ALGTEKST-TERVIKTEKST

Kinnitatud kantsleri 18.10.2024 korraldusega nr 183

Redaktsiooni jõustumise kuupäev: 18.10.2024

Logimise poliitika

Sisukord

[1 Üldine 2](#_Toc178077824)

[2 Mõisted 2](#_Toc178077825)

[3 Käsitlusala 2](#_Toc178077826)

[4 Põhimõtted 2](#_Toc178077827)

[5 Eesmärgid 3](#_Toc178077828)

[6 Logide haldamine 3](#_Toc178077829)

[6.1 Logitavad andmed 3](#_Toc178077830)

[6.2 Logitavad sündmused 3](#_Toc178077831)

[6.3 Logiandmete kaitse 4](#_Toc178077832)

[6.4 Logiandmete analüüs 4](#_Toc178077833)

[7 Järelevalve 5](#_Toc178077834)

[8 Dokumentatsioon ja ülevaatus 5](#_Toc178077835)

[9 Rakendamine 5](#_Toc178077836)

**1 Üldine**

Tallinna Tehnikaülikooli (edaspidi ülikool) logimise poliitika on koostatud vastavuses ISO 27001:2022 standardi nõuete ning ülikooli infoturbe poliitikaga. Logimise poliitika eesmärk on tagada logide tekkimine, säilitamine ja analüüsimine viisil, mis toetab ülikooli infoturbe aluspõhimõtteid ja eesmärke, kaitstes infotehnoloogilisi varasid ning teavet, tagades nende käideldavuse, tervikluse ning konfidentsiaalsuse (sealhulgas vajadusel õigusliku tõendusmaterjali saamiseks logide kaudu).

**2 Mõisted**

**Logid** – süsteemi või rakenduse tegevuste automaatselt või käsitsi loodud salvestused, mis sisaldavad infot toimingute, sündmuste, muudatuste, turvaintsidentide ja muude asjaolude kohta.

**Logimine** – tegevuste, sündmuste ja muudatuste salvestamise protsess.

**Logiagregatsioon** – erinevatest allikatest pärit logide koondamine keskse süsteemi kaudu, mis võimaldab põhjalikumat analüüsi ja järelevalvet.

**Anomaaliate tuvastamine** – protsess, mille käigus tuvastatakse logidest kõrvalekalded tavapärasest käitumisest, mis võivad viidata turvaintsidentidele.

**3 Käsitlusala**

Logimise poliitika hõlmab kõiki ülikooli kasutuses olevaid infosüsteeme ja infotehnoloogilisi varasid, kaasa arvatud neid, mida hallatakse kolmanda osapoole poolt. Poliitika reguleerib logide loomist, säilitamist ja analüüsi, sealhulgas erandolukordi, tõrkeid ja muid olulisi sündmusi. Poliitika kehtib kõikidele infosüsteemi komponentidele ning nendega seotud isikutele, s.t. ülikooli töötajad, üliõpilased ja kolmandad osapooled. Logimise eest vastutavad isikud tagavad logide korrektse ja turvalise loomise, säilitamise ja analüüsi.

**4 Põhimõtted**

Kõik infosüsteemid ja infotehnoloogilised varad peavad genereerima logisid vastavalt määratletud vajadustele ja turvanõuetele. Logisid tuleb säilitada turvaliselt ja konfidentsiaalsena, piisavalt pikka aega, et toetada potentsiaalsete turvaintsidentide uurimist ja lahendamist. Juurdepääs logidele peab olema piiratud ainult volitatud isikutega, kellel on põhjendatud vajadus. Logisid tuleb regulaarselt analüüsida, et tuvastada võimalikke turvaintsidente, rikkumisi ja ebatavalist käitumist. Logid peavad olema kaitstud volitamata muutmise ja kustutamise eest. Logimise konfiguratsioon peab olema dokumenteeritud ja regulaarselt üle vaadatud, tagamaks selle asjakohasust ja tõhusust. Logide säilitamise periood ja regulatiivsed nõuded on määratud JIRA varade moodulis iga infosüsteemi või infotehnoloogilise vara kohta.

Ülikoolis kogutakse erinevate info- ja andmesüsteemide logisid, mis talletavad nimetatud süsteemide toimimist, kasutust ja muudatusi. Logisid tuleb jälgida regulaarselt ning nende muutmine kasutajate poolt ei ole lubatud, s.t peab olema keelatud olekus.

Logimise- ja monitooringutööriistad peavad vastama ülikooli infoturbe standardile ja olema regulaarselt uuendatud.

Infosüsteemid ja infotehnoloogiliste varade logid koondatakse kesksesse logihaldusesse ehk toimub logimisagregatsioon tagamaks võimekust tuvastada keerukamaid turvaintsidente.

Logide kogumise, säilitamise ja analüüsi eest vastutavad isikud peavad olema teadlikud oma vastutusest ning nende tegevus peab olema dokumenteeritud.

**5 Eesmärgid**

Logide säilitamise ja haldamise eesmärgiks on tagada süsteemide ja rakenduste tegevuste läbipaistvus ja auditeerimisvõimekus, mis võimaldab kiiret tuvastamist ja reageerimist turvaintsidentidele ja nende kasutamist muudel eesmärkidel, nagu analüüs ja talitluspidevuse tagamine.

Logide haldajatel on kohustus aidata kaasa regulatiivsete nõuete järgimisele ja auditite läbiviimisele, pakkudes vajalikke logiandmeid. Logisid kasutatakse ka turvameetmete tõhususe hindamiseks ja parandamiseks, toetades proaktiivset turvalisuse juhtimist.

**6 Logide haldamine**

**6.1 Logitavad andmed**

Iga sündmuselogi peab sisaldama vähemalt järgmist teavet:

* kasutaja ID-d;
* Infosüsteem või infotehnoloogiline vara;
* süsteemi tegevused, sh selgelt tuvastatavad automaatprotsessid;
* autentimise ning sisse- ja väljalogimise sündmused: kui autentimine toimub läbikolmanda osapoole identiteedihaldusteenuse,siis selliste sündmuste logimine ja haldamine toimub vastava teenuse logide kaudu. Rakenduse enda logidesse neid sündmusi ei talletata;
* asjakohaste sündmuste kuupäevad, kellaajad ja asjakohased üksikasjad
	+ Tuleb kasutada järgnevat standardit: UTC ajavööndis ning ISO8601 formaadis YYYY-MM-DDTHH:mm:ss.SSSZ;
* sisendväärtused (nt failide nimed, päringu objektid, autentimismeetod);
* seadme identifitseerimisandmed, süsteemi identifikaator ja asukoht;
* logitava sündmuse või tegevuse liik või klass (nt kasutaja tuvastamine, administreerimine ning liigi detailid);
* võrguaadressid ja protokollid;
* korrelatsiooni ID: kasutatud sündmuste ahela jälgimiseks;
* sessiooni ID: kui rakendatakse sessioonipõhist jälgimist.

**6.2 Logitavad sündmused**

Järgmised sündmused tuleb logida (välja arvatud juhul, kui see on tehniliselt võimatu ja erandina kooskõlastatud):

* edukad ja tagasilükatud süsteemi juurdepääsu katsed, sh mittekohaldatavad autentimiskatsed ja *bruteforce* rünnakud;
* edukad ja tagasilükatud andmetele ja muudele ressurssidele juurdepääsu katsed;
* kui rakendusel on olemas administraatori liides või muud vahendid süsteemi konfiguratsiooni muutmiseks, siis tuleb logida kõik edukad ja tagasilükatud süsteemi konfiguratsiooni muutmise katsed. Juhul, kui konfiguratsiooni muutmine toimub rakendusest väljaspool (nt serveri või infrastruktuuri tasemel), jääb selle logimine süsteemi halduse või infrastruktuuri logide vastutusalasse;
* infosüsteemi või infotehnoloogilise vara poolt loodud hoiatused ja veateated;
* andmeteeksportimise ja –importimise toimingud;
* privileegide kasutamine;
* külastatud failid ja juurdepääsu liik, sealhulgas oluliste andmefailide kustutamine;
* juurdepääsukontrollisüsteemi poolt tõstetud häiresignaalid;
* turvasüsteemide, näiteks viirusetõrjesüsteemide ja sisse tungimise tuvastamise süsteemide aktiveerimine ja deaktiveerimine;
* identiteetide loomine, muutmine või kustutamine, sh rollide muudatused;
* kasutajate poolt rakendustes tehtud tehingud. Sealhulgas need kasutajad, kus kasutaja on tehniline kasutaja (rakendus), mis teeb automatiseeritud toiminguid;
* logide vastuvõtuaeg nende haldamise ja töötlemise süsteemis;
* logide haldamise ja töötlemise programmide ja rakenduste kasutamine.

**6.3 Logiandmete kaitse**

Kasutajatel, sealhulgas privilegeeritud juurdepääsuga isikutel, ei tohi olla õigust oma tegevuse logisid kustutada või deaktiveerida (v.a juhud, kus ei ole tehniliselt võimalik piirata). Kõik logiandmed talletatakse ja kaitstakse volitamata juurdepääsu eest, pääsuõigused logiandmetele dokumenteeritakse vastavalt infotehnoloogiliste varade juurdepääsuhalduse korrale.

Logiteavet tuleb kaitsta volitamata muutmise eest, sealhulgas tuleks vältida:

* logide edastamisel logimisagregatsiooni tuleb kasutada krüpteeritut edastamist, nt kasutades TLS protokolli;
* salvestatud sõnumitüüpide muudatuste lubamist;
* redigeeritavate või kustutatavate logifailide võimaldamist;
* sündmuste salvestamata jätmist või minevikus salvestatud sündmuste ülekirjutamist, kui logifaili hoidev andmekandja maht on täitunud;
* kõik logimise seadistused ja protseduurid peavad olema versioonikontrollitud ja ajakohastatud vastavalt muudatustele süsteemides ja regulatsioonides.

Logide kaitsmiseks võib kasutada järgmisi meetodeid:

* krüptograafiline räsimine;
* salvestamine ainult kirjutuskaitstud failis;
* salvestamine avalikus läbipaistvusfailis (public transparency file).

Logide kättesaadavus ja terviklikkus peab olema tagatud ka andmekao või süsteemirikete korral. Logifailide varukoopiad peavad olema kaitstud samade turvameetmetega nagu esmased logifailid.

Logid, mida tuleb säilitada pikema perioodi jooksul, tuleb arhiveerida vastavalt andmetele ja/või regulatsioonidega kehtestatud nõuetele. Logide säilitustähtajad on toodud välja määratletud infosüsteemi või muu infotehnoloogilise vara juures.

Kui organisatsioonil on vaja vigade tuvastamiseks saata kolmandale osapoolele süsteemi- või rakenduslogisid, tuleks logidest võimaluse korral eemaldada nõutud andmed, kasutades andmete maskeerimise tehnikaid. Enne kolmandale osapoolele logide saatmist tuleks eemaldada kasutajanimed, IP-aadressid, hostinimed, organisatsiooni nimi ja muu asjasse puutumatu informatsioon.

**6.4 Logiandmete analüüs**

Logianalüüs hõlmab infoturbe sündmuste analüüsi ja tõlgendamist, et tuvastada ebatavaline tegevus või anomaalne käitumine, mis võib viidata võimalikule kompromiteerimisele. Infotehnoloogiaosakonna infoturbetalitus analüüsib ülikooli logiandmeid. Infoturbetalitus kasutab selleks automatiseerituid vahendeid, mis tuvastavad ja hoiatavad anomaaliate ja potentsiaalsete turvaintsidentide eest.

Logianalüüsi tulemused peavad olema dokumenteeritud ja regulaarselt üle vaadatud, et hinnata ja parandada logimise efektiivsust. Logianalüüsi tulemused integreeritakse infoturbe riskihalduse protsessi, et tuvastatud riskid ja nõrkused saaksid asjakohaselt hinnatud ja käsitletud.

**7 Järelevalve**

Infoturbejuht koordineerib logimise poliitika rakendamist, järelevalvet ja regulaarset läbivaatamist. Infoturbejuht korraldab regulaarsed harjutused ja testid, et tagada logimissüsteemide ja -poliitikate tõhusus.

Korrapäraselt viiakse infoturbe juhi koordineerimisel läbi järelevalvet ja auditeid, et tagada logimise poliitika nõuete täitmine.

Avastatud mittevastavuste korral rakendatakse parandusmeetmeid ning need dokumenteeritakse.

**8 Dokumentatsioon ja ülevaatus**

Kõik logimise seadistused ja protseduurid dokumenteeritakse selgelt ja on kättesaadavad volitatud isikutele. Logimise poliitikat vaadatakse vähemalt kord aastas läbi ja ajakohastatakse, et tagada selle asjakohasus ja tõhusus.

**9 Rakendamine**

Käesoleva logimise poliitika rakendamine ja järgimine on kõigi ülikooli töötajate ja kolmandate osapoolte kohustus tagamaks ülikooli infosüsteemide ja andmete turvalisus.

Poliitika peab olema kättesaadav kõikidele asjassepuutuvatele isikutele ning neile peab olema korraldatud poliitika tutvustamine ja koolitus.

Poliitika vaadatakse üle ja uuendatakse vähemalt kord aastas või vastavalt vajadusele, et tagada selle vastavus muutuvatele regulatiivsetele nõuetele ja tehnoloogia arengule.