ALGTEKST-TERVIKTEKST

Kinnitatud kantsleri 03.06.2024 korraldusega nr 126

Redaktsiooni jõustumise kuupäev: 03.06.2024

Turvanõrkuste haldamise kord

Sisukord

[1 Üldine 1](#_Toc168301397)

[2 Käsitlusala 1](#_Toc168301398)

[3 Turvanõrkuste haldamine 1](#_Toc168301399)

[4 Turvanõrkuste tuvastamine 1](#_Toc168301400)

[5 Turvanõrkuste hindamine ja prioriteetide määramine 1](#_Toc168301401)

[6 Turvanõrkuste leevendamine ja kõrvaldamine 1](#_Toc168301402)

[7 Testimine 2](#_Toc168301403)

[8 Erisused 2](#_Toc168301404)

[9 Järelevalve 2](#_Toc168301405)

# Üldine

Turvanõrkuste haldamise poliitika eesmärk on määratleda poliitika ja kontrollmeetmed, mis on vajalikud tehniliste haavatavuste (vulnerabilities) hindamiseks ja haldamiseks Tallinna Tehnikaülikooli (edaspidi: ülikool) infosüsteemides ja infotehnoloogilistes varades, eesmärgiga saavutada ülikooli poolt aktsepteeritud riskitase.

# Käsitlusala

Käesolev poliitika kehtib kõikidele ülikooli infosüsteemidele ja infotehnoloogilistele varadele, protsessidele ja osalistele, kes kuuluvad ülikooli infoturbe halduse süsteemi käsitlusalasse.

# Turvanõrkuste haldamine

Turvanõrkuste haldamise eelduseks on infosüsteemide ja infotehnoloogiliste varade register. Turvanõrkuste haldamise protsess sisaldab varade arvestust, turvanõrkuste tuvastamist, hindamist, prioriteetide määratlemist, leevendamist, kõrvaldamist ja testimist.

# Turvanõrkuste tuvastamine

Turvanõrkuste tuvastamiseks kasutatakse automaatseid nõrkuste tuvastamise vahendeid, mis skaneerivad infosüsteeme ja infotehnoloogilisi varasid avastamaks turvanõrkusi. Turvanõrkuste tuvastamist korraldab infoturbejuht koos infotehnoloogia osakonda kuuluva infoturbe talitusega.

Infoturbe talituse poolt kasutatavad turvanõrkusi tuvastavad tehnoloogilised lahendused on võetud varana arvele ning on juurde märgitud turvanõrkuste teabeallikad.

Täiendavalt skaneerib ülikooli infosüsteeme ja infotehnoloogilisi varasid Riigi Infosüsteemide Amet (CERT.EE), kes teavitab infoturbe talitust võimalikkest haavatavustest.

# Turvanõrkuste hindamine ja prioriteetide määramine

Avastatud turvanõrkused hinnatakse lähtuvalt standardsetest haavatavuste hindamise metoodikatest (CVE, CVSS, OVAL, SCAP, VMF, PVG, jt). Antud hinnangud on osaliselt automatiseeritud lähtuvalt kasutatavatest infotehnoloogilistest vahenditest. Infoturbe talitus lähtuvalt hinnangutest määratleb haavatavuste prioriteedi (riskitaseme), sh leevendusmeetmete rakendamise aja (Tabel 1 Haavatavuste riskitasemed ja leevendusajad).

Infoturbe talitus informeerib avastatud turvanõrkustest ja selle riskitasemest infosüsteemi äriprojektijuhti ja süsteemiadministraatorit või infotehnoloogilise vara omaniku esimesel võimalusel alates selle avastamisest, kuid mitte hiljem kui kolme tööpäeva jooksul.

Tabel 1 Haavatavuste riskitasemed ja leevendusajad

|  |  |
| --- | --- |
| Haavatavuste riskitase | Leevendusmeetme rakendamise aeg |
| Kriitiline | Alla 3 päeva |
| Kõrge | Alla 7 päeva |
| Keskmine | 90 päeva |
| Madal | 180 päeva |

# Turvanõrkuste leevendamine ja kõrvaldamine

Infosüsteemi või infotehnoloogilise vara turvanõrkuste leevendamise ja kõrvaldamise eest vastutab süsteemiadministraator. Kui süsteemiadministraator on määramata, siis kõrvaldamise eest vastutab infosüsteemi omanik või äriprojektijuht.

Kriitiliste ja kõrgete turvanõrkuse avastamise ja teavituse saamise järel tuleb asuda koheselt, kuid mitte hiljem kui leevendusmeetme rakendusaeg, rakendama leevendusmeetmeid turvanõrkusest tuleneva riski maandamiseks. Kui on olemas juba teadaolev turvaparandus või uuendus, siis tuleks kasutada seda turvanõrkuse leevendamiseks või kõrvaldamiseks. Juhul kui uuendust ei ole võimalik paigaldada tehniliste piirangute või tootja ei ole asjakohast parandust välja andnud, siis tuleb asuda rakendama järgnevaid leevendusmeetmeid:

* Lülitada välja nõrkust puudutav infosüsteem või infotehnoloogiline vara;
* Piirata ligipääs infosüsteemile või infotehnoloogilisele varale võrgutasandil;
* Nõrkust sisaldavad infosüsteemid või infotehnoloogilised varad varjestada sobivate liiklusfiltritega:
* Muud asjakohased leevendusmeetmed maandamaks riskitaset.

Turvanõrkuste kõrvaldamiseks tuleb kasutada uuendusi, mis pärinevad usaldusväärsetest allikatest ning enne kasutuselevõttu tuleb hinnata ja testida nende toimivust.

Keskmiste ja madalate turvanõrkuste puhul tuleb leevendusmeetmed rakendada mitte hiljemalt kui on välja toodud rakendamise aeg. Võimalusel rakendada selle aja jooksul meetmed, mis turvanõrkuse lõplikult kõrvaldavad.

Juhul kui infosüsteemi süsteemiadministraator või äriprojektijuht või infotehnoloogilise vara omanik ei ole peale teavitamist asunud rakendama kriitiliste või kõrgete haavatavuste riskitasemete juures leevendusmeetmeid ettenähtud aja jooksul, siis infoturbejuhil või tema volitatud isikutel on õigus asuda leevendusmeetmeid rakendama iseseisvalt. See võib tuua kaasa infosüsteemi või infotehnoloogilise vara käideldavuse kao. Sellisel juhul infoturbe talitus ei vastuta võimalikke kaasnevate kahjude eest.

Kui infosüsteemi administraator või äriprojektijuht või infotehnoloogilise vara omanik on rakendanud leevendusmeetmed või kõrvaldanud turvanõrkuse, siis tuleb sellest kirjalikult informeerida infoturbe talitust. Seejärel infoturbe talitus teeb järelkontrolli veendumaks nõrkuse kõrvaldamisest või selle leevendamisest.

# Testimine

Turvanõrkuste halduse etalontoimivuse juurde käivad regulaarsed turva- ja läbistustestid, mida viiakse kriitiliste süsteemikomponentide peal läbi vähemalt kord aastas või suuremate muudatuste korral usaldusväärsete väliste partnerite poolt. Testimiste tulemustest lähtuvalt tuleb algatada leevendusmeetmete rakendamine ja turvanõrkuste kõrvaldamine vastavalt haavatavuste riskitasemele.

# Erisused

Mõningatel juhtudel on vajalik kõrvalekalle haavatavuste haldamise protseduurist tehniliste piirangute või kolmandate osapoolte lepinguliste kohustuste tõttu. Sellised erandid tuleb kirjalikult dokumenteerida ning need kinnitatakse infoturbejuhi poolt.

# Järelevalve

Turvanõrkuste haldamise korra rakendamise järelevalvet teeb siseaudit lähtuvalt siseauditi tööplaanist, kuid mitte harvem kui kord kolme aasta jooksul.