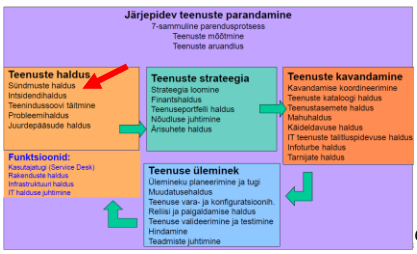
Teenuste käitlemise protsessid

Sündmuste haldus

Event Management

Loeng 2

Teenuste haldus



Primary source: Service Operation

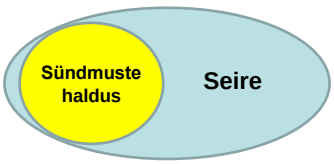
Guido Leibur

Mõiste, eesmärk ja käsitlusala

Sündmuseks nimetatakse iga tuvastatavat juhtumit millel on oluline seos IT teenuste haldamise ja tarnega ja mis iseloomustavad kõrvalekallet tavapärasest. Tüüpiliselt on sündmused teated või alarmid, mis luuakse IT teenuste halduse, konfiguratsioonielementide või seiretööriistade abil.

Eesmärk
Tagada tõhus sisend IT teenuste halduseks, kus õigeaegselt avastatakse võimalikud ohud ja kõrvalekalded teenuste kvaliteedis.

Käsitlusala
- konfiguratsioonielemendid
- keskkonna tingimused
- tarkvara litsentside optimaalne jaotus
- turvasündmused
- tavategevused



Seire (*Monitoring*) – tegeleb kõigi sündmustega
Sündmuste haldus – tegeleb meile tähtsate kõrvalekalletega tavapärasest

Guido Leibur

Olulisus ärile, sündmuste tüübid

Sündmuste halduse mõju ärile on peamiselt **kaudne**. Sündmuste haldus võimaldab:
- tagada intsidentide varajase avastamise,
- vähendada mahukat seiret
- parandada mahu- ja käideldavuse halduse protsesse “pudelikaelade” õigeaegse avastamise kaudu
- automatiseerida teatavaid haldustegevusi jne

Sündmuste tüübid:

1) **Informatiivsed sündmused** (tööülesanne on teostatud, kasutaja on mingisse rakendusse sisse loginud, e-mail on kohale jõudnud jne)
2) **Hoiatavad sündmused** (kasutaja üritab rakendusse sisse logida vale parooliga, protsessi koormus on ohtlikult kõrge, tööjaama skaneerimine avastas keelatud tarkvara kasutamise jne)
3) **Erandlikud sündmused.** Tihti on siis vajadus olukorda täpsemalt analüüsida (serveri mälu kasutus on tõusnud 95%-le, transaktsiooni teostamise aeg on 10% suurem lubatust, teenuse osutamine on katkenud jne)

Olulised põhimõtted

1) Sündmuste teated peavad minema ainult neile isikutele, kellele need on olulised
2) Sündmuste haldus peab olema tsentraliseeritud mõistlikul määral
3) Kõik teated peavad (võimalusel) olema standardiseeritud
4) Sündmuste käsitlemine tuleks maksimaalselt automatiseerida
5) Kõik olulised sündmused tuleb salvestada
6) Olulistele sündmustele tuleb rakendada korrelatsioonanalüüsi

Protsessi kirjeldus 1

1. Sündmuse toimumine

   Mitte kõiki sündmusi ei avastata ja ei registreerita. Milliseid sündmusi soovitakse hiljem hallata – see tuleb eelnevalt kokku leppida (tavaliselt kavandamise (*Disain*) faasis).

2. Sündmuse teate tekitamine

   Enamus konfiguratsioonielemente (CI) on kavandatud sellistena, et nad on võimelised selliseid teateid tekitama. Seda tehakse kas:
   - küsitlemise kaudu (tsentraalse haldusvahendi poolt)
   - sündmus tekkib konfiguratsioonielemendis teatavate tingimuste täitmisel.

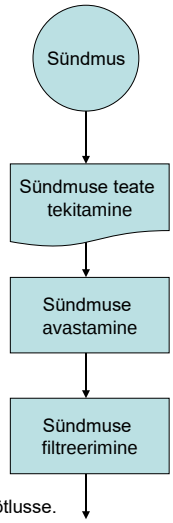
   Suur osa CI on võimeline genereerima sündmusi avatud protokollis SNMP.

3. Sündmuse avastamine

   Pärast teate tekitamist see fikseeritakse tavaliselt sama (avastanud) süsteemi poolt või tsentraalse sündmusi fikseeriva haldusvahendi poolt.

4. Sündmuse filtreerimine

   Sündmuste filtreerimise eesmärk on tõkestada ebaoluliste sündmuste jõudmine järgnevasse protsessi. Ignoreeritud sündmused tuleb ka logida. Filtreerimist võib kasutada ka selleks, et ainult esimene (-sed) sündmused jõuavad järgnevasse töötlusse.



Protsessi kirjeldus 2

5. Sündmuse olulisus

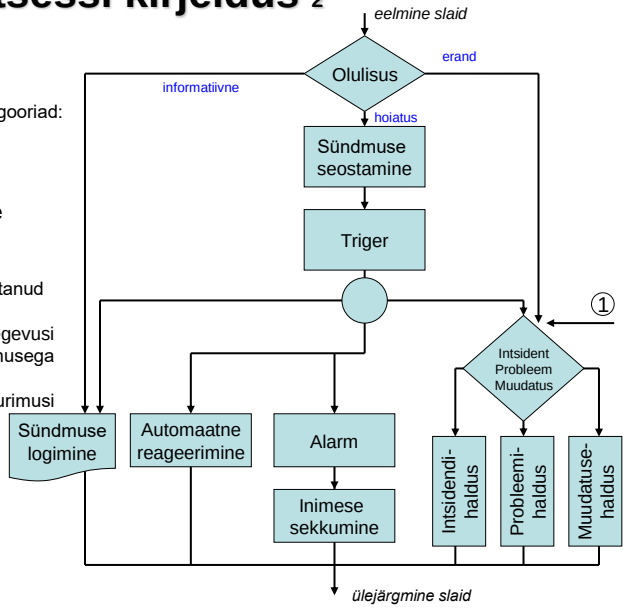
   Soovituslikud sündmuse kategooriad:
   - informatiivne
   - hoiatus
   - erand

6. Sündmuse seostamine

   Võetakse arvesse näiteks:
   - sarnaste sündmuste arvu
   - CI arvu, millised on põhjustanud sarnaseid sündmusi
   - kas mingeid varasemaid tegevusi saab seostada selle sündmusega
   - kas sündmus on erandlik
   - kas mingeid täiendavaid uurimusi on vaja teostada
   - sündmuse prioriteetsuse seadmine jm

7. Triger

   Mehhanism, kus algatatakse reageerimine sündmusele.



Protsessi kirjeldus 3

8. Reageeringu valik

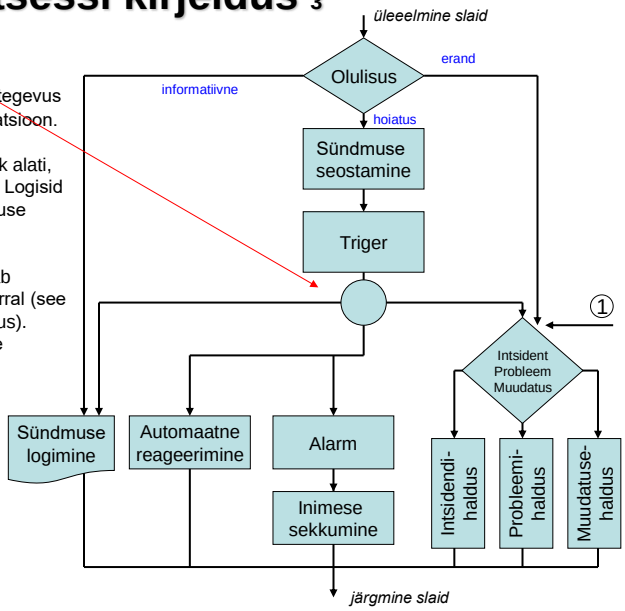
Reageering võib olla üks kindel tegevus või erinevate tegevuste kombinatsioon.

Sündmuste logimine on kasulik alati, sõltumata muudest tegevustest. Logisid kasutatakse tihti täpse vea põhjuse määratlemiseks.

Automaatset reageerimist saab kasutada hästi tuntud vigade korral (see on hea probleemihalduse tulemus). Näiteks teenuse taaskäivitamine (*restart*).

Alarmi ja inimese sekkumist rakendatakse juhtudel, kus automaatset reageerimist ei saa rakendada.

Intsident, probleem või muudatus võib olla kas eraldi või üheaegselt olla avatud ühe sündmuse jaoks.



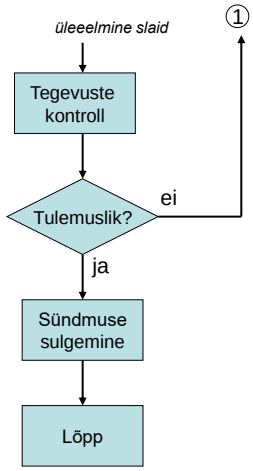
Protsessi kirjeldus 4

9. Tegevuste kontroll

Tähtis on tuhandete sündmuste seas kontrollida olulisi. Tihti saab kontrolli teha automaatselt, kuid seda tuleb teha ka käsitsi. Kui sündmused on üle antud intsidendi-, probleemi-, muudatusehalduse või mõnele muule protsessile, siis on oluline, et vastavaid tegevusi ei dubleeritaks. Kontrolli kasutatakse ka sündmuste halduse protsessi parandamiseks.

10. Sündmuse sulgemine

Paljude automaatprotsesside juures toimub sündmuste avamine ja sulgemine automaatselt.
Kui sündmus on üle antud mõnele teisele protsessile (näit intsidendihaldus), siis võib ta sündmuste halduse protsessis sulgeda.

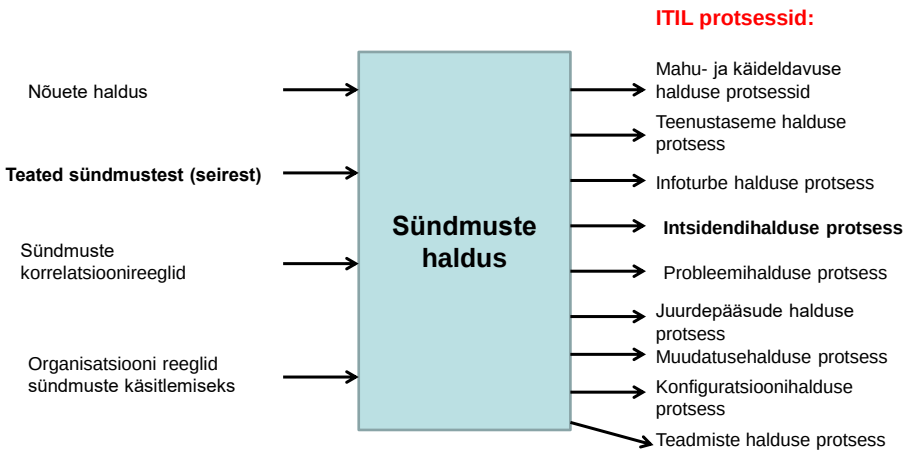


Sündmuste algatajad

Sündmuse algataja võib olla suvaline muutus. Tähtis on eristada meile olulisi sündmusi. Olulise sündmuse trigeriks võib olla:

- erandid suvalisele varem määratletud konfiguratsioonielemendi toimimisele,
- erandid IT automaatprotsesside (protseduuride) töös,
- erandid äriprotsesside töös, millised on sündmuste halduse monitooringu all,
- automatiseeritud tööülesannete lõpetamine,
- staatuse muutus seadmete või andmebaaside kirjetes,
- kasutajate või automaatprotsesside poolt rakendustele või andmebaasidele ligipääs,
- olukord, kus seade, andmebaas, rakendus vm on saavutanud varem määratletud läve

Liidesed teiste protsessidega



Informatsiooni juhtimine

Sündmuste halduses kasutatav oluline informatsioon on:

- SNMP sõnumid (IT infrastruktuuris kasutatav standardne moodus *CI* olekuinfo vahetamiseks),
- eri tarnijate seirevahendite sündmused,
- eri sündmusi seostavad mehhanismid,
- sündmuse kirjeldamisel ei ole selle salvestamiseks ühtset standardit. Samas peaks iga sündmust kindlasti kirjeldama vähemalt järgmiste andmetega:
  - seade
  - komponent, konfiguratsioonielement
  - tõrke tüüp
  - aeg
  - lubatud erisused
  - soovituslik väärtus jt

Meetrika

Meetrika näited:

- sündmuste arv eri kategooriates
- sündmuste arv olulisuse alusel
- sündmuste (suhte)arv, kus oli vajadus inimese sekkumiseks
- sündmuste (suhte)arv, mis viisid intsidentide või muudatusteni
- korduvate sündmuste (suhte)arv
- sündmuste (suhte)arv, mille põhjustajaks oli jõudlus
- sündmuste (suhte)arv, mille põhjustajaks oli käideldavus
- sündmuste (suhte)arv teenuste lõikeis
- sündmuste ja intsidentide suhtearv
- jne

Rollid

Kasutajatugi (sh ka seire) – sündmuse olulisuse hindamine, sündmuse seostamine, otsus sündmuse edasise käsitlemise kohta, kasutajate informeerimine.

IT teenuste haldurid – osalevad teenuse kavandamise (*Design*) faasis ja määratlevad hiljem haldamiseks vajalike sündmuste genereerimise, samuti vajalikud korrelatsioonimehhanismid. Teenuste muutmise faasis testivad vajalike sündmuste genereerimist. Teenuste halduse faasis abistavad kasutajatuge keerulisematele sündmustele reageerimises.

Süsteemiadministraatorid – jälgivad oma vastutusvaldkonna sündmusi ja teevad otsuseid sündmustest järelduvate tegevuste osas.

Sündmuste halduse kavandamine

Tavaliselt käivitub tõhus sündmuste haldus mõni aeg pärast uue teenuse evitamist. Ehk sündmuste halduse protsess kavandatakse koos käideldavuse, mahuhalduse ja IT teenuste halduse protsessidega. Samas ei tohi sündmuste halduse protsessi kunagi lugeda lõplikuks (staatiliseks), vaid teda tuleb pidevalt parendada. Sündmuste halduse protsessi kavandamine sisaldab:

1) **Instrumenteerimist** - määratleb mida *CI*-dest jälgitakse ja kuidas CI-de näitajate muutustele reageeritakse
2) **Vigadest teavitamine** – oluline on et kõik komponendid (eriti rakendused) oleksid kavandatud toetamaks sündmuste halduse protsessi. Näiteks JMX *(Java Management Extension).*
3) **Vigade avastamine ja alarmide formeerimine** – sisaldab mehhanismi sündmuste filtreerimiseks, seostamiseks ja eskaleerimiseks.
4) **Lävede määratlemine** – kavandamise käigus seatakse esmased läved. Hiljem lävesid endid ei hallata sündmuste halduse protsessiga, vaid vastavate teiste IT teenuste haldust käsitlevate protsessidega.

Tehnoloogia

Järgnevaid soovitusi peab arvestama sündmuste halduse tehnoloogia (tööriistade) kavandamisel:

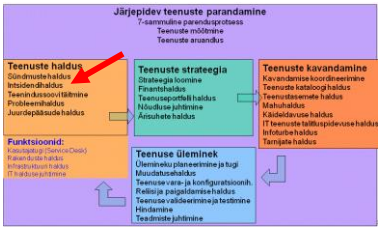
- sobivus erinevate keskkondadega ja avatud liidesed võimaldamaks seiret ja info kogumist üle erinevate komponentide ja teenuste keskkondade
- lihtne evitada ja mõistlik hind
- “standardne” agent monitoorimaks või fikseerimaks soovitud sündmusi
- sündmuste tsentraalne kogumine ühte või mitmesse asukohta
- uute toodete/teenuste kavandamise ja testimise faasi toe võimalus
- häirelävede seadmise võimalus
- hea raporteerimise funktsionaalsus

Intsidendihaldus

Incident Management

Teenuste haldus

Primary source: Service Operation
Further expansion: Continual Service Improvement



Guid

Mõiste, eesmärk ja käsitlusala

Intsidendiks nimetatakse iga IT teenuse mitteplaneeritud katkestust või IT teenuse kvaliteedi halvenemist. Konfiguratsioonielemendi tõrge, kus IT teenus veel mõjutatud ei ole, on samuti intsident.

Intsidentide haldus on protsess, mis käsitleb kõiki intsidente nagu süsteemide ja teenuste tõrked, klientide märkused ja päringud, tehnilise personali tähelepanekud ja automaatsed seiresüsteemi teated.

Eesmärk
Taastada normaalne teenus (SLA-s määratletud ajaks) nii kiiresti kui võimalik ja minimiseerides sealjuures ebasoovitavaid mõjusid äriprotsessidele.

Käsitlusala
Intsidendihaldus käsitleb kõiki sündmusi, mis ei ole normaalse haldusprotsessi osa ja mis on esile kutsunud või mis võivad esile kutsuda ebasoovitavaid hälbeid IT teenuste kvaliteedis.

Mitte kõik sündmused ja kasutajapöördumised ei ole intsidendid.

Guido Leibur

Olulisus ärile

Intsidendid on tavaliselt kergesti märgatavad äripoolel ja seetõttu on intsidendihalduse protsess, mis võib teenuste haldusest enam huvitada äripoolt.

Intsidendihalduse väärtus äripoolele sisaldab:
- võimekust avastada ja kiiresti lahendada äripoolele olulisi intsidente tagades seeläbi kõrgema teenuste käideldavuse,
- võimekust joondada IT tegevusi reaalajalistele äriprioriteetidele,
- võimekust kavandada potentsiaalseid teenuse parendusi,
- täiendava koolitusvajaduse määratlemist kas IT või äripoolel, seda seni esinenud intsidente analüüsides

Guido Leibur

Põhimõtted

1) Intsidendid tuleb kiiresti avastada ja edastada lahendamiseks;
2) Intsidendid tuleb lahendada äripoolele aktsepteeritava aja (tavaliselt SLA-s kirjas) jooksul;
3) Intsidentidest tuleb õigeaegselt ja piisaval määral intsidendist mõjutatud teenuse kasutajatele teada anda;
4) Kõik intsidendid tuleb salvestada tsentraalselt ja ühtses formaadis;
5) Intsidentide kirjed peavad olema auditeeritavad;
6) Intsidentide prioretiseerimise kriteeriumid peavad olema kokku lepitud

Põhimõisted

1) **Intsidentide käsitlemise aeg** - tuleneb äriteenuste prioriteetidest ja on eelnevalt fikseeritud (SLA-s või OLA-s). Kogu tugipersonal peab neist aegadest olema teadlik. Ajad on tavaliselt teenusepõhised.
2) **Intsidendi mudelid**. Suur osa intsidente ei juhtu esmakordselt ja korduvate intsidentide lahendamiseks on kasulik välja töötada kindlad mudelid (töövood). Intsidendi mudel võiks sisaldada:
   - intsidendi käsitlemise konkreetseid samme ja ajalist järjekorda,
   - vastutusi (kes mida tegema peab),
   - intsidendi käsitlemise aega ja eskalatsioonireegleid,
   - tõendamiseks-säilitamiseks vajalikke tegevusi (turvaintsidentide korral)
3) **Olulised intsidendid**. Olulise intsidendi mõiste tuleks äripoolega kokku leppida ja oluliste intsidentide lahendamiseks koostada erinevad töövood. Intsidendi olulisus sõltub intsidendi ärimõjust. Väiksemas organisatsioonis võiks oluliste intsidentide lahendamist juhtida kasutajatoe juht, suuremates mõjutatud äriteenuse juht.
4) **Intsidendi kirje olekud:** **avatud -> töös -> lahendatud -> suletud**

Intsidentide liigid

ISKE-st tulenevalt

1) **Käideldavuse intsident** – avastab reeglina kas IT seire või üksikjuhtudel klient

2) **Terviklusintsident** – avastab reeglina klient, üksikjuhtudel IT (kui IT omab vastavaid seirevahendeid)

3) **Konfidentsiaalsuseintsident** – avastab reeglina IT turvaseire, üksikjuhtudel klient

Guido Leibur

Protsessi kirjeldus 1

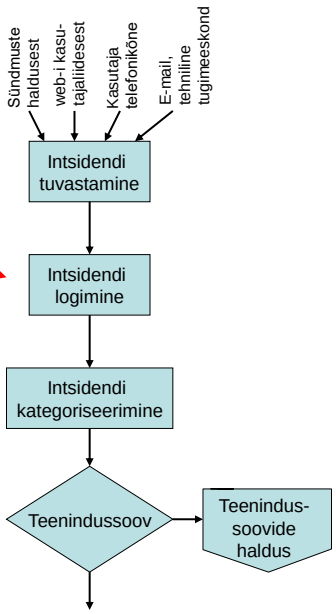
1) Intsidendi tuvastamine

Protsess algab intsidendi fikseerimisest (tuvastamisest). Tavapärane on tuvastada intsident sündmuste halduse kaudu (monitooringu süsteemi vahendusel), mitte oodata kuni kasutajad sellest hakkavad teavitama.

2) Intsidendi logimine

Peaks sisaldama alljärgnevat infot:

- unikaalne ID
- intsidendi kategooria (2-4 taset)
- intsidendi pakilisus
- intsidendi mõju
- intsidendi prioriteetsus
- salvestamise aeg
- salvestaja (operaatori) nimi või ID
- teavitamise moodus (vt sisendeid)
- kasutaja nimi /osakond / asukoht / telefon
- tagasiteavitamise moodus (telefon, e-mail vm)
- intsidendi kirjeldus
- intsidendi olek (aktiivne, ootel, suletud vm)
- intsidendiga seostatavad CI-d
- tugiisik (-grupp) kellele intsident on suunatud
- seostatud probleem / tuntud viga
- tegevuste kirjeldus intsidendi likvideerimiseks
- intsidendi lahendamise aeg
- intsidendi sulgemise aeg



Guido Leibur

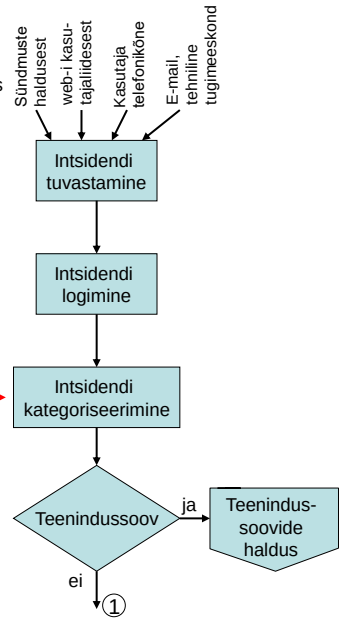
Protsessi kirjeldus 2

3) Intsidendi kategoriseerimine

Kategoriseerimine on intsidendi logimise üks osa.
Kategoriseerimine on oluline hilisemas probleemihalduses, kus analüüsitakse seni esinenud intsidente. Sagedamini **teenusepõhised**.
Kategoriseerimiseks võib kasutada eri tasemeid, näiteks:
- riistvara: server, mälukaart või
- tarkvara: rakendus, finantssüsteem

Kategooriad on tihti ettevõtteis erinevad. Alustades seda aga nullist, tuleks järgida seda, et:
- kategooriate loomisse on kaasatud vastav tugipersonal, klienditoe juht, intsidentide ja probleemihalduse protsesside juhid
- määratleda esmalt olulised (ülemise taseme) kategooriad
- rakendada mõneks ajaks testperioodi
- vaata kategooriaid regulaarselt üle

Teenindussoovide kontroll intsidendihalduses ei tähenda, et teenindussoov oleks intsidendihalduse protsessi osa. Praktikas sageli on osa teenindussoove kasutajate poolt määratletud kui intsidendid ja sellisel juhul tuleb nad suunata oma protsessi.



Guido Leibur

Protsessi kirjeldus 3

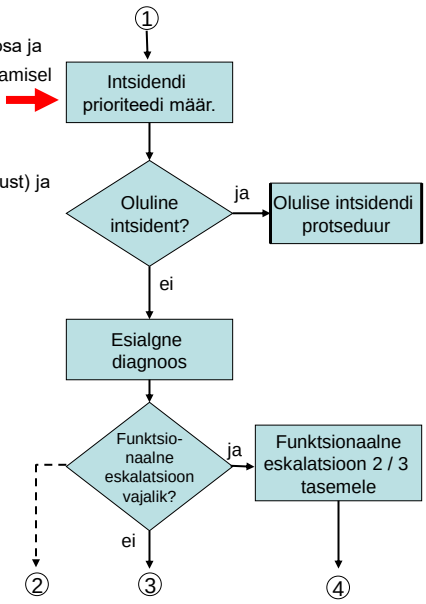
4) Intsidendi prioriteedi määramine

Intsidendi prioriteet on samuti üks intsidendi logimise osa ja ta on vajalik erinevate intsidentide samaaegsel lahendamisel lahendava personali tegevuste joondamiseks.

Tavaliselt võetakse prioriteedi määramisel arvesse:
- intsidendi pakilisust (kui kiiresti äripool vajab lahendust) ja
- intsidendi mõju ulatust. Siin tuleb arvesse võtta:
  - äririske
  - mõjutatud teenuste arvu
  - mõjutatud kasutajate arvu
  - finantskahju suurust
  - ärimaine kahjustamist
  - regulaatori või seadusandluse mõjusid

Prioriteedid:

		Mõju		
		Kõrge	Keskmine	Madal
Pakilisus	Kõrge	**1**	**2**	**3**
	Keskmine	**2**	**3**	**4**
	Madal	**3**	**4**	**5**



Guido Leibur

Protsessi kirjeldus 4

4) Intsidendi prioriteedi määramine (jätkub)

		Mõju		
		Kõrge	Keskmine	Madal
Pakilisus	Kõrge	**1**	**2**	**3**
	Keskmine	**2**	**3**	**4**
	Madal	**3**	**4**	**5**

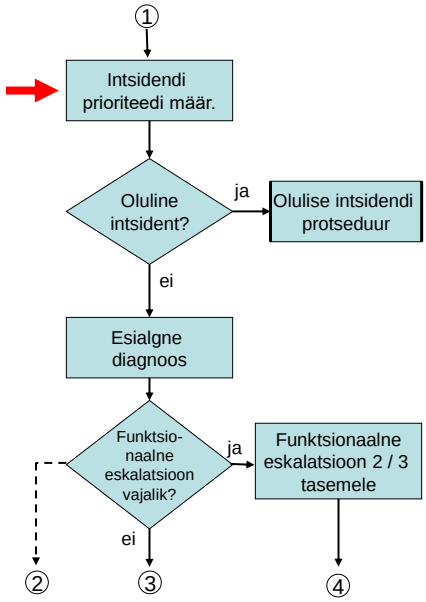
Prioriteet	Kirjeldus	Eesmärk lahendamise aeg
1	Kriitiline	15 min
2	Kõrge	1 tund
3	Keskmine	8 tundi
4	Madal	24 tundi
5	Planeerimine	ei määratleta

Täpsed intsidentide lahendamise ajad määratletakse kokkuleppel äripoolega ja fikseeritakse SLA-s. Samuti on eesmärkajad arvutatavad käideldavusest.

Mõnedes organisatsioonides võetakse prioriteedi määramisel arvesse ka kliendisegmente (VIP kliendid jt).

Intsidendi prioriteetsus on dünaamiline ja võib ajas muutuda!

Guido Leibur



Protsessi kirjeldus 5

5) Intsidendi esialgne diagnoos ja lahendamine

Kui intsident on tulnud läbi kasutajatoe, siis peab esialgse diagnoosi andma kasutajatoe analüütik – tüüpilisilt siis, kui klient on veel telefoniliinil (kui intsidendi algatajaks on klient). Täpse diagnoosi andmiseks tuleks kasutada ka konfiguratsioonihalduse sõltuvusi, erinevaid monitooringu tööriistu ja tuntud vigade andmebaasi.

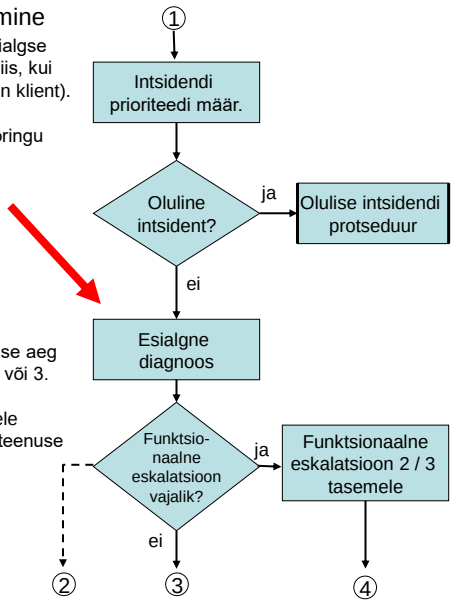
Tuntud vigade andmebaas!
Known error database (KEDB)

6) Intsidendi eskalatsioonid

Funktsionaalne (horisontaalne) eskalatsioon – rakendatakse kui kasutajatoes ei suudeta intsidenti lahendada või kui kasutajatoes intsidendi lahendamise aeg on täis saanud. Intsident suunatakse tehnilise toe 2. või 3. tasemele.
2. ja 3. tasemel suunatakse intsident kas konkreetsele lahendajale (kui see suudetakse määratleda) või IT teenuse haldurile.

Ka peale intsidendi edasisuunamist jääb intsidendi omanikuks ikkagi kasutajatugi!

Guido Leibur



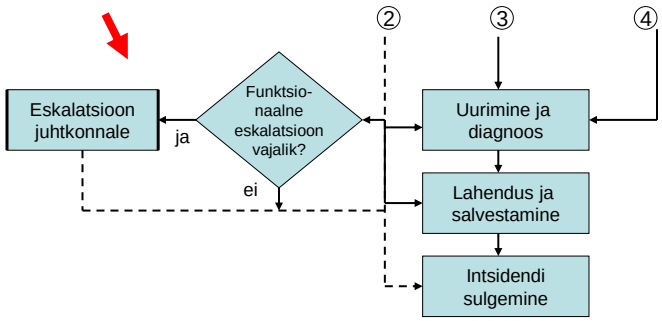
Protsessi kirjeldus 6

6) Intsidendi eskalatsioonid

Funktsionaalne (horisontaalne) eskalatsioon
Hierarhiline (vertikaalne) eskalatsioon - rakendatakse kui:
- informatsiooni andmist juhtidele eriti oluliste intsidentide (näiteks prioriteediga 1) korral
- konkreetse intsidendi lahendamine on võtnud kauem aega, kui SLA-s kokku lepitud.

Konkreetsed eskalatsiooniajad ja eskalatsiooniahelad tuleb eelnevalt kokku leppida.
Kasutajatoe töötajad peavad teavitama kasutajaid kõikidest eskalatsioonidest.

Intsidente tuleb lahendada vastavalt nende prioriteetidele!



Guido Leibur

Protsessi kirjeldus 7

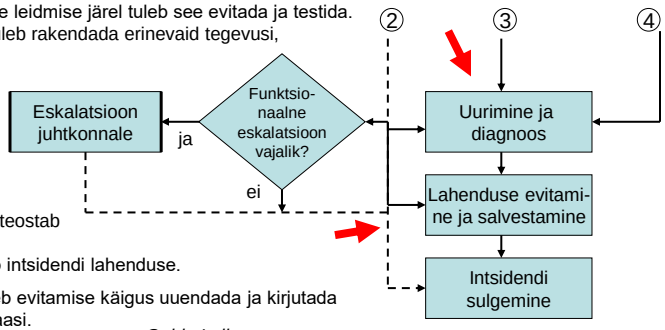
6) Uurimine ja diagnoos

Uurimine sisaldab järgmisi tegevusi:
- selgitatakse täpselt mis on läinud valesti või mida soovitakse (otsitakse) kasutaja poolt,
- tuleb aru saada sündmuste ajalisest järjestusest,
- tuleb fikseerida intsidendi mõju ulatus (teenused, kasutajad, piirkond jm),
- teadmiste baasist analoogsete intsidentide otsimist.

Diagnoosi käigus dokumenteeritakse kõik vahepealsed tegevused.
Mõistlik on aja kokkuhoiuks uurimist ja diagnoosi paralleelselt sooritada.

7) Lahenduse evitamine ja salvestamine

Potentsiaalse lahenduse leidmise järel tuleb see evitada ja testida.
Teenuste taastamisel tuleb rakendada erinevaid tegevusi, mis võivad sisaldada:
- klienditugi evitab lahenduse ise (näit restardib serveri),
- palutakse klientidel teatavaid taastavaid tegevusi,
- klienditoe 2 / 3 tase teostab teatavaid tegevusi
- väline partner evitab intsidendi lahenduse.



Intsidendi kirjeldust tuleb evitamise käigus uuendada ja kirjutada kokkuvõte teadmiste baasi.

Guido Leibur

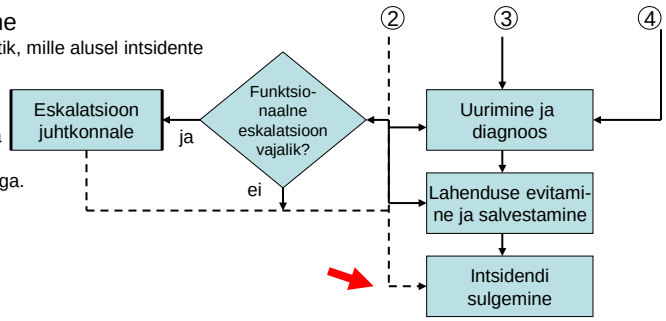
Protsessi kirjeldus 8

8) Intsidendi sulgemine

Kasutajatugi peab kontrollima, et intsident on täielikult lahendatud ja et kasutajad on rahul ja nõus intsidendi sulgemisega.
Sulgemisel peab kasutajatugi kontrollima:
- sulgemise kategooriat, st kas esialgu määratud kategooria ikka vastas tegelikkusele.
- kasutajate rahulolu,
- intsidendi dokumentatsiooni korrektsust,
- jätkuvaid (lahendamata) või korduvaid probleeme. Koos intsidenti lahendanud spetsialistidega veenduma, et intsident ei saa enam korduda. Vajadusel avama probleemi.
- formaalselt sulgema intsidendi

Intsidendi taasavamine

Tuleb fikseerida reeglistik, mille alusel intsidente uuesti avatakse (näit vigade ilmnemisel 1-2 päeva jooksul). Sellisel juhul tuleb ikkagi avada uus intsident, kuid ta tuleb seostada eelmisega.



Guido Leibur

Intsidendi sisendid ja algatajad

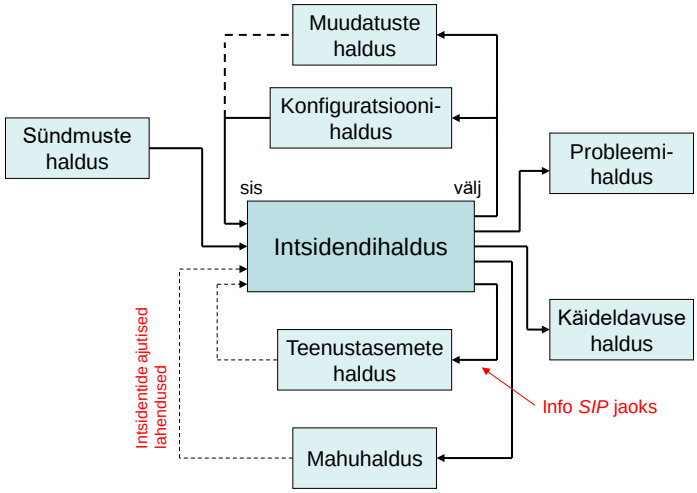
1) Kõige olulisemaks sisendiks intsidentide avamisel peaks olema sündmuste haldusest (seirest) tekkivad automaatsed alarmid ja teated, ning kasutajatugi.

2) Tehniline tugipersonal ja IT teenuste haldurid

3) Kasutajate teated

4) Tarnijad, koostööpartnerid

Liidesed teiste protsessidega



Näidatud on olulisemad seosed

SIP = Service Improvement Plan – teenuse parandamise plaan

Guido Leibur

Kasutajate informeerimine

1) Intsidendi avamisest
2) Intsidendi lahendamise käigust
3) Vajadusel täiendava info küsimine
4) Intsidendi eskaleerimisest
5) Oluliste intsidentide korral informeeritute ring laiem
6) Kliendi rahulolu küsimine enne intsidendi sulgemist
7) Kasutajate eelnev teavitamine teadaolevatest teenuse katkestustest

Guido Leibur

Süsteemi-informatsiooni juhtimine

Suurem osa intsidendihalduse protsessis kasutatavast informatsioonist lähtub:

1) intsidendihalduse tööriistast, mis sisaldab infot:
   - intsidentide ja probleemide ajaloo kohta,
   - intsidendi kategooriat,
   - tegevuste kirjeldusi intsidendi likvideerimiseks,
   - diagnostika skripte, mis aitavad kasutajatoe 1.tasemel lahendada intsidente

2) Intsidentide salvestusi, mis omavad järgmist infot:
   - unikaalne ID
   - intsidendi klassifikatsioon
   - iga tegevuse ajaline logi
   - salvestuse uuendaja nimi ja aeg
   - intsidendi kirjeldus
   - intsidendi kategooria ja prioriteetsus
   - seosed teiste intsidentidega
   - intsidendi sulgemise üksikasjad

Samuti kasutatakse teadmiste baasi ja konfiguratsioonihalduse baasi informatsiooni.

Guido Leibur

Meetrika

Meetrika, mida võiks kasutada ja milles kohta võiks anda aru sisaldab:

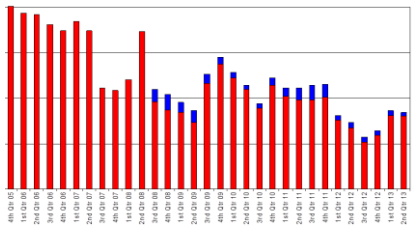
- kogu intsidentide arv, intsidentide arv teenuste lõikeis
- avatud intsidentide arv
- oluliste intsidentide suhtearv
- oluliste intsidentide algpõhjused
- intsidentide ärimõju
- keskmine intsidendi lahendamiseks kulunud aeg
- õigeaegselt lahendatud intsidentide suhtearv
- keskmine intsidendi hind
- taasavatud intsidentide suhtearv
- valesti suunatud intsidentide (suhte)arv
- valesti kategoriseeritud intsidentide (suhte)arv
- kasutajatoe 1.tasemel lahendatud intsidentide suhtearv
- kaughalduse vahenditega lahendatud intsidentide arv
- jm

Guido Leibur

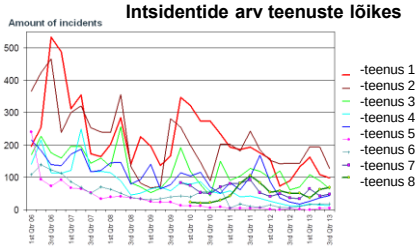
2. Intsidendihaldus 19

Meetrika näiteid

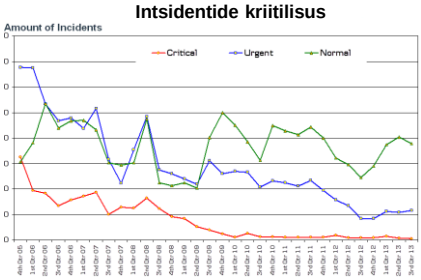
Intsidentide koguarv



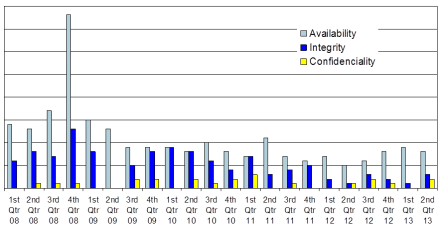
Intsidentide arv teenuste lõikes



Intsidentide kriitilisus



Intsidentide tunnused



Guido Leibur

2. Intsidendihaldus 20

Rollid

Intsidendihaldur (protsessijuht vastutab):

- intsidendihalduse protsessi tõhusa ja tulemusliku toimivuse eest,
- juhtimisinformatsiooni loomise eest
- 1.ja 2. kasutajatoe tasemel teostatavate tööde eest
- intsidendihalduse protsessi tulemusliku toimivuse seire ja parendamise ettepanekute tegemise eest
- intsidendihalduse süsteemi haldamise ja arendamise eest
- oluliste intsidentide lahendamise juhtimise eest
- intsidendihalduse protsessi haldamise ja arendamise eest

Kasutajatoe 1.tase – kasutajatugi (*Service Desk*), võtab vastu ja registreerib intsidente

Kasutajatoe 2.tase – IT spetsialistid, kes lahendavad keerukamaid intsidente

Kasutajatoe 3.tase – välised partnerid, outsourcitud teenuseosutajad

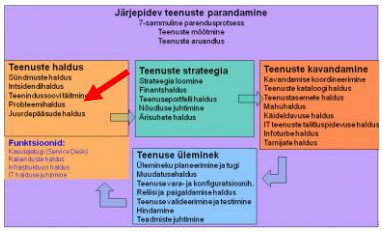
Guido Leibur

Probleemihaldus

Problem Management

Teenuste haldus

Primary source: Service Operation
Further expansion: Continual Service Improvement



Guid

2. Probleemihaldus 1

Mõiste, eesmärk ja käsitlusala

Probleem on tundmatu algpõhjus ühele või mitmele intsidendile.

Probleemihaldus on protsess, mis käsitleb kõigi probleemide haldust nende eluea jooksul.

Eesmärk
Ennetada võimalikke probleeme ja neist tulenevaid intsidente. Samuti kaotada korduvate intsidentide tekkimine ning minimiseerida nende intsidentide mõju, milliseid ei suudeta ära hoida.

Käsitlusala
Probleemihaldus käsitleb tegevusi, mis on vajalikud intsidentide algpõhjuse leidmiseks ja lahendamiseks. Probleemihaldus (nagu intsidendihalduski) käsitleb ka ajutisi lahendusi.

Probleemid defineeritakse, intsidendid juhtuvad!

Intsidendihaldus on suunatud **kiirele** tulemile, probleemihaldus tulemi **kvaliteedile**.
Guido Leibur

Olulisus ärile

Probleemihaldus, intsidendihaldus ja muudatusehaldus töötavad koos tagamaks IT teenuste käideldavuse ja kvaliteedi kasvu äripoole jaoks.

Probleemihaldus on oma fookusega tulevikus ehk oluline on ennetada võimalikke IT teenuste mittetoimimisi.

Põhimõtted 1

1) Intsidente tuleb alati käsitleda probleemidest lahus
2) Probleeme tuleb hallata ühtses andmebaasis
3) Probleemidele tuleb rakendada ühtset klassifikatsiooni ja prioretiseerimise põhimõtteid.

Intsident ei saa muutuda probleemiks!

Küll võib intsidendi põhjal defineerida probleemi.

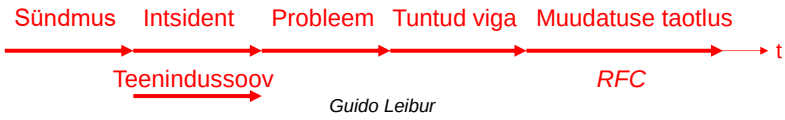
2. Probleemihaldus 4

Põhimõtted

Üks osa probleeme on unikaalsed ja neid lahendatakse individuaalsel moel.

Teine (tihti suurem) osa probleeme on korduvad, kus juurpõhjus on teada, kuid majanduslikult on nende kõrvaldamine ebamõistlik. Oluline on siis analoogselt intsidendihaldusele välja töötada ajutised lahendused ja salvestada need tuntud vigade baasi.

Probleemihalduse protsess on kas **reageeriv** (*reactive*) või **ennetav** (*proactive*).



Guido Leibur

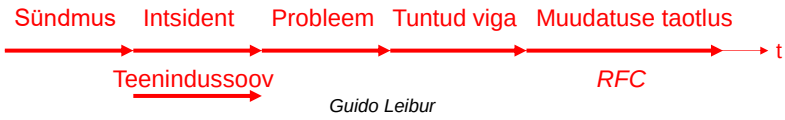
2. Probleemihaldus 5

Põhimõtted

Üks osa probleeme on unikaalsed ja neid lahendatakse individuaalsel moel.

Teine (tihti suurem) osa probleeme on korduvad probleemid kus juurpõhjus on teada, kuid majanduslikult on nende kõrvaldamine ebamõistlik. Oluline on siis analoogselt intsidendihaldusele välja töötada ajutised lahendused ja salvestada need tuntud vigade baasi.

Probleemihalduse protsess on kas **reageeriv** (*reactive*) või **ennetav** (*proactive*).



Guido Leibur

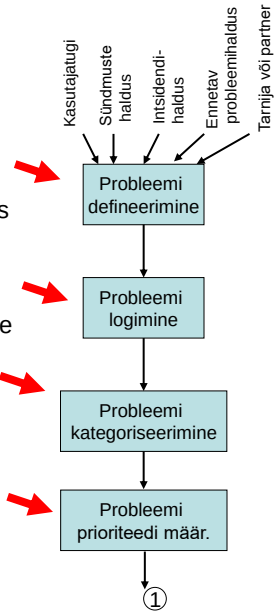
Reageeriva protsessi kirjeldus 1

1. **Probleemi defineerimine** võib toimuda erinevaist allikaist pärineva info alusel.

2. **Logimine** – pannakse kirja praktiliselt sama info, mis intsidentide korral. Oluline on probleem seostada võimalike põhjustega (varasemad intsidendid).

3. **Kategoriseerimine** – toimub analoogselt intsidentide kategoriseerimisele.

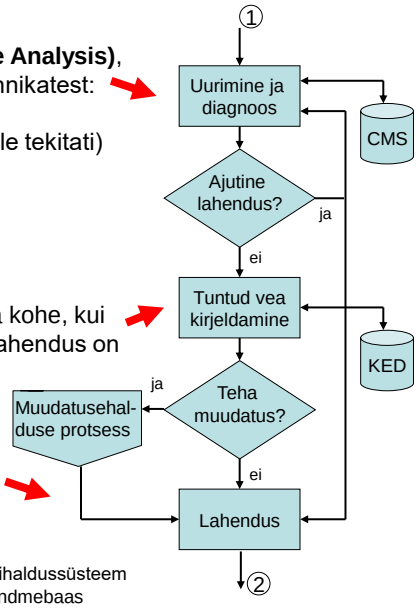
4. **Prioriteedi määramine** – toimub analoogselt intsidentide prioriteedi määramisele. Täiendavalt tasub siin arvesse võtta varasemate seotud intsidentide esinemise sagedust ja mõju ulatust.



Guido Leibur

Reageeriva protsessi kirjeldus 2

5. **Uurimine ja diagnoos (RCA-Root Cause Analysis)**, kus kasutatakse mõnda alljärgnevatest tehnikatest:
   - 5.1 kronoloogiline analüüs
   - 5.2 “valu” suuruse analüüs (mida äripoolele tekitati)
   - 5.3 Kepner’i ja Tregoe meetod
   - 5.4 ajurünnak
   - 5.5 Ishikawa (kalasaba) diagramm
   - 5.6 Pareto analüüs
6. **Ajutised lahendused**
7. **Tuntud vea kirjeldamine** – see tuleb teha kohe, kui juurpõhjus veale on leitud, või kui ajutine lahendus on välja töötatud.
8. **Probleemi lahendamine** – enamikel juhtudel toimub lahendamine läbi muudatusehalduse protsessi. Siiski väga kallite lahenduste korral võidakse jääda kasutama ajutist lahendust. **Sellisel juhul jääb probleem avatuks.**



CMS – konfiguratsioonihaldussüsteem
KED – tuntud vigade andmebaas

Guido Leibur

5.3 Kepner'i ja Tregoe meetod

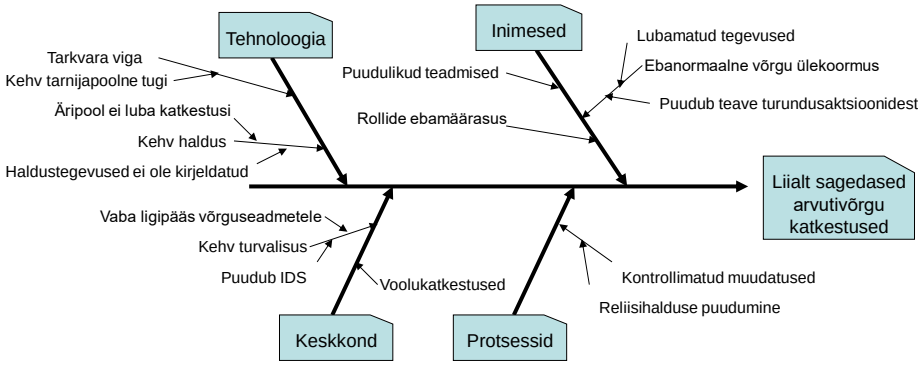
Charles Kepner ja Benjamin Tregoe väljatöötatud meetod probleemide analüüsiks koosneb viiest etapist.

- probleemi määratlemine
- probleemi kirjeldamine. Kirjeldus peks sisaldama:
  - **identiteeti.** Milline süsteemi osa ei tööta korrektselt?
  - **asukohta.** Kus probleem ilmnes?
  - **aega.** Millal probleem ilmnes?
  - **ulatust.** Milline on probleemi ulatus (suurus)? Kui palju süsteemiosi on sellega seotud?
- võimalike põhjuste kirjeldamine
- enam tõenäoste põhjuste testimine
- juurpõhjuse verifitseerimine

Guido Leibur

5.5 Ishikawa diagramm

Kaoru Ishikawa (1915-1989) – Jaapani kvaliteedi kontrolli juhtiv teadlane.



Enam tõenäosed põhjused kirjutatakse nooleotsale lähemale.

Guido Leibur

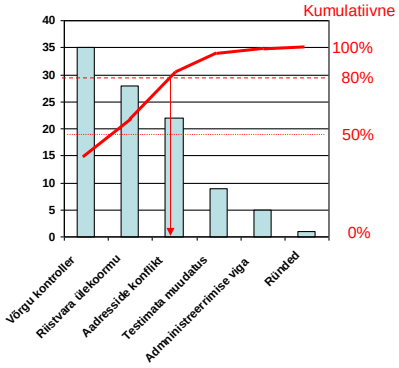
5.6 Pareto analüüs

Selle tehnika puhul on eesmärk eristada potentsiaalselt olulisemad probleemi põhjused vähemolulistest.

1) Koostage tabel võimalikest (esilagu oletuslikest) põhjustest ja esinemissagedusest (Σ = 100%)
2) Sorteerige tabeli read vähenevate esinemissageduste järgi
3) Lisage tabelile kumulatiivne %
4) Üle kumulatiivse 80% jäävaid põhjuseid tasub täpsemalt edasi analüüsida

Võrgu katkestus

Põhjus	Esinemissagedus, %	Kumulatiivne, %
Võrgu kontroller	35	35
Riistvara ülekoormus	28	63
Aadresside konflikt	22	85
Testimata muudatus	9	94
Administreer. viga	5	99
Ründed	1	100
Summa	100%	



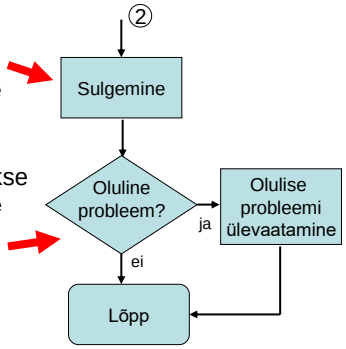
Guido Leibur

Reageeriva protsessi kirjeldus 3

9. Probleemi sulgemine – kontrollitakse kas mõni asjassepuutuv intsident ei ole jäänud avatuks, et probleem on korrektselt kirjeldatud tuntud vigade andmebaasis ja et kasutajad on rahul.

10. Olulise probleemi ülevaatamine – seda tehakse vahetult pärast probleemi sulgemist. Ülevaatuse käigus tehakse enda jaoks järeldused:
- asjadest, mida tehti õieti
- asjadest mida tehti valesti
- mida saaks tulevikus paremini teha
- kuidas vältida probleemi kordumist
- kas edaspidist järelkontrolli on vaja või mitte

Järeldused tuleks dokumenteerida ja hiljem äripoolega läbi arutada.



Tuntud vigade andmebaasi tuleb kanda ka need puudused, millega mõnikord uued rakendused tootmiskeskkonda (*Live* keskkonda) lähevad. Näiteks äripoolel on evitamisega kiire ja lubatakse teatavaid puudujääke.

Guido Leibur

Ennetava protsessi kirjeldus

1. **Trendide analüüs** – klienditugi, süsteemiadministraatorid, IT teenuse haldurid
2. **Ärivajadustega kursisolek** – IT teenuse haldurid
3. **Varem esinenud intsidentide regulaarne analüüs** – klienditugi, IT teenuse haldurid

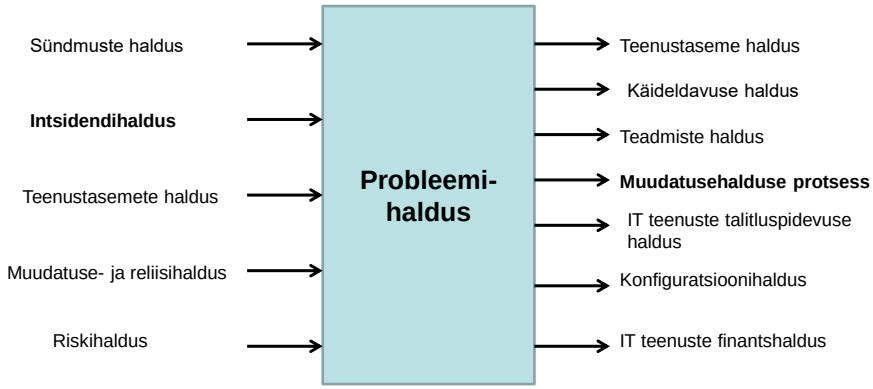
Sisendid ja liidesed teiste protsessidega

Sisendid probleemihaldusele võivad tulla: intsidendihaldusest, kasutajatoest, testimise viimastest faasidest, tarnijailt, süsteemiadministraatoritelt, IT teenuse halduritelt, jm.

Probleemihaldus on seotud muudatusehalduse protsessiga, konfiguratsioonihalduse protsessiga, reliisihaldusega, käideldavuse haldusega, mahuhaldusega, IT teenuste haldusega, IT teenuste talitluspidevuse haldusega, finantshaldusega.

Sisendid ja liidesed teiste protsessidega

Neist olulisemad



Informatsiooni juhtimine

1. **Konfiguratsioonihalduse süsteemis (*CMS*)** hoitakse infot konfiguratsioonielementide ja nendevaheliste seoste kohta. Siit saab uurimiseks ja diagnoosiks väärtusliku infot.

2. **Tuntud vigade andmebaas (*KEDB*)** – kus hoitakse seni toimunud intsidentide ja probleemide lahenduskäikude kohta käivat infot. Siia salvestatakse ka info ajutiste lahenduste kohta. Vältimaks info dubleerimist, on probleemihaldur ainus isik, kes sisestab uue probleemi kirje andmebaasi.
   Andmebaasi eesmärk on kiirendada intsidentide ja probleemide lahendamist.

Nii *CMS* kui *KEDB* moodustavad ühe osa suuremast teenuste teadmiste juhtimise süsteemist (*Service Knowledge Management System – SKMS*).

Meetrika

Võiks kasutada alljärgnevaid mõõdikuid:

- summaarne probleemide arv mingil ajaperioodil
- SLA eesmärkaegade jooksul lahendatud probleemide suhtearv
- avatud probleemide (suhte-)arv ja vastav ajaline suundumus
- keskmine probleemi lahendamise hind
- oluliste probleemide arv
- edukalt lahendatud oluliste probleemide suhtearv
- tuntud vigade andmebaasi lisandunud kirjete arv
- tuntud vigade kirjelduste täpsus andmebaasis (auditi tulemusena)
- edukalt ja õigeaegselt lahendatud oluliste probleemide suhtearv
- korduvate probleemide osatähtsus

Guido Leibur

Rollid

Probleemihalduse juht – vastutab suures organisatsioonis probleemihalduse protsessi koordineerimise eest.

Probleemi lahendav grupp – probleemihalduri juhtimisel töötav spetsialistide grupp.

IT teenuse haldur / Süsteemi administraator – defineerib (avab) oma valdkonna teenuste probleemid, koordineerib nende lahendamist ja sulgeb need.

Kasutajatugi (*Service Desk*) – teeb ettepanekuid IT teenuse haldurile probleemide avamiseks. Haldab tuntud vigade andmebaasi.

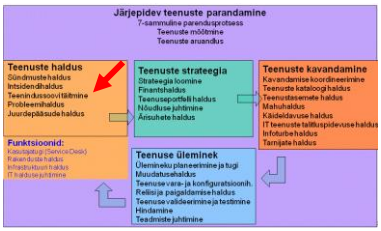
Guido Leibur

Teenindussoovi täitmine

Request Fulfillment

Teenuste haldus

Primary source: Service Operation



Guid

2. Teenindussoovi täitmine [1]

Mõiste, eesmärk ja käsitlusala

Teenindussooviks nimetatakse iga kasutaja nõuet kas informatsiooni, nõuande, **standardse** muudatuse või IT teenuse järele.

Näiteks on teenindussoov: tellimused, standardpäringud ja konsultatsioonid

Eesmärk
Pakkuda kasutajatele lihtne ja kiire moodus nende nõustamiseks ja standardsete teenuste väiksemahuliseks osutamiseks.

Käsitlusala
Kui intsidendihaldus käsitleb tavaliselt sündmusi, mis on raskesti ette planeeritavad, siis teenindussoovi täitmine käsitleb sündmusi, millede lahenduskäigud **peavad olema ette planeeritud!**

Näiteks: parooli muutmine, uue kasutaja lisamine IT teenusele, täiendava tarkvara installeerimine tööjaama, standardpäring, konsultatsioon jne.

Guido Leibur

Olulisus ärile

Äripoolel on võimalus saada kiire ja tulemuslik lahendus standardsete IT teenuste näol. See omakorda võimaldab parandada äripoole tootlikkust ja kvaliteeti.

Teenindussoovi täitmise kaudu peaks vähenema ka bürokraatia, mis omakorda alandab osutatava teenuse omahinda.

Põhimõtted

Paljud teenindussoovid on sarnased (korduvad) ja realiseeritavad **standardse** muudatuste halduse protsessi kaudu.

Teenindussoovi omanikuks on kasutajatugi (*Service Desk*).

Sarnaste teenindussoovide rahuldamiseks on mõttekas välja töötada teenindussoovide käsitlemise mudel (*Request Model*).

Kõik teenindussoovid peavad olema tsentraalselt hallatud.

Iga teenindussoovi täitmine peab olema äriliselt põhjendatud.

Sisendid ja liidesed teiste protsessidega

Peamine sisend teenindussoovile on kasutajatugi (*Service Desk*).

Teenindussoovid on seotud:

- kasutajatoe funktsiooniga
- intsidendihalduse protsessiga
- probleemihalduse protsessiga
- muudatusehalduse protsessiga
- reliisihalduse protsessiga
- teenuse vara- ja konfiguratsioonihalduse protsessiga

Vajadusel tuleb teenindussoovid siduda konkreetsete intsidentide ja probleemidega, mis tingisid selle teenindussoovi.

Guido Leibur

Protsessi kirjeldus 1

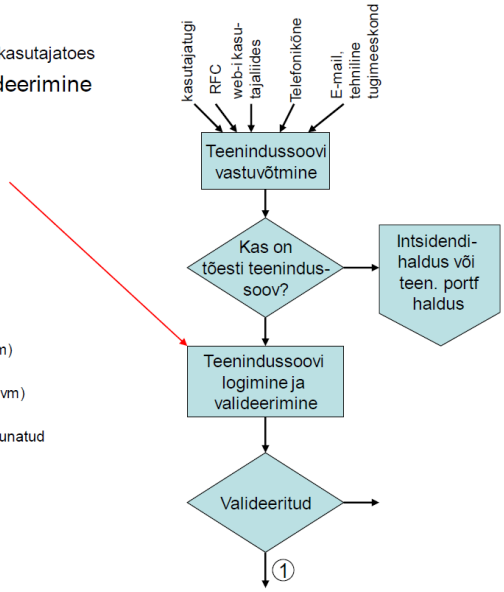
1) Teenindussoovi vastuvõtmine

Enamikel juhtudel toimub vastuvõtmine kasutajatoes

2) Teenindussoovi logimine ja valideerimine

Peaks sisaldama alljärgnevat infot:

- unikaalne ID
- teenindussoovi kategooria (2-4 taset)
- teenindussoovi pakilisus
- teenindussoovi mõju
- teenindussoovi prioriteetsus
- salvestamise aeg
- salvestaja (operaatori) nimi või ID
- teavitamise moodus (vt sisendeid)
- kasutaja nimi /osakond / asukoht / telefon
- kulude lokaliseerimise koht
- tagasiteavitamise moodus (telefon, e-mail vm)
- teenindussoovi kirjeldus
- teenindussoovi olek (aktiivne, ootel, suletud vm)
- teenindussooviga seostatavad CI-d
- tugiisik (-grupp) kellele teenindussoov on suunatud
- intsidendi lahendamise aeg
- intsidendi sulgemise aeg



2. Teenindussoovi täitmine 6

Protsessi kirjeldus 2

3) Teenindussoovi kategooria määramine

Seda kas:

- teenuse alusel

- tegevuste alusel
- tüübi järgi (näit. infopäring versus standardne muudatus)

4) Teenindussoovi prioretiseerimine

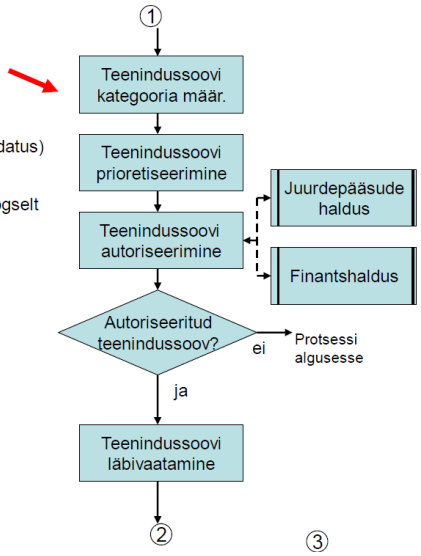
Võtab arvesse nii pakilisust kui mõju ulatust (analoogselt intsidendihalduse protsessile).

5) Teenindussoovi autoriseerimine

Autoriseeritakse kas IVO (ligipääsuõigused) või vahetuse ülemuse poolt

6) Teenindussoovi läbivaatamine

Tehakse kas kasutajatoes või suunatakse teistele tegemiseks



Guido Leibur

2. Teenindussoovi täitmine 7

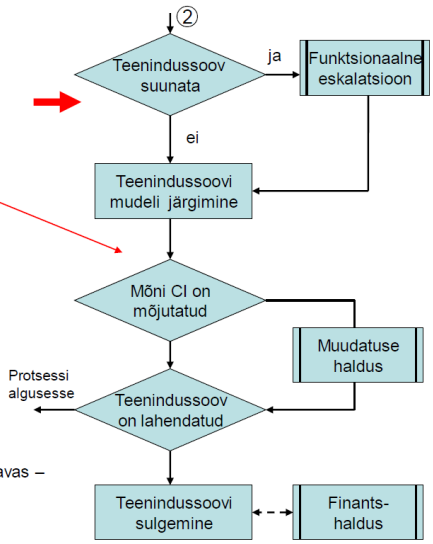
Protsessi kirjeldus 3

5) Teenindussoovi mudeli järgimine

Praktiline teenindamine

6) Teenindussoovi sulgemine

Sulgeb teenindussoovi sama isik, kes selle ka avas – teenindussoovi omanik



Guido Leibur

Informatsiooni juhtimine

Teenindussoov on sõltuv järgmistest infoallikaist:

Teenindussoov ise sisaldab infot:

- teenuse nimetus
- pöörduja nimi
- protsessi nimetus, mille järgi pöördumist lahendatakse
- kellele suunati kasutajapöördumine lahendamiseks
- registreerimise ja lahendamise kronoloogia
- sulgemise detailid

Muudatuse taotlused. Mõningatel juhtudel (enamasti kui pöördumine on seotud konfiguratsioonielemendiga) algatatakse teenindussoov muudatusetaotluse poolt.

Teenuste portfell, mida tuleb silmas pidada konkreetse teenindussoovi teostamisel.

Turvapoliitikad kirjeldavad tellitavaid juurdepääsuõigusi, samuti jälgivad litsentside kasutamist.

Guido Leibur

Meetrika

Teenindussoovi täitmise protsessi hoidmine tõhusa ja tulemuslikuna tähendab alljärgneva meetrika kasutamist:

- summaarne teenindussoovide arv
- teenindussoovi alamprotsesside kestvused
- avatud teenindussoovide arv
- keskmine teenindussoovide täitmise aeg (sõltuvalt tüübist)
- eesmärkaja suhtes õigeaegselt suletud teenindussoovide suhtearv
- keskmine teenindussoovi hind (sõltuvalt tüübist)
- teenindussoovi käsitlemise kliendirahulolu tase

Guido Leibur

Rollid

Teenindussoovi esialgne käsitlemine toimub kas kasutajatoe (*Service Desk*) või intsidendihalduse protsessi poolt.

Hilisem teenindussoovi käsitlemine toimub kas hankemeeskonna, ostujuhi, väljastpoolt IT-d asuva struktuuriüksuse või välise partneri poolt.

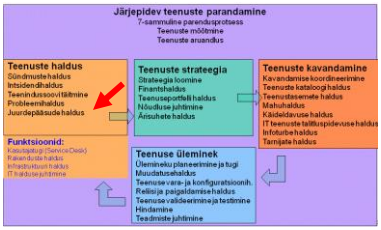
Guido Leibur

Juurdepääsude haldus

Access Management

Teenuste haldus

Primary source: Service Operation



Guid

Mõiste, eesmärk ja käsitlusala

Juurdepääsude haldus on protsess, mis võimaldab autoriseeritud kasutajatel juurdepääsu teenustele ja tõkestab juurdepääsu mitteautoriseeritud kasutajatele.

Eesmärk
Võimaldada kasutajatel juurdepääs teenusele või teenuste grupile vastavalt nende tegelikele vajadusele ja minimiseerides sealjuures liigseid riske. See on infoturbe halduses ja käideldavuse halduses määratletud tegevuste teostamine.

Käsitlusala
Juurdepääsude haldus on turva- ja käideldavuse halduse tulemuslik teostamine organisatsioonis, et võimaldada hallata organisatsiooni **andmete** ja **intellektuaalse vara** konfidentsiaalsust, käideldavust ja terviklikust.

Juurdepääsude haldus saab alguse tavaliselt kliendipöördumisest ja ta teostatakse enamasti kasutajatoes.

Olulisus ärile

1. Võimaldab kontrollitud juurdepääsude kaudu tagada organisatsiooni tulemuslikuma informatsiooni konfidentsiaalsuse juhtimise.
2. Töötajad omavad õige taseme juurdepääsuõigusi tegemaks oma tööd tulemuslikult.
3. Tõenäoselt on vähem vigu kriitiliste teenuste andmete sisestamisel.
4. Võimalus paremini auditeerida teenuste kasutamist
5. Parem võimalus vajadusel kiiresti tõkestada teenuse kasutamine (kui see vajalikuks osutub)
6. Tavaliselt on juurdepääsude haldus ka erinevate regulaatorite nõue.

Põhimõisted

1. **Juurdepääs (*Access*)** viitab teenuste laiendatud funktsionaalsuse tasemele või andmetele, mida kasutajad plaanivad kasutada.
2. **Identsus (*Identity*)** viitab informatsioonile, mis on individuaalselt kättesaadav ja verifitseerib selle kasutaja staatuse organisatsioonis. Identsus on alati unikaalne ühe kasutaja jaoks.
3. **Õigused (*Rights*)** viitavad konkreetsetele seadetele kuidas kasutaja või kasutajate grupp saab ligi teatavatele teenustele või teenuste grupile. Õigusi liigitatakse: lugemise, kirjutamise, teostamise, muutmise ja kustutamise õigusteks.
4. **Teenused või teenuste grupid.** Enamus kasutajaid kasutab mitmeid teenuseid. Hõlbustamaks juurdepääsude haldust toimub juurdepääsuõiguste andmine tavaliselt teenustele lülitades kasutajaid vastavasse teenuste gruppi.
5. **Kataloogiteenus (*Directory Services*)** on vastaval tarkvaral põhinev teenus, mis võimaldab anda juurdepääsuõigusi ressurssidele (objektidele). Kataloogiteenus põhineb OSI X.500 standardil. Sagedamini kasutatav protokoll on LDAP (*Lightweight Directory Access Protocol*).

Guido Leibur

Protsessi kirjeldus

1. **Juurdepääsu taotlemine** toimub kas:
   - personalisüsteemi poolt genereeritud taotluse poolt (inimese tööletulekul, lahkumisel jm)
   - muudatusetaotluse (*RFC*) poolt
   - teenindussoovi täitmise haldusprotsessi poolt
   - realiseerides eelnevalt autoriseeritud skripti
2. **Verifitseerimine.** Igat juurdepääsunõuet teenustele tuleb verifitseerida kahel põhjusel:
   - kasutaja, kes soovib juurdepääsu on õige isik (näiteks kasutajanime ja parooli abil)
   - kasutajal on legitiimsed õigused nõutud juurdepääsule (näiteks IVO nõusolek)
3. **Õiguste andmine.** Juurdepääsude halduses toimub õiguste andmine kuid otsused kellele milliseid õigusi – see sünnib väljaspool seda protsessi. Küll kuulub siia aga rollikonfliktide formaalne selgitamine.
4. **Identsuse staatuse monitooring.** Kasutajate rollid organisatsioonis võivad ajas muutuda erinevatel põhjustel. Juurdepääsuhalduse protsess ja tööriist(-ad) peavad võimaldama kergesti rolle muuta.
5. **Juurdepääsu logimine ja jälgimine.** Juurdepääsude muutmine peab olema logitud ja logidele juurdepääs piiratud.
6. **Juurdepääsude või õiguste sulgemine.** Sulgemise sisuline osa ei kuulu juurdepääsude haldamise protsessi, küll aga formaalne osa.

Guido Leibur

Sisendid ja liidesed teiste protsessidega

Juurdepääsu taotlus saab alguse kas:

1. **Muudatusetaotlusest (*RFC*)** – näiteks mõne projekti käigus on vaja lisada või muuta kasutajaid.
2. **Teenindussoovidest** – tavaliselt registreeritakse kasutajatoe (*Service Desk*) süsteemis ja teostatakse kasutajatoe poolt.
3. **Personalitöötaja pöördumine** – tavaliselt samuti läbi kasutajatoe.
4. **Osakonnajuhatajate või struktuuriüksuste juhtide pöördumine** – tavaliselt läbi kasutajatoe.

Juurdepääsude haldus on seotud personaliprotsessidega, infoturbe halduse protsessiga, muudatusehalduse protsessiga, teenustasemete haldusprotsessiga.

Guido Leibur

Informatsiooni juhtimine

1. **Identsus** ühe kasutaja jaoks sisaldab näiteks nime, aadressi, kontaktinfot (telefon, e-mail), füüsilist dokumentatsiooni (pass, sertifikaat jm), ID, biomeetriline info, kehtivusaeg.
   Juurdepääsuõigusi võidakse anda ka ajutiselt.

2. **Kasutajad, grupid, rollid ja teenuste grupid.** Haldamise huvides tihti infot grupeeritakse näiteks kasutajaprofiili, mingisse õiguste gruppi või mujale. Suur osa nn infrastruktuuri üldkasutatavaid teenuseid tehakse kõigile firma töötajatele kättesaadavaks (näiteks võrguteenus, e-mail, intranet, jt). Osa kasutajagruppe või teenuseid võivad omada kõrgendatud turvanõudeid (näiteks VPN kasutamine, muud täiendavad kontrollid). Teenuste ja kasutajate vahel on õiguste osas mitu-mitmele seos.

Guido Leibur

Meetrika

Juurdepääsuhalduse protsessi tulemuslikkuse hindamiseks võib kasutada järgmisi mõõdikuid:

- juurdepääsutaotluste summaarne arv
- juurdepääsuõiguste arv teenuste, osakondade lõikeis
- intsidentide arv, kus on olnud vajadus tagasi võtta juurdepääsuõigusi
- intsidentide arv, mis on põhjustatud ebakorrektseist juurdepääsuõigustest

Rollid

Kasutajatugi (*Service Desk*) – registreerib ja teostab juurdepääsuõiguse andmist. Teavitab kasutajaid, koostab aruandeid.

IVO (infovara omanik) – kinnitab juurdepääsuõiguse infovarale

Peakasutaja või IVO – teostab juurdepääsuõiguse andmise (äri) rakendustele

IT teenusehaldur või süsteemiadministraator – teostab juurdepääsuõiguse andmise arvutisüsteemse keskkonna (infrastruktuuri) objektidele.