tunduvalt. Seadmetesse ladestuv tolm vähendab ka jahutuse efektiivsust.

Samuti mõjutavad seadmeid suure amplituudiga kiired temperatuurikõikumised: külmadele pindadele võib kondenseeruda veeaur ja see võib seadmeid rikkuda (seetõttu ei tasu ka pikka aega õues olnud ja allapoole kastepunkti jahtunud seadmeid kohe vooluvõrku lülitada).

Veel on oluline seadmeruumide turvalisus inimeste seisukohast: kogu ruum peab olema vajalikul määral kaitstud, võtmed kindlatel isikutel jne.

Veeõnnetused võivad lihtsalt rikkuda suures koguses seadmeid, seetõttu on oluline näiteks see, et seadmeruumides ei oleks radiaatoreid ja kanalisatsiooni- ning veetorusid.

Tulekahjude puhuks võiks seadmeruumides olla gaaskustutus, kuna automaatne veekustutus rikub seadmed. Tule leviku piiramiseks tasub kasutada kõrgema turvaklassiga uksi ja tulelukkudega ventilatsiooni.



Erinevatel tootjatel võivad olla oma nõudmised seadmeruumidele: tavaliselt on ära toodud nõuded temperatuurile, vibratsioonile ja õhuniiskusele. Ka kallimates riistvara hoolduslepingutes või teenustaseme lepingutes võivad sisalduda nõuded seadmeruumidele.

## **Toitehäired**

Elekter on tuntud probleemide allikas, ning Eesti tingimustes esineb nii üle- kui alapingeid ning volukatkestusi. Olenevalt asukohamaast või siis ka teenindavast firmast võib elektri kvaliteet varieeruda, on ka selliseid võimalusi, et elektritoide on teenindava firma poolt garanteeritud.

Reeglina see siiski nii ei ole, ning elektritoide on heal juhul garanteeritud mingites piirides, ütleme 97 % ajast ja teatavate lubatud pingekõikumiste raames. Lisaks pinge kõikumisele või puudumisele mõjutavad arvuteid ka muud häired elektrivõrgus: kõrvalekalded sinusoidsest lainekujust, häired sageduses, äkilised ülepinged (äike).

Seetõttu tulebki seadmeruume/seadmeid varustada katkematu toitepinge allikatega (UPS), elektrigeneraatorite jms seadmetega, mis kaitsevad seadmeid elektrivoolu probleemide eest.

Vajadused elektrivoolu kestvusele ning kvaliteedile võivad suuresti varieeruda, varieerub ka sobivate kaitsevahendite hulk:

- Kaitse hetkeks: kaitse ülepingete jms tugevate seadmeid otseselt kahjustavate toitehäirete eest. Selles vahemikus on saadaval kaitsmed jms, osaliselt võib kaitsta ka elektritarbijatelt nõutav infrastruktuur, kuid reeglina on sellised seadmed arvututehnika kaitsmiseks liialt aeglase reaktsioonijaga ning ülepinge pääseb seadmeid kahjustama.
- Kaitse mõneks minutiks: enamus volukatkestusi langeb sellesse vahemikku, 1-30 minutit, see on aeg, mille jaoks on saada UPS'id.
- Kaitse mõneks tunniks: sellises suurusjärgus on vajalikud juba elektrigeneraatorid. Varuda tuleb ka kütust generaatoritele.
- Kaitse päevadeks ja nädalateks: reeglina tasub kolida sinna, kus on paremad tingimused või ehitada oma elektrijaam :)

Vastavalt teie asutuse vajadusele tuleb otsustada, kas elektritoide peab tuleb garanteerida pidevalt, ning kasutada elektritootmise seadmeid, või piisab sellest, et seadmete töö on garanteeritud vaid mingi aja jooksul, mis on piisab seadmete töö korrektseks lõpetamiseks. Tegelikult on Eesti tingimustes korralik UPS normaalse töö eeltingimuseks, ning eelkõige on tarvis ikkagi sellist UPSi, mis alati ka pinge ja sageduse normis hoiab. Samuti ei maksa unustada, et ka UPSi akud on kindla eluaega ning neid tuleb regulaarselt vahetada.

Juhul, kui teil on vajalik pidev toide, ning otsustate generaatori kasuks ei maksa unustada, et generaatorit ajab reeglina ringi diisel- või bensiinimootor, mis vajab regulaarset hooldust, kütust ning testimist.

Nii UPSid kui generaatorid tuleb valida vastavalt oma seadmete volutarbele. UPSide puhul on lisaks veel oluline, kui kauaks peab elektrivool peale volukatkestuse algust säilima. Võimsamad ja pikema kestvusega UPSid peavad maksavad ka rohkem.

## **Kliima**

Ka kliima mõjutab arvutustehnikat väga tugevalt. Liiga kõrge temperatuur on kõige tavalisem põhjus kõvaketaste enneaegseks riknemiseks. Jahutusseadmed on olulised serveriruumi komponendid, mis tagavad, et arvutustehnika töötab õigel temperatuuril. Maja üldine soojus ning arvutite endi poolt genereeritud soojus tagab üldiselt selle, et temperatuur püsiks piisavalt kõrgel.

Jahutusseadmete hooldamine on reeglina keerukas, nii ei maksa selliseid seadmeid ise hooldada, vaid tasub palgata kliimaseadmete hooldamiseks spetsiaalne firma.

Jahutusseadmed on tavaliselt ka suure voolutarbimisega ning serveriruumi elektrivoolu planeerimisel tuleb sellega arvestada. Mõelda tuleb ka selle peale, et kui kasutame elektrikatkestuse puhul generaatorit, mis võib avariitoidet pakkuda tundide või päevade kaupa, siis tuleb ka jahutusseadmeid toita avariitoidest – vastasel juhul on meil küll seadmetele vajalik toide, kuid ülekuumenemise tõttu me seadmeid siiski kasutada ei saa.

## **Ilm ja muud välised tegurid**

Kuigi ilma parandamiseks suurt midagi ette võtta ei saa, tuleks arvestada ka ekstreemsete välistingimuste mõju. Näiteks ei pruugi kinnituisanud teid pidi olla võimalik pääseda serveriruumini ning samuti võib tuisk ja jäätumine takistada kliimaseadmete välismoodulite tööd. Tugevad tuuled võivad lõhkuda elektriliine ning mõnikord ka maju. Üleujutuste puhul võib vee alla sattuda ka keldris asuv seadmeruum.

## ***Inimfaktor***

### **Lõppkasutaja vead**

Lõppkasutajatete eksimused on kõige tavalisemad, kuna reeglina on lõppkasutajaid süsteemis kõige rohkem. Reeglina on lõppkasutajate vead aga väikese mõjuga, kuna nende õigused süsteemi mõjutada on piiratud. Kõige tavalisem on see, et lõppkasutaja põhjustab vea oma rakenduse ebaõige kasutamisega.

Kõige tavalisemad probleemid on seotud andmete rikkumisega: fail kirjutatakse üle, sisestamisel eksitakse, faile kustutatakse.

Nimekiri probleemidest, mille põhjustavad lõppkasutajad on tegelikult lõputu, ning probleeme võib esineda väga erinevaid, sõltuvalt nii rakendustest kui kasutajatest.

Lõppkasutajate probleemi ei saa täielikult lahendada, kuid kindlasti saab seda vähendada. Eelkõige on siin kolm meetodit, mis tõhusaid tulemusi omavad:

- Kasutajate harimine. Kasutaja peaks teadma, mida nad teevad, millist mõju nende tegevus avaldab süsteemile ja andmetele.
- Kasutajate õiguste piiramine. Vastavalt oma süsteemi võimalustele tuleb kasutajatele anda ligipääs andmetele vastavalt vajadusele, ehk siis nii palju kui vaja ja nii vähe kui võimalik.
- Varukoopiad. Andmete hävimise ning eksliku muutmise eest kaitseva kõige paremini varukoopiad. Varukoopiaid tuleb teha regulaarselt ning hoida sellises kohas, kust neid ruttu kätte saab.

### **Süsteemioperaatorite vead**

Süsteemioperaatorid on reeglina tavalistest kasutajatest teadlikumad, ning seetõttu teevad harvem vigu. Kuid neil on ka suuremad õigused, nii on eksimuse potentsiaalsed kahjud suuremad. Operaatorid viivad protseduure läbi etteantud juhendite põhjal ja seetõttu on operaatorite vead sageli põhjustatud just eksimustest juhendites.

Operaatoritel peaks olema juhendid kõikide nende poolt läbi viidavate operatsioonide jaoks. Muidugi ei pruugi operaatorid neid juhendeid järgida ning juhendite mittejälgimisel võivad olla ka omad põhjused:

- vigased juhendid: juhendid on kas aegunud (nuppe pole enam tarkvaras, kirjadon teised) või ei kata vajalikku funktsionaalsust
- operaatori suutmatus või soovimatus.

Sõltuvalt probleemist tuleb erinevalt läheneda: kas juhendeid parandada või rakendada meetmeid operaatori suhtes.

Lisaks sellele võib operaator operatsioone läbi viies ka eksida, inimesed on ekslikud ning sellega tuleb arvestada. Sellisteks puhkudeks on oluline, et operaator või keegi teine kontrolliks läbi viidud protseduure ning vea puhul teavitataks vajalikke inimesi.

## **Süsteemiadministraatorite vead**

Süsteemiadministraatorid tegelevad eelkõige süsteemide hooldamisega, ning seetõttu on neil ligipääs süsteemi kõikidele osadele ning võimalus ka mõjutada süsteemi kõikide osade tööd. Süsteemiadministraatorid peavad sageli läbi viima protseduure ilma korrektsete juhenditeta.

Suurte õiguste tõttu on süsteemiadministraatoritel tavaliselt võimalus peatada terve süsteemi töö – ning võimalus seda teha ka eksituse tõttu.

Üks võimalus süsteemi tööd tõsiselt segada on eksida süsteemide seadistamisel: nii on näiteks võimalik andmeid hävitada (näiteks andmete salvestamisel mälu kettale), samuti muuta süsteem aeglaseks (mingi ressursi puudus) ning paljudel muudel viisidel tööd häirida.

Arvestades muidugi dokumentatsioone ning eri operatsioonide läbiviimisel vajalikke teadmisi võib tegelik vigade vähesus olla üllatav. Dokumentatsioon kipub sageli olema segane ning puudulik ja muudatuste mõju ei pruugi olla alati täpselt prognoositav.

Rakenduste ja süsteemide ümberseadistamise protsess on väga oluline süsteemiadministraatorite vigade ja nende mõju vähendamisel.

Ümberseadistamise protsess on kasulik kirja panna reeglitenä, kuidas protsessi läbi viiakse. Sellised reeglid aitavad süsteemiadministraatoritel silmas pida, kas kõik organisatsiooni seisukohalt olulised aspektid on kaetud.

Samuti võivad süsteemiadministraatorid eksida ka regulaarsete ja igapäevaste operatsioonide läbiviimisel. Võimalused on eksimiseks on väga laiad, ning vead ei pruugi ilmnedä sugugi kohe.

Süsteemiadministraatorite vigade eest kaitsevad süsteemi eelkõige varukoopiad, ning sealjuures mitte ainult andmetest, vaid ka programmide ja seadistutest – sh. ka riistvara seadistustest.

## **Varundus**

Varundus on igasuguste katastroofiliste situatsioonide lahendamisel mõõdapääsmatu komponent, kuna reeglina tähendab katastroof ikkagi andmete hävimist. Seetõttu tuleb varundust väga tähelepanelikult plaanida et varundusest ka reaalselt kasu oleks. Nii tuleks hoida varundatud andmeid peale varundusseadme vahetu läheduse ka mujal, tagamaks andmete säilimise ruumi(de) füüsilise hävimise korral.

Kindlasti tuleb kontrollida regulaarselt varunduse toimimist ja taastamise toimimist: ainult nii saate kindel olla, et ka katastroofide puhul taastamine õnnestub.

## **Katastroofiplaan**

Katastroofiplaan on juhend selle kohta, kuidas käituda süsteemiga ilmnevate probleemide puhul. Katastroofiplaan aitab säilitada külma verd ning tagada mõtestatud tegevuse ka suurte probleemide korral.

Algatuseks sobib hästi see, et kujutate ette et teie seadmeruumi koos selles olevate seadmetega pole enam, ning teie ülesanne on kogu süsteem uuesti käima saada.

Katastroofiplaanis võiks olla vähemalt järgmised punktid:

- Millised sündmused tähendavad katastroofi teie süsteemi jaoks.
- Kes omab õigust käivitada katastroofiplaan, ehk kes on need inimesed, kes süsteemi seisundi võivad kuulutada katastroofiliseks.
- Kõikide osapoolte rollid ja kohustused.
- Nimekiri vajalikest seadmetest süsteemi käivitamiseks, andmed nende olemasolu ja asukoha kohta.
- Ülevaade süsteemi käivitamiseks vajalikest andmetest.
- Inimeste tööplaanid, kavad, kes keda millal asendab jne.
- Kuidas ja kuhu moodustada ajutised seadmeruumid.
- Plaan, kuidas viia süsteemi töökeskus üle ajutisest seadmeruumist (uude) seadmeruumi.

Katastroofiplaanid võivad muutuda väga mahukateks, kui kõike seda väga detailselt kirja panna. Samas on detailsus vajalik, kuna tõsise katastroofi korral võib plaan olla ainus asi, mis teie süsteemist järel on (peale varukoopiate).

Katastroofiplaanid tuleks hoida mitmel kujul – nii elektroonilisel kui kindlasti ka paberkujul, kuna tõsise probleemi puhul ei pruugi te enam elektroonilisi dokumente kätte saada. Samuti tuleks katastroofiplaane hoida mitmes kohas – nii on garanteeritud nende säilimine. Nii näiteks tasub neid hoida samades kohtades, kus hoitakse varundusmeediat.

Peale katastroofiplaani väljatöötamist tuleks seda kindlasti testida. Sõjaväes nimetatakse sellist asja õppuseks ning nagu sõjaväes, kehtib ka siin reegel, et „raskem õppustel, kergem lahingus“. Tavaliselt küll ei tehta katastroofiplaani 100% ja täies mahus läbi vaid imiteeritakse osalises mahus, millest peaks siiski piisama tõestamiseks, et teie plaan töötab (ka sõdurid ei alusta õppuse jaoks sõda).

## **Taastestrateegiad**

Katastroofist taastumisel (katastroofiks valmis olemiseks) võib kasutada erinevaid taastestrateegiaid, mis määravad ära, milliseid varusid me hoiame, kuhu varuruumidesse süsteemi käima paneme, jms.

Võib rääkida järgmistest taastevalikutest (strateegiatest):

- ei taasta midagi (Do Nothing)

Kui teenuse katastroofijärgne jätkamine ei oma mõtet (vähem kasutajaid, parem alternatiiv, majanduslikult üle jõu käiv), siis võidakse otsutada, et süsteemi ei taastata. See valik eeldab kokkulepet kliendiga.

- ajutine lahendus (Manual Workaround)

Kui teenuse taastamine (teiste valikute abil) võtab aega, võib äripoolle töö (väiksemas mahus, hädavajalikud toimingud)seni jätkuda ilma IT teenuseid kasutamata.

- vastastikune hädaabi (Reciprocal Arrangement)

Asutused võivad omavahel kokku leppida, et aidatakse üksteist vastastikku süsteemikatastroofide puhul (pakutakse pinda serveritele, oma võrguühendust, jms).

- külmad varud, reserv (Cold Stand-by, Gradual Recovery)

Selle strateegia puhul on olemas sobiva infrastruktuuriga (võrk, elekter, jahutus) ruumid, kuid pole seadmeid (riistvara) ega ka tarkvara. Seadmed tuleb hankida, tarkvara paigaldada ja seadistada, andmed varukoopiatelt taastada. Taasteaeg külma strateegia puhul on reeglina üle 72h

- soojad varud, töövalmis reserv (Warm Stand-by, Intermediate Recovery)

Olemas on kõik, mis külma strateegia puhul, lisaks ka vajalik riistvara ja paigaldatud baastarkvara. Teenuse taastamiseks on vaja seadmed ja tarkvara seadistada ning taastada andmed varukoopiatelt. Taasteaeg 24h-72h

- kuumad varud, töötav reserv (Hot Stand-by, Immediate Recovery)

Kuuma taastestrateegia puhul hoitakse pidevalt käimas olemasoleva süsteemi identset koopiat. Tegu võib olla koormust jagavate paralleelselt töötavate süsteemidega. Katastroofi korral võtab varusüsteem töö üle. Taasteaeg <2h, kui andmed on reaalajas replitseeritud. Taasteaeg <24h, kui on vaja andmete taastamist varukoopiatelt.