Document ID (autonummer): 048169, Titel: MIT-Richtlijnen-Beveiligen beheerinterfaces, te gebruiken tot 24 uur na, Huidige datum: 26-02-2026, Huidige tijd: 10:01 Versie: 3

Samenvatting / Doel

Beheerinterfaces worden gebruikt om systemen of applicaties te beheren. Het spreekt voor zich dat dit voor kwaadwillende personen geliefde omgevingen zijn om toegang toe te krijgen. Onder beheerinterfaces worden alle mogelijke vormen van toegang bedoeld die gebruikt kunnen worden bij het beheren en configureren van apparatuur en software.Denk hierbij aan management websites, BIOS toegang op werkplekken en diverse manieren van remote management van Windows.
Doelstelling van dit document is het aanreiken van een aantal aanbevelingen die gebruikt kunnen worden bij het inrichten en beveiligen van beheerinterfaces.

Gerelateerde informatie

Advies

Als advies gewenst is bij het implementeren van de aanbevelingen uit dit document dan kan contact opgenomen worden met het MIT Security Operations Center (SOC).
Hier kun je ook terecht met overige vragen of opmerkingen met betrekking tot de genoemde aanbevelingen.

Het SOC is via mail bereikbaar op soc@mumc.nl of telefonisch via tst. 72700.

Uitvoerenden en verantwoordelijken (evt. bevoegdheden)

Alle medewerkers van het MUMC+, leveranciers of derden die betrokken zijn bij het inrichten en beheren van apparatuur en/of software die voorzien zijn van een beheerinterface

Werkwijze

Aanbeveling beveiligen beheerinterfaces

Maak bij het inrichten en beveiligen van beheerinterfaces daar waar mogelijk gebruik van onderstaande aanbevelingen.

1. **Fysieke beveiliging**

   1. 1. Zorg dat fysieke toegang, ook tot beheerinterfaces, alleen mogelijk is voor gemachtigde personen.

2. **Beheerinterface enkel bereikbaar via beheer omgeving (al dan niet remote), niet voor het gehele netwerk**

   2.1. Toegang tot beheerinterfaces is alleen mogelijk vanuit dezelfde OTAP-beheeromgeving
   2.2. Pas waar mogelijk out-of-band management toe. Bij out-of-band management wordt gebruik gemaakt van een aparte interface voor het uitvoeren van beheerwerkzaamheden. Een voorbeeld hiervan is een managementnetwerk of een usb-poort voor het uitvoeren van beheer.
   2.3. Indien een host, appliance, server of service een eigen firewallmodule of access control list aanbiedt, dient deze op zo veilig mogelijke wijze te worden geconfigureerd, met minimale toegang tot de dienst die het apparaat aanbiedt.

3. **Versleutelde communicatie met de beheerinterface is vereist**

3.1. Gebruik versleuteling conform algemeen geaccepteerde standaarden. Een goed startpunt hiervoor is het document: "ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)" van het Nationaal Cyber Security Centrum (NCSC).
3.2. Gebruik geen self-signed certificaten, maar maak gebruik van certificaten die zijn uitgegeven door de Certificate Authority (CA) van het MUMC+ of een vertrouwde externe CA.

4. Authenticatie

4.1. Wijzig z.s.m. de standaard accounts en/of wachtwoorden.
4.2 .Toegang tot beheerinterfaces is alleen mogelijk door geauthentiseerde beheerders met een B-account.
4.3. Gebruik waar mogelijk encrypted Active Directory (AD) authenticatie.
4.4 .Zorg dat voor kritische systemen (backup-servers, vSphere) er een lokaal 'backdoor' account beschikbaar is in gevallen dat AD niet beschikbaar is.
4.5. Lokale accounts moeten voldoen aan het MUMC-wachtwoordbeleid zoals beschreven in "Richtlijn voor het gebruik van wachtwoorden", Zenya 004093
4.6. Er is een time-out policy actief, hierdoor wordt een sessie nadat deze een bepaalde tijd inactief is geweest verbroken.
4.7. Gebruik waar mogelijk een banner die juridisch voldoet.
4.8. Noteer accountgegevens en wachtwoorden in een password management tool en zet deze nooit in (beheer)documenten. Deel deze gegevens nooit met onbevoegden.

5. Autorisatie

5.1. Maak indien mogelijk gebruik van Identity Management.
5.2. Gebruik autorisaties op basis van het "need to know" principe, deel niet meer bevoegdheden uit dan nodig.
5.3. Maak indien mogelijk gebruik van Role Based Access Control (RBAC).

6. Datum en tijd

6.1. Gebruik indien mogelijk de MUMC+ NTP servers en de juiste tijdzone bij het instellen van datum en tijd.
6.2. Indien NTP niet mogelijk is: stel de tijd handmatig in en controleer de tijd regelmatig

7. Onveilige of onnodige services en protocollen

7. 1. Schakel alle niet gebruikte services uit.
7.2. Schakel alle niet gebruikte communicatie protocollen uit

8. SNMP toegang (Simple Network Management Protocol)

8.1. SNMP is uitgeschakeld indien het niet wordt gebruikt.
8.2. SNMP-toegang mag enkel versleuteld aangeboden worden.
8.3. De standaard Read-Only en Read-Write communities moeten gewijzigd worden

9. Firmware /software actueel houden

9.1. Zorg dat bij een nieuwe relevante security release de firmware/software actueel gehouden wordt, met inachtneming van het OTAP-proces.
9.2. Gebruik veilige protocollen en werkwijzen om firmware/software te down- en uploaden.
9.3. Gebruik verificatie mechanismen (bijvoorbeeld MD5 en SHA1 hashes) om de integriteit van updatebestanden te controleren alvorens ze te installeren.

9.4. Scan datadragers (bv. usb apparaten) en updatebestanden op virussen of andere malware, ook als deze van leveranciers komen.

10. Accounting (logging)

10.1.Gebruik waar mogelijk logging.(inbraakpogingen dienen (centraal) gemonitord te worden.
10.2. Zorg voor adequate logging van toegangspogingen.
10.3. Zorg voor adequate logging van uitgevoerde handelingen.
10.4. Sla deze logs indien mogelijk centraal op.
10.5. Voer regelmatig controles uit op de logging.

11. Medewerker uit dienst, einde inhuur, functiewijziging, versneld intrekken van rechten

11.1. Alle wachtwoorden die bij de medewerker bekend zijn, moeten worden gewijzigd.
11.2. Alle accounts die de medewerker heeft, moeten worden geblokkeerd of verwijderd.
11.3 Zorg dat de medewerker geen gebruik kan maken van diensten om zijn account zelf weer te activeren.

12. Afvoer, retour leverancier, storing

12.1. Apparatuur die om welke reden dan ook wordt afgevoerd, dient te worden ontdaan van alle configuraties, logfiles, backups en dergelijke.
12.2. Gebruik bij het veilig afvoeren van apparatuur de door het MUMC+ gehanteerde standaarden beschreven in “Beleid Afvoeren van ICT middelen en datadragers”, Zenya 004516 en “Afvoeren van ICT middelen en datadragers voor gebruikers” Zenya 005414.

Bronvermeldingen

--