Best practice voor het veilig gebruik van accounts

Dagelijks worden digitale aanvallen gepleegd op cruciale systemen van zorginstellingen, maar omdat hackers al lange tijd gebruik maken van dezelfde aanvalstechnieken kun je daar ook iets aan doen. Door bijvoorbeeld alert te zijn en veilig en bewust om te gaan met je accounts. Tips hiervoor vind je hiernaast.

Vooral privileged accounts zijn erg gewild bij hackers, maar ook accounts met minder verregaande rechten.

Privileged accounts en accounts met uitgebreide en hoge rechten

Gebruik je een account waarmee je bijvoorbeeld IT-systemen, applicaties, infrastructuur en software beheert of een account waarmee je belangrijke handelingen kunt doen in een systeem? Of gebruik je een local admin account, een domain admin account of een account dat goedkeuring geeft op financiële uitgaven? Voorkom dan misbruik door hackers door het toepassen van tips hiernaast.

Gebruik verschillende typen accounts

1. Gebruik een priviliged account alleen voor het uitvoeren van de afgesproken taken en NIET voor normale gebruiker activiteiten zoals bijvoorbeeld web-browsen, mailen, downloaden en experimenteren met software die niet door de organisatie goedgekeurd is.

2. Zorg dat serverbeheer accounts en domain admin accounts niet in kunnen loggen op systemen waar normale gebruiker activiteiten op worden uitgevoerd (mailen, browsen etc).

3. Beperk gebruik van domain admin accounts tot domeincontrollers en limiteer gebruik tot servers waar het strikt noodzakelijk is. Gebruik voor andere beheertaken op andere systemen, andere accounts.

4. Gebruik voor het beheer van cloud-applicaties of infrastructuur andere accounts dan lokale accounts.

Rechten

1. Volg interne procedures voor het intrekken, toekennen en auditen van rechten en het aanmaken van accounts.

2. Geef accounts alleen die rechten die nodig zijn voor het uitvoeren van de taak waarvoor het account bedoeld is.

3. Geef service accounts alleen die rechten die noodzakelijk zijn voor de taak.

4. Geef gebruikers en beheerders geen local admin rechten. Gebruik een local admin account met een uniek wachtwoord dat alleen bruikbaar is op één systeem.

Wachtwoorden

1. Gebruik voor privileged accounts complexe en unieke wachtwoorden. Overweeg hiervoor een wachtwoordmanager. Indien dit niet mogelijk is voor bepaalde accounts, gebruik dan een lange onthoudbare wachtwoordzin van minstens 3 willekeurige woorden.

2. Gebruik niet dezelfde wachtwoorden voor verschillende accounts op verschillende systemen of platformen.

3. Zorg voor een sterke wachtwoordlengte (idealiter 25+ tekens) en complexiteit voor service accounts en zorg ervoor dat deze wachtwoorden periodiek verlopen en veranderen. Overweeg "Group Managed Service Accounts" te gebruiken die dit automatiseren.

4. Verander wachtwoorden van default accounts van systemen of verwijder default accounts.

Algemeen

1. Gebruik multifactorauthenticatie (MFA), ook voor leveranciersaccounts.

2. Voorkom dat credentials uit het geheugen gestolen kunnen worden. Overweeg bijvoorbeeld credential guard, remote credential guard, restricted admin en gebruik van de "protected user group".

3. Als je klaar bent met je werkzaamheden, dan log je altijd netjes uit.

Overige accounts

Ook accounts met minder verregaande rechten zijn interessant voor hackers, omdat ze via deze accounts alsnog toegang kunnen krijgen tot de accounts met meer rechten. Voorkom ook misbruik van deze accounts door onderstaande tips toe te passen.

1. Gebruik een sterke wachtwoordzin van minstens 3 willekeurige woorden.

2. Gebruik multifactorauthenticatie (MFA).

Deze factsheet is tot stand gekomen door een samenwerking van:

ZCERT COMPUTER EMERGENCY RESPONSE TEAM VOOR DE ZORG

Stichting Samenwerkende Rijnmond Ziekenhuizen SRZ