Standaard voor Systeemhardening

Leids Universitair Medisch Centrum (LUMC)

Versiebeheer

Versie	Auteur	Datum	Opmerking
0.1	Michel Dieben	22-12-2020	Eerste opzet
0.2	Michel Dieben	31-05-2021	Concept voor ISMS LUMC
0.3	Sylvia Vogelaar	27-09-2021	Aanpassing aan LUMC breed.
0.9	Michel Dieben	08-10-2021	Eisen voor internet facing systemen toegevoegd
1.0	Juriaan Rijnbeek	08-10-2021	Beoordeeld en definitief bevonden.
1.5	Michel Dieben	17-11-2023	Aanvulling technische eisen website
1.9	Michel Dieben	30-05-2024	Splitsing beleidsregels internet facing systemen naar ISMS126 - Webapplicaties

INHOUDSOPGAVE

1. INLEIDING

Om de veiligheid van het LUMC netwerk te garanderen behoren op alle aangesloten systemen passende maatregelen te zijn getroffen om te voorkomen dat het systeem door ongeautoriseerde derden benaderd of gebruikt kan worden.

2. STANDAARDEN SYSTEEMHARDENING

Systeemeigenaren behoren er zeker van te zijn dat alle onderdelen waarvoor zij verantwoordelijk zijn aan de volgende beveiligingseisen voldoen:

- Alle gastaccounts zijn verwijderd;
- Alle ongebruikte poorten zijn gesloten;
- Alle standaardwachtwoorden zijn gewijzigd;
- Alle wachtwoorden voldoen aan het beleid sterke wachtwoorden;
- Alle beheeraccounts zijn significant beveiligd en er vindt logging plaats conform NEN7513;
- Alle onnodige services zijn uitgeschakeld;
- Fysieke toegang is significant beveiligd en beheerd;
- Alle onderdelen worden zo snel mogelijk gepatched, actief onderhouden en bijgewerkt volgens de richtlijnen van de leverancier en best practices van de industrie;
- Het systeem is voorzien van actieve endpoint protection.

*Onderdelen: fysieke en virtuele systemen die gezamenlijk deel uitmaken van het systeem als geheel.

*Systeem: verzameling van onderdelen dat bij elkaar als één geheel wordt gebruikt of beschouwd.

2.1 TOELICHTING EXTERNE TOEGANG

Voor het gebruik van externe toegang (zoals via SSH of RDP) gelden de volgende eisen:

- Er wordt gebruik gemaakt van public/private key encryption zoals bijvoorbeeld SSH keys. Uitsluitend gebruik maken van gebruikersnaam/wachtwoord is niet toegestaan;
- Er wordt gebruik gemaakt van Access Control Lists waarin gespecificeerd wordt welke gebruikers, systemen of IP-adressen toegang hebben.

Voor specificaties van X.509 certificaten zie het Encryptiebeleid en de Standaard voor toepassing cryptografie binnen het LUMC.

2.2 TOELICHTING INTERNET FACING SYSTEMEN

Voor systemen die via internet te benaderen zijn (zoals bijvoorbeeld webapplicaties, API's, SFTP servers, enz.) gelden aanvullende eisen. Deze zijn beschreven in ISMS126 – Webapplicaties.