Informatie

Windows CIS Hardening benchmark en risico’s

Table of contents

Hardening

Standaard ofwel default configuraties van besturingssystemen op bijvoorbeeld servers en laptops zijn niet ontworpen met een primaire focus op veiligheid maar op maximale bruikbaarheid. Dit houdt in dat systemen met een standaard configuratie extreem kwetsbaar zijn en eenvoudige doelwitten vormen voor cybercriminelen.

Het aanpassen van configuratie-instellingen om risico's te verlagen wordt ook wel hardening genoemd. Het gaat hierbij onder andere om:

- Het uitschakelen of verwijderen van overbodige functies en gebruikersaccounts
- Het toekennen van veilige waarden aan beveiligingsinstellingen
- Het wijzigen van standaard wachtwoorden op systemen

Een systeem dat gehardend is, geeft maximale bescherming tegen cybercriminelen door kansen op een incident te verlagen. Als zich toch een incident voordoet blijft schade zoveel mogelijk beperkt, en daarmee ook de kosten (en tijd) voor herstel.

Risico

Een system dat niet (voldoende) is gehardend loopt het risico om gehackt te worden. Als een systeem kwetsbaar is of als hacker zich toegang kan verschaffen zijn de grootste risico's:

- Installatie van kwaadaardige software
- Ongeautoriseerde toegang tot het hele netwerk
- Toegang tot gevoelige informatie
- Aantasting of verwijdering van data
- Aantasting van (bedrijfs-) kritische applicaties en processen
- Een Denial of Service situatie waarbij het system onbruikbaar is
- Gebruik van het systeem bij cyberaanvallen

Account Policies

Via Account Policies kan een veilig wachtwoordbeleid worden geconfigureerd. Hierbij wordt rekening wordt gehouden met het omgegaan van mislukte inlogpogingen. Het hoofdstuk bestaat uit 2 delen:

- Password Policy
- Account Lockout Policy

Account Policies - Password Policy (wachtwoordbeleid)

De eenvoudigste manier om toegang te krijgen tot een systeem is door in te loggen.
Naast het feit dat een wachtwoord voldoende lang en complex moet zijn en regelmatig gewijzigd moet worden, is het belangrijk dat het wachtwoord veilig en dus versleuteld word opgeslagen.

Hoe langer een gebruiker hetzelfde wachtwoord gebruikt, hoe groter de kans dat een hacker dit kan achterhalen. Een hacker kan wachtwoorden achterhalen door middel van *brute force,* aanvallen waarbij een enorm aantal inlogpogingen gedaan wordt met steeds verschillende (veelgebruikte) login/wachtwoord combinaties. Als het wachtwoord van een individuele gebruiker eenmaal is achterhaald – dit kan ook op een andere server en/of plek zijn – dan blijft dit een zwakke plek totdat het wachtwoord is gewijzigd.
Wachtwoorden die onvoldoende complex zijn – bijvoorbeeld omdat ze alleen uit alfanumerieke karakters bestaan – zijn extreem eenvoudig te ontdekken met publiekelijk beschikbare hack-tools.

Risico

Als de password policy niet goed is ingesteld loop je het risico dat een wachtwoord eenvoudig wordt achterhaald. Als een hacker eenmaal een wachtwoord heeft achterhaald verkrijgt hij/zij hiermee toegang tot een systeem op een manier die niet gekenmerkt wordt als een hack en dus heel lastig is te ontdekken. Hij is dan alleen te ontdekken door gedrag in het systeem en dan is het eigenlijk al te laat. Als gebruiker kan hij overal bij; potentieel gevoelige informatie bekijken en/of verwijderen, toegang verkrijgen tot andere systemen in het netwerk, het systeem manipuleren en zelfs een heel netwerk platleggen.

Account Policies - Account Lock-out Policy

Deze instellingen bepalen na hoeveel verkeerde inlogpogingen een gebruikersaccount op inactief wordt gezet en na welke periode dit account dan weer gebruikt kan worden.
Strengere instellingen verminderen de kans van slagen van een brute force aanval aanzienlijk. Als deze aanval bijvoorbeeld 100.000 wachtwoorden wil proberen en na iedere 3 inlogpogingen 15 minuten moet wachten, duurt het een jaar om alle wachtwoorden te proberen. Om te voorkomen dat een gebruiker zichzelf per ongeluk buitensluit moet deze lock-out periode ook weer niet te lang zijn. Door het verkeer van mogelijke hackers te beperken, voorkomen lock-out instellingen ook een Denial of Service (DoS) conditie waarbij alle accounts continue inactief zijn.

Risico

Als de lock-out periodes niet of niet goed zijn ingesteld loopt het systeem vergroot risico dat een brute force aanval effectief is en de wachtwoorden binnen een korte termijn achterhaald worden. Verder loopt het systeem het risico dat er geen toegang meer verkregen kan worden door een Denial of Service-aanval.

Local Policies

Dit zijn instellingen die lokaal op de server gedaan worden. Dit hoofdstuk bestaat uit 2 delen:

- User Rights Assignment
- Security Options

Local Policies - User Rights Assignment

Deze instellingen bepalen welke rechten nodig zijn om securitygevoelige processen op het systeem uit te voeren. Het gaat hierbij om processen rondom het uitvoeren van applicaties voor bijvoorbeeld backup en restore van gegevens, beheer van toegang voor het domein, beheer van geheugen, aansturen van hardware.
De rechten op deze processen moeten alleen aan die gebruikers of groepen worden toegekend die ze echt nodig hebben en waarvan de beveiliging optimaal is.

Risico

Het risico dat het men loopt als deze rechten niet goed zijn ingesteld is dat een hacker de controle van een systeem overneemt en dit aantast. Alle inloggegevens en gevoelige informatie van andere gebruikers kunnen worden achterhaald, waardoor de identiteit van een andere gebruiker kan worden aangenomen en de hacker toegang krijgt tot diens resources. Daarnaast kan een hacker uitvoerbare bestanden overschrijven en backdoors installeren om continue toegang tot het systeem te waarborgen. Ook kunnen processen dusdanig worden aangepast dat kritische applicaties langzaam worden of crashen.
Een hacker kan allerlei kwaadaardige software installeren en hiermee bijvoorbeeld een Denial of Service-aanval starten. Gevoelige informatie kan worden ingezien of openbaar worden gemaakt via het netwerk. Verder kan data worden verminkt of zelfs helemaal verloren gaan.
Via de toegang tot het systeem en het netwerk kan de hacker de bewijslast verwijderen of dusdanig corrumperen dat het lastig is om te achterhalen wat er gebeurd is na een beveiligingsincident.

Local Policies - Security Options

Deze instellingen hebben voornamelijk betrekking tot de beveiliging van het netwerkverkeer.
Er moet bijvoorbeeld worden ingesteld dat servers onderling versleuteld met elkaar communiceren. Anders kan een ‘kleine’ infectie in het netwerk toegang geven tot het hele netwerk.

Local Policies - Security Options - Accounts

Bij de installatie van een Windows server zijn er 2 standaard gebruikers die worden mee geïnstalleerd: administrator en guest.
De veilige instelling is om beide accounts uit te zetten. Het gaat hier om de lokale administrator, er kan beter via het domein administrator toegang worden verkregen indien dit nodig is. Mocht de lokale administrator toch nodig zijn dan kan via de safe-mode alsnog als lokale administrator worden ingelogd. Ook als beide accounts aanstaan is het hernoemen van de loginnamen verstandig omdat dit het lastiger maakt voor een hacker om een login/wachtwoord combinatie te raden.

Risico

Als deze instellingen niet zijn geconfigureerd loopt men risico dat een hacker zich via een van de standaard accounts toegang verschaft tot het systeem.

Local Policies - Security Options – Audit

Deze instellingen bepalen hoe het systeem met de audit policy omgaat, het gaat niet om wat er geaudit wordt. Zo kunnen de meer precieze audit mogelijkheden worden geactiveerd en kan er worden ingesteld of het systeem automatisch moet worden uitgeschakeld als er niet naar de security log kan worden geschreven.

Risico
Als deze instellingen niet goed zijn, loopt de organisatie het risico dat er onvoldoende gedetailleerde audit informatie beschikbaar is. Verder kan een hacker een server laten vastlopen door een grote hoeveelheid security events (activiteit) te genereren.

Local Policies - Security Options – Devices
Deze instellingen bepalen hoe het systeem met externe hardware omgaat zoals USB-sticks, externe harddisks of printers.

Risico
Als deze instellingen niet goed zijn geconfigureerd dan is er risico dat gebruikers data die zij niet mogen inzien naar een externe opslag kunnen kopiëren waardoor zij alsnog inzicht in de data krijgen.

Local Policies - Security Options - Domain controller
Deze instellingen hebben alleen betrekking op Domain Controllers. Het gaat hierbij om (lokale) instellingen die bepalen onder welke accounts verbinding kan worden gemaakt en of deze verbindingen versleuteld moeten zijn.

Risico
Als deze instellingen niet goed zijn, is het systeem onder andere kwetsbaar voor zogenaamde man-in-the-middle aanvallen waarbij een hacker kan 'meeliften' op een bestaande verbinding. Om deze risico's tegen te gaan is het ook aan te raden om infrastructurele maatregelen te nemen.

Local Policies - Security Options - Domain member
Deze instellingen reflecteren de manier waarop een Member Server zich aanmeldt bij het domein; of de verbinding versleuteld dient te zijn, zowel aan de server- als aan de clientzijde.

Risico
Als deze instellingen niet goed staan, loopt de organisatie het risico dat een hacker via de onderlinge verbindingen tussen de systemen het domein kan binnendringen. Belangrijk is dat niet alleen de informatie die over een verbinding gaat versleuteld is maar dat ook de integriteit van de verbinding zelf gecontroleerd wordt.

Local Policies - Security Options - Interactive logon
Er kan rechtstreeks op het systeem worden ingelogd, bijvoorbeeld via een toetsenbord, om dit veilig te kunnen doen moet ook het wachtwoordbeleid goed zijn ingericht.

Risico
Bij niet veilige instellingen, loopt de organisatie het risico dat een hacker via dit systeem in het domein kan binnendringen. Het verstandigst is daarom deze vorm van toegang tot een minimum te beperken

Local Policies - Security Options - Microsoft network client
Deze instellingen regelen hoe de verbindingen tussen client- en server-systemen worden opgezet en gebruikt. Het gaat hierbij om de instellingen aan de clientzijde.

Risico
Als deze instellingen niet goed zijn, loopt de organisatie het risico dat actieve sessies tussen een client en een server worden misbruikt. Hackers kunnen mogelijk pakketjes met informatie onderscheppen en deze vervolgens aanpassen. Soms worden hierbij ook onversleutelde wachtwoorden onderschept.

Local Policies - Security Options - Network access

Deze instellingen regelen de netwerktoegang via de gedeelde resources en de toegang tot de registry. De registry is een database die veel gevoelige systeemconfiguraties bevat. Toegang tot de registry moet altijd goed zijn afgeschermd.

Risico

Als deze instellingen niet goed zijn, is het systeem extra gevoelig voor het anoniem achterhalen van gebruikersnamen en gedeelde resources waarbij deze informatie gebruikt kan worden voor social hacking (het op sociale manier achterhalen van wachtwoorden) en DoS aanvallen. Als een hacker toegang krijgt tot de registry kan hij tevens toegang krijgen tot het systeem.

Local Policies - Security Options - Network security

Deze instellingen zorgen ervoor dat netwerkverkeer niet ongeautoriseerd of onversleuteld over het netwerk gaat. Vooral bij oudere systemen of applicaties gebaseerd op oudere protocollen kan onversleuteld netwerkverkeer voorkomen, zoals bij Windows systemen gebaseerd op oudere versies. Deze kunnen gebruik maken van verouderede encryptiemethodes of bijvoorbeeld null sessies die helemaal geen authenticatie hebben.

Risico

Het risico bij het niet goed configureren van deze instellingen is dat een hacker via een man-in-the-middle aanval kan 'meeliften' op een bestaande verbinding en zich zo toegang kan verschaffen tot het systeem.

Local Policies - Security Options – Shutdown

Deze instellingen beschermen het systeem tegen een inlogpoging waarbij een hacker zich fysiek toegang heeft verschaft tot een systeem. Ook als hij geen inloggegevens heeft kan hij het systeem uitzetten.

Risico

Het risico van een niet veilige instelling is dat een systeem kan worden uitgezet, wat tot een Denial-of-Service conditie leidt.

Local Policies - Security Options - System object

Deze instellingen zorgen ervoor dat (belangrijke) bestanden hoofdlettergevoelige naamgevingen hebben. Hierdoor kan er niet een malafide applicatie met dezelfde naam als een reguliere applicatie worden aangemaakt waarbij alleen de hoofdletters verschillen.

Risico

Als deze instellingen niet correct zijn, loopt een organisatie verhoogd risico dat er een applicatie geplaatst kan worden die er op het eerste oog correct uitziet maar toch kwaadaardig is.

Local Policies - Security Options - User Account Control

Deze instellingen bepalen met welke rechten een applicatie kan worden geïnstalleerd en uitgevoerd. Ook als een gebruiker als administrator is ingelogd is het verstandig niet direct de hoogste rechten uit te delen. In plaats daarvan zal het systeem iedere keer als deze rechten nodig zijn om bevestiging vragen aan de ingelogde gebruiker.

Risico

Als deze instellingen niet goed zijn geconfigureerd, kunnen rechten aan applicaties worden toegekend die niet wenselijk zijn. Als een applicatie de hoogste rechten heeft, kan deze in feite het hele systeem overnemen. Ook verhindert een veilige instelling dat kwaadaardige applicaties zichzelf kunnen installeren met de hoogste rechten en dat eenmaal geïnstalleerde applicaties zichzelf de hoogste rechten toewijzen.

Windows Firewall With Advanced Security

Als de firewall van de server niet goed is ingesteld, zijn de poorten aan de buitenkant van de server niet goed beschermd. Hierdoor kunnen deze worden misbruikt om toegang te krijgen. Dit is vooral gevaarlijk als er applicaties draaien niet regelmatig geüpdatet kunnen worden, bijvoorbeeld omdat ze noodzakelijk zijn voor productie.
Met de firewall kun je toegang verschaffen via het private domein of publieke segment. Hierbij dient feitelijk geen toegang te worden verschaft via het publieke segment en heel beperkt via het domein segment.

Windows Firewall With Advanced Security - Domain Profile

Deze instellingen configureren de 'interne' firewall van het systeem. De instellingen in dit hoofdstuk hebben betrekking op netwerkverkeer binnen het domein.
De firewall is feitelijk de eerste verdedigingslijn van het systeem. Hierbij moet met zowel in- als uitkomend verkeer rekening worden gehouden. Inkomend verkeer moet alleen worden binnengelaten als daar toestemming voor is. Voor uitgaand verkeer geldt eigenlijk het tegenovergestelde. Het controleren heeft geen zin want een geïnfecteerd systeem kan altijd naar buiten maar kan wel het log systeem plat leggen. De logbestanden zijn de belangrijkste plek waar ontdekt kan worden hoe een hacker probeert binnen te komen en moeten daarom zo worden ingesteld zodat deze informatie altijd bewaard blijft.

Risico

Het risico dat een organisatie loopt als deze instellingen niet goed zijn geconfigureerd, is dat al het netwerkverkeer ongehinderd het systeem binnen kan komen waardoor het voor een hacker eenvoudiger wordt om kwetsbaarheden uit te buiten.

Windows Firewall With Advanced Security - Private Profile

Deze instellingen configureren de 'interne' firewall van het systeem. De instellingen in dit hoofdstuk hebben betrekking op het privé netwerkverkeer.
De firewall is feitelijk de eerste verdedigingslijn van het systeem. Hierbij moet met zowel in- als uitkomend verkeer rekening worden gehouden. Inkomend verkeer moet alleen worden binnengelaten als ze daar toestemming voor hebben. Voor uitgaand verkeer geldt eigenlijk het tegenovergestelde. Het controleren heeft geen zin want een geïnfecteerd systeem kan altijd naar buiten maar kan wel het log systeem plat leggen. De logbestanden zijn de belangrijkste plek waar ontdekt kan worden hoe een hacker probeert binnen te komen en moeten daarom veilig worden ingesteld zodat deze informatie altijd bewaard blijft.

Risico

Het risico dat een organisatie loopt als deze instellingen niet goed zijn geconfigureerd is dat al het netwerkverkeer ongehinderd het systeem binnen kan komen waardoor het voor een hacker eenvoudiger wordt om kwetsbaarheden uit te buiten.

Windows Firewall With Advanced Security - Public Profile

Deze instellingen configureren de 'interne' firewall van het systeem. De instellingen in dit hoofdstuk hebben betrekking op het openbare netwerkverkeer. Dit is het meest gevaarlijke netwerkverkeer en moet daarom, naast infrastructurele maatregelen, goed zijn afgeschermd.
De firewall is feitelijk de eerste verdedigingslijn van het systeem. Hierbij moet met zowel in- als uitkomend verkeer rekening worden gehouden. Inkomend verkeer moet alleen worden binnengelaten als ze daar toestemming voor hebben. Voor uitgaand verkeer geldt eigenlijk het tegenovergestelde. Het controleren heeft geen zin want een geïnfecteerd systeem kan altijd naar buiten maar kan wel het log systeem plat leggen. De logbestanden zijn de belangrijkste plek waar ontdekt kan worden hoe een hacker probeert binnen te komen en moeten daarom veilig worden ingesteld zodat deze informatie altijd bewaard blijft.

Risico

Het risico dat een organisatie loopt als deze instellingen niet goed zijn ingesteld is dat al het netwerkverkeer ongehinderd het systeem binnen kan komen waardoor het voor een hacker eenvoudiger wordt om kwetsbaarheden uit te buiten.

Advanced Audit Policy Configuration

Deze instellingen bepalen welke gebeurtenissen worden gelogd. Dit is een belangrijke veiligheidsinstelling omdat deze aangeeft wanneer er een hackpoging in uitvoering is en hierover informatie opslaat.
Bij een geslaagde hackpoging is dit ook de belangrijkste body-of-evidence en helpt met het achterhalen van wat er is gebeurd en welke maatregelen er genomen moeten worden om incidenten in de toekomst te voorkomen.
De volgende gebeurtenissen worden hierbij geaudit:

- Succesvolle en niet succesvolle inlogpogingen en afmeldingen
- Het aanmaken en wijzigen van gebruikers
- Het opstarten en afsluiten van systeemprocessen zoals applicaties.
- Het aansluiten en verwijderen van externe systemen zoals harddisks
- Wijzigingen in system beleid (zoals wachtwoordbeleid)
- Gebruik van de hoogste rechten door applicaties
- Wijzigingen van het system zoals aan- of uitzetten van de firewall

Risico

Het risico dat een organisatie loopt als deze auditinstellingen niet goed zijn geconfigureerd is dat er na een beveiligingsincident niet kan worden achterhaald wat er exact is gebeurd. Hierdoor kan de oorzaak niet worden verholpen en is er een vergroot risico dat eenzelfde incident zich nogmaals voordoet

Administrative Templates (Computer)

Deze templates bevatten beveiligingsinstellingen voor het systeem die via de Group Policy gedaan worden. De instellingen op systeemniveau worden doorgevoerd in de Registry.
Als deze instellingen niet goed zijn, is de Group Policy voor het hele domein waarschijnlijk niet correct, en hebben alle servers binnen dit domein onveilige instellingen.

Administrative Templates (Computer) - Control Panel

Deze instellingen configureren de lock screen voor het systeem. Een systeem dat is afgesloten moet niet meer toegankelijk zijn voor gebruikers totdat ze inloggen.

Risico

Als deze instellingen niet goed zijn geconfigureerd, creëert dit een risico omdat het systeem nog steeds beschikbaar en kwetsbaar is, ondanks dat het is afgesloten met een lock screen. Zo kan bijvoorbeeld de camera nog misbruikt worden terwijl niemand is ingelogd.

Administrative Templates (Computer) – LAPS

Deze instelling configureren het lokale administrator wachtwoord. Vaak wordt hetzelfde lokale administratie wachtwoord gebruikt als een nieuw systeem wordt geïnstalleerd. Deze instelling voorkomt dat er een makkelijk wachtwoord wordt gekozen bij het installeren van een nieuw systeem.

Risico

Het risico dat wordt gelopen als deze instelling niet goed staat geconfigureerd is dat het lokale administrator wachtwoord makkelijk verkregen wordt, waardoor het systeem en daarmee het hele netwerk wordt aangetast.

Administrative Templates (Computer) - MSS (Legacy)

Dit zijn instellingen waarmee het netwerkprotocol kan worden ingesteld. Het gaat hierbij onder andere om IP-instellingen en het routen van IP-verkeer.

Risico

Als deze instellingen niet goed zijn geconfigureerd kan een hacker zich ongezien verbergen in het netwerk en Denial of Service aanvallen uitvoeren. Verder kan hij systemen identificeren en het netwerk in kaart brengen.

Administrative Templates (Computer) – Network

Deze instellingen bepalen de manier waarop systemen via het netwerk kunnen worden gevonden en geconfigureerd.

Risico

Als deze instellingen niet correct zijn geconfigureerd loopt de organisatie het risico dat een hacker het hele netwerk in kaart brengt, op andere systemen kan komen en zelfs systemen configureert.

Administrative Templates (Computer) - SCM: Pass the Hash Mitigations

Deze instellingen zorgen ervoor dat lokale wachtwoorden op een systeem niet worden hergebruikt bij nieuwe installaties en dat de lokale wachtwoorden niet onversleuteld in het geheugen worden opgeslagen.

Risico

Het risico dat een systeem loopt als deze instellingen niet goed zijn geconfigureerd is dat hackers de gegevens kunnen achterhalen van gebruikers op nieuwe systemen. Met deze gegevens kunnen hackers dan ook inloggen op andere systemen waardoor het aantal servers wat een hacker kan aanvallen substantieel groter wordt.

Administrative Templates (Computer) – System

Deze instellingen bepalen hoe een systeem opstart en de toegang tot de Command line. Dit is belangrijk indien een systeem eenmaal geïnfecteerd is en moet worden schoongemaakt.
Ook de manier en snelheid waarop de Group Policy wordt toegepast wordt hier ingesteld. De Group Policy bevat belangrijke veiligheidsinstellingen en moet zo snel mogelijk op het systeem worden toegepast.
Verder wordt de manier waarop een systeem communiceert met externe support hier ingesteld. Iedere vorm van communicatie die niet noodzakelijk is moet worden vermeden.

Risico

Het risico dat een organisatie loopt als deze instellingen niet correct zijn geconfigureerd is dat de impact van een geïnfecteerd systeem niet gereduceerd kan worden na het herstarten van het systeem. Hierbij is de command line een belangrijke tool, Eventueel gevoelige informatie die via de Command line getoond wordt moet worden afgeschermd.
Zolang de Group Policy nog niet (volledig) is toegepast, is het systeem gevoelig voor de kwetsbaarheden die door de Group Policy worden afgedekt. Dit een hacker de mogelijkheid om het systeem aan te tasten.

Administrative Templates (Computer) - Windows Components

Deze instellingen configureren Windows applicaties die meegeleverd worden bij een nieuwe Windows installatie. Deze applicaties hebben een directe verbinding met het systeem. Het gaat hierbij onder andere om applicaties die op afstand verbinding maken en updates installeren, maar ook anti-malware en externe opslag.

Risico

Het risico dat een organisatie loopt als deze instellingen niet goed zijn geconfigureerd is dat hackers via deze applicaties toegang krijgen tot het systeem. Dit zijn basisapplicaties die vaak de hoogste rechten hebben en daardoor ook zeer gevoelig voor kwetsbaarheden. Rechten tot deze applicaties moeten worden beperkt en applicaties die niet gebruikt worden dienen helemaal uitgezet of verwijderd te worden.

Administrative Templates (User)

Deze templates omvatten beveiligingsinstellingen voor de users op het systeem die via de Group Policy geconfigureerd worden. De instellingen op systeemniveau worden doorgevoerd in de Registry.
Als deze instellingen niet juist zijn geconfigureerd, is de Group Policy voor het hele domein waarschijnlijk niet correct. Hierdoor kunnen alle gebruikers op de servers binnen dit domein onveilige instellingen hebben.

Administrative Templates (User) - Control Panel

Deze instellingen configureren hoe er moet worden omgegaan met onbeheerde systemen.

Risico

Het risico dat een organisatie loopt als deze instellingen niet goed zijn geconfigureerd, is dat een onbeheerd systeem kan worden gebruikt om een ander systeem over te nemen.

Administrative Templates (User) - Start Menu and Taskbar

Deze instellingen omvatten hoe er moet worden omgegaan met notificaties op afgesloten systemen.

Risico

Het risico dat wordt gelopen is dat een hacker, hoewel het systeem is afgesloten, nog steeds gevoelige informatie kan zien.

Administrative Templates (User) – System

Deze instelling configureert hoe de Microsoft Experience service staat ingesteld. Deze service verzamelt informatie van gebruikers van Microsoft om hun systemen te verbeteren.

Risico

Het risico dat wordt gelopen als deze configuratie niet goed staat ingesteld is dat een derde partij informatie kan verzamelen. Dit geeft een mogelijk onwenselijk beeld van gebruikers en het gebruik van systemen.

Administrative Templates (User) - Windows Components

Deze instellingen configureren Windows applicaties die meegeleverd worden bij een nieuwe Windows installatie. Deze applicaties hebben een directe verbinding met het systeem. Het gaat hierbij onder andere om de applicaties om updates te installeren, resources te delen en media af te spelen.

Risico

Het risico dat een organisatie loopt als deze instellingen niet goed zijn geconfigureerd is dat hackers via deze applicaties toegang krijgen tot het systeem. Dit zijn basis applicaties die vaak de hoogste rechten hebben en daardoor ook zeer gevoelig voor kwetsbaarheden. Rechten tot deze applicaties moeten worden beperkt en applicaties die niet gebruikt worden dienen helemaal uitgezet of verwijderd te worden.