

Logimise nõuded (sh välisele partnerile)

Nõuded tulenevad SiMi käskkirjast '*Siseministeeriumi valitsemisala infosüsteemide turvatestimise, turvanõrkuste haldamise ning nende logimise nõuete kord*'

Logimise nõuded arendustiimidele ning välistele partneritele (täitmist kontrollib meeskond, kes välist teenust tellib):

1. Logimiseks tuleb kasutada alus süsteemi võimalusi ja standardseid teeeke.
2. Logi peab olema loetav tekstilisel kujul UTF-8 kodeeringus.
3. Süsteemispetsiifilised andmed logikirjes peab võimaluse korral koostama JSON-formaadis.
4. Logitavates andmetes tuleb enne logifaili kirjutamist kodeerida kõik mittekuvatavad (*non-printable*) sümbolid, süsteemispetsiifilised andmed, logides sisalduvad kasutaja sisestatud väärtused ning välja- ja reaeraldajad (st kogu kasutaja sisendit peab olema võimalik taastada, va punktis 8 toodud andmed), välistamaks logisüste ja sellega seonduvaid ründeid. Logitavad andmeväljad eraldatakse tabulatsiooniga.
5. Juhul kui ühe päringu kohta tekib kirjeid mitmesse logisse, siis peab olema võimalik neid kirjeid ühise välja abil siduda. Selleks ei sobi kellaaeg, aga sobib näiteks unikaalne **päringu ID**.
6. Kõik väljanimed kirjeldused, parameetrite nimetused ja muu informatsioon peab olema võimalusel inglise keeles.
7. Logitud peavad olema kõik tegevused andmetega, sh:
 - 7.1. kõik autentimise katsed (hoolimata tulemusest);
 - 7.2. kõik kasutajate poolt algatatud tegevused;
 - 7.3. kõik taustaprotsesside tegevused;
 - 7.4. nii õnnestunud kui ka ebaõnnestunud tegevused.
8. Andmed, mida on keelatud logida:
 - 8.1. kasutajate autentimisega seotud saladust või salasõna teksti või räsi kujul;
 - 8.2. privaativõtmised;
 - 8.3. seansivõtme väärtus (nt seansi tokenid või -küpsised) – logida võib ainult seansivõtimest tuletatud räsi või muud pöördumatut tuletist;
 - 8.4. andmebaasidest tagastatud päringute täisvastused tekstilisel kujul – logida võib andmete tagastamise fakti või vastuse pikkust;
 - 8.5. biomeetriliste andmete väärtust taasesitamist võimaldaval kujul;
 - 8.6. andmed, mille logimise keeld tuleneb õigusaktidest (nt krediitkaardiandmed).
9. Sisendandmed peavad olema eristatavad rakenduselt endalt pärinevatest andmetest, kuid olema arusaadavad ilma rakenduse andmebaasita.
10. Logikirjed jaotatakse võimalusel järgnevalt (eraldi konfigureeritavatesse failidesse):
 - 10.1. Seansilogi - info kasutajate tuvastamise, rakendusse või kõrgema turvalisusega rakenduse osasse sisenemiste, väljumiste, seansi aegumise, tühistamise jmt kohta.
 - 10.2. Tegevuslogi - kogu informatsioon kasutajate ja taustaprotsesside tegevuste kohta koos sisendparameetritega (sh väliste ressursside kasutamise kohta). Tegevuse- ja seansilogi kirjes peab olema vähemalt:
 - 10.2.1. Silumislogi - arendajate jaoks vajalik debug info, toodangukeskkonnas peaks debug vaikimisi välja olema lülitatud;
 - 10.2.2. Turvalogi/auditlogi - turvalisusega seotud eeldefineeritud sündmused, mis võimaldavad tuvastada, mis tegevusi mis järjestuses tehti ning leida viiteid võimalikele turvaprobleemidele (SQL injection, IP muutus seansi keskel kui see pole lubatud, kasutaja käivitas käsu, mida tal ei ole lubatud käivitada jms). Sinna kuuluvad turvalisuse seisukohalt kriitilised sündmused (sisenemine, väljumine, kasutaja loomine, rolli muut(u)mine, seadistuste muut (u)mine) ning tegevused, mis toovad kaasa rahalisi või juriidilisi tagajärgi.
 - 10.3. Vealogi - erinevate veaolukordade info, mida võimalusel jaotada kaheks:
 - 10.3.1. tehniline vealogi - erinevad süsteemsed veateated (probleemid liidestega, süsteemsete taustatööde veateated, vead, mida ei ole püütud (unhandled exceptions));
 - 10.3.2. kasutajate vealogi - kasutajate tegevuse tõttu esile kutsutud vead mis on käsitletud (handled exceptions).
11. Logide spetsiifika (mida logitakse, kuidas sündmused logifailidesse on jagatud, rakendusspetsiifiliste logide struktuur ja detailid) peavad olema kirjeldatud teenuse dokumentatsioonis.
12. Logimine peab olema optimeeritud, st et peab vältima liigsete logiandmete edastamist logihaldussüsteemi ning välistama informatsiooni dubleerimist logides, juhul kui seda ei ole eraldi nõutud. Vajaduse korral filtreeritakse logid teenuses.
13. Logimisvahendid ja informatsioon logi kohta peab olema kaitstud volitamata muudatuste, hävitamise ja juurdepääsu eest.
14. Logisid peab logi edastav teenus saatma reaalaajas SMIT'i kesksesse logihaldussüsteemi. Kasutusel peab olema ühtne NTP (Network Time Protocol) ajateenus.
15. Logide keskne kogumine sisaldab:
 - 15.1. reaalaajas saadetavate logivoogude vastuvõtmist ja salvestamist;
 - 15.2. salvestatud logivoogude arhiveerimist olenevalt saadetavate logide tüübist ja neile kehtestatud säilitustähtaegadest.
16. Salvestatavad logiandmed signeeritakse digitaalselt.
17. Logiandmete turvaliseks edastamiseks SMITi kesksesse logihaldussüsteemi väljapoolt SMITi hallatavat taristut peab kasutama VPNi või mTLS-i ühendust.
18. Arhiiviväärtusega logide terviklus peab olema tagatud kolmanda poole usaldusteenuse (nt. TrueTrail) abil.
19. Tõestusväärtusega logisid ei tohi hoiustada ega töödelda rakenduse serveris või andmebaasis. Selline kirje on vaid informatiivse väärtusega ning seda logikirjena ei käsitata.
20. **Ligipääs logiandmetele**
 - 20.1. Logikeskkondadele ligipääs peab olema kitsendatud ja piiratud, logides sisalduvaid andmeid tohib töödelda vaid kasutaja, kellel on selleks õigus ja teadmusvajadus.
 - 20.2. Logisid on keelatud töödelda väljaspool lubatud keskkondi (kaasarvatud kopeerida). Arhiveeritud ja väljaspool logitaristut hoitavad või edastatavad logiandmed on alati krüpteeritud.
 - 20.3. Logisid ei tohi avalikustada ega jagada teistele osapooltele, kui selleks ei ole põhjendatud vajadust.
 - 20.4. Logide töötlemisel peab järgima andmete töötlemisel kehtivaid isikuandmete ning avaliku teabe töötlemist reguleerivaid õigusakte, sh täitma konfidentsiaalsuse kohustust nii töö- või teenistussuhte ajal kui ka pärast selle lõppemist.
21. Logide säilitustähtaegade määramine ja kustutamine peab vastama andmekogu põhimääruses või teenuse kokkuleppes sätestatud tingimustele.
22. Säilitustähtaja määramisel peab silmas pidama, et ressursikasutus oleks proportsionaalne ja mõistlik.
23. Kui logide säilitusajaga ei ole teenuse dokumentatsioonis täpsustatud, peab logisid hoidma käesoleva aasta kohta ning säilitama neid kuni ühe aasta.
24. Logimise puhul kehtivad vähemalt sama taseme turvanõuded, mida on rakendatud logitavale teenusele.
25. Kui rakenduse äriloojika ei vasta kehtestatud nõuetele tuleb tehnoloogilist lahendust eelnevalt infoturbeosakonnaga kooskõlastada.

Logikirjes peab sisalduma vähemalt teave, et vastata küsimustele: kes, millal, mida, kus ja kust süsteemis tegi ning mis oli tegevuse tulemus.

Logikirje miinimumnõuded on

1. Logikirjes (minimaalselt tegevus- ja seansilogi) peab sisalduma vähemalt teave, et vastata järgmistele küsimustele:
 - 1.1. **KES** on tegevuse teostaja, sealjuures:
 - 1.1.1. peab ta olema unikaalne vähemalt teenuse piires;
 - 1.1.2. peab ta olema seostatav füüsilise isikuga, kui see on võimalik;
 - 1.1.3. tema automaatprotsessid peavad olema selgelt tuvastatavad.
 - 1.2. **MILLAL** on ajamärgistus, mis sisaldab täpset sündmuse kuupäeva ning kellaaega, sealjuures peab aeg olema:
 - 1.2.1. vähemalt sekundi täpsusega;
 - 1.2.2. UTC ajavööndis;
 - 1.2.3. ajaformaadis ISO8601 koos ajavööndi infoga, näiteks formaat YYYY-MM-DDTHH:mm:ss.SSSZ.
 - 1.3. **MIDA** on logitava tegevuse või sündmuse liik või klass, näiteks kasutaja tuvastamine, administreerimine, operatsioon ja kasutus, ning liigi või klassi tegevuse detailid. Märgitakse:
 - 1.3.1. üheselt tuvastatav viide objektile või selle komponendile, mida kasutati;
 - 1.3.2. tegevuse tüüp, näiteks *login*, *timeout*, *search*, *request*, *query*, või kasutatud meetod ja nende sisendandmed;
 - 1.3.3. tegevusega seotud muud andmed ja sisendväärtused, mida tegevuse käigus töödeldi või mis on olulised, näiteks failide nimed, päringu objektid, autentimismeetod.
 - 1.4. **KUS** on süsteemi identifikaator, mille abil on võimalik teha kindlaks täpne rakendus ja selle instants, mille suhtes tegevus tehti.
 - 1.5. **KUST** on seadme unikaalne identifikaator, näiteks nimi, IP-aadress või seadme sertifikaat, kust tegevus toime pandi, sealjuures peab:
 - 1.5.1. identifikaatori abil olema võimalik üheselt tuvastada seade, kust sündmus toime pandi;
 - 1.5.2. IP-aadressi puhul olema tuvastatav lõppseadme IP-aadress.
 - 1.6. **TULEMUS** – kui ei ole kokku lepitud teisiti, siis päringute vastuseid täies mahus ei salvestata. Logisse peab kirjutama tulemust kirjeldavad andmed, näiteks tulemuse tüüp (success, attempt, failure, error), vastuse suurus (nii baitides kui ka ridade arvuna).

Logikirje elementide soovituslik järjestus:

{when}\t{where}\t{what}\t{whence}\t{who}\t{procid?}\t{result}\t{msg-payload?}