Haagse Hogeschool
Lectoraat CyberSecurity in het MKB
Analyse- advies rapport

Website: HHS

Opdrachtgever: Komp u ter hulp
Opdrachtnemer: Haagse Hogeschool
15 juli 2021
Versie 1.0

Studenten/adviseurs
Halit Cankara
Randy Vos

Een DDoS attack: wat is het en wat zijn de gevolgen?
Voordelen gebruik van best practice

1.1 Aanbeveling 1: IT Asset Management

IT Asset Management systeem is een belangrijk onderdeel van algemene systemen, die nodig zijn om de IT-infrastructuur te beheren. Zonder goed IT Asset Management zal de organisatie tijd en middelen verspillen aan het beheren van inventaris, het kopen van onnodige apparatuur en software, en het handhaven van licentie compliance voor software. Met een goed functionerend IT Asset Management systeem kan de organisatie verwachten de totale kosten van eigendom voor IT-infrastructuur verlagen en een solide basis te bieden om uw IT-infrastructuur efficiënt te laten werken. Het beheer van IT-middelen gaat over meer dan alleen het kiezen van de beste software en apparaten.
Wanneer je ITAM doelgericht inzet, profiteer je van voordelen zoals:

- Verbeterde communicatie tussen bedrijfsonderdelen (zoals verkoop, marketing, administratie, winkelpersoneel);
- Verbeterde software naleving;
- Kostenbesparing in IT-middelen
- Verbeterde gegevensbeveiliging;
- Verbeterde dienstverlening door verbeterde beschikbaarheid van gegevens;
- Beter gebruik van budgetten en eenvoudig besluiten door beter begrip van IT-middelen en hun functie in de organisatie

1.2 Aanbeveling 2: ITIL-certificering

ITIL (Information Technology Infrastructure Library) is een raamwerk dat is ontworpen om de IT-beheerprocessen beter beheren. Het biedt concrete handvatten om een IT-organisatie in te richten en te beheren.

ITIL-certificering is een absolute must om de hoge kosten die IT-investeringen met zich meebrengen te verlagen en om een stevige basis te leggen voor de totale kosten van eigendom.
Daarnaast is het behalen van een ITIL-certificering een mooie aanvulling op het curriculum en toont de student aan dat hij in staat is om IT-beheerprocessen te beheren en in te richten.

Sinds kort is de nieuwste versie van het ITIL framework uitgebracht: ITIL 4. Dit omvat 34 richtlijnen, omschreven als middelen en activiteiten om werk uit te voeren of een doelstelling te bereiken. Deze praktijken zijn onderverdeeld in drie categorieën:

- Algemene managementpraktijken, waaronder projecten en portefeuilles, bedrijfsrisico's, beveiliging van informatie, voortdurende verbetering.
- Management op het gebied van dienstenbeheer, zoals bedrijfsanalyse, dienstenontwerp en -continuïteit, servicedesk, monitoring en incidentenbeheer, veranderingsprocessen, en beheer van IT-middelen
- Management op het gebied van technisch beheer, waaronder softwareontwikkeling, implementatie, infrastructuur en platform.

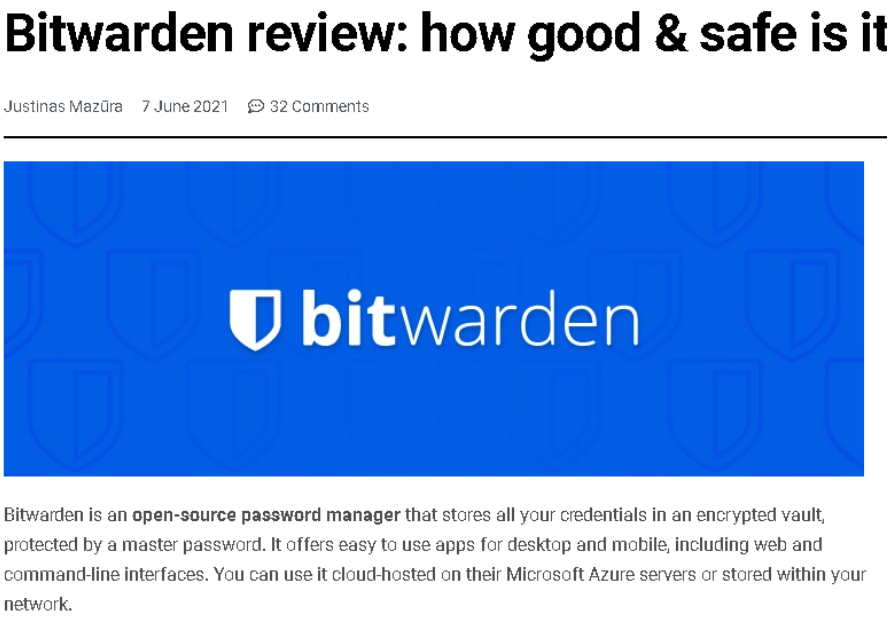
Wat is IT Asset Management?
ITIL uitgelegd (in Jip en Janneke taal)

1.3 Aanbeveling 3: Gebruik malware detectie

Malwaredetectie is van cruciaal belang nu malware op het internet zo in opmars is, mede omdat het functioneert als een vroegtijdig waarschuwingssysteem voor de computerbeveiliging met betrekking tot malware en cyberaanvallen. Het houdt hackers buiten de deur en voorkomt dat informatie wordt onderschept. Antimalware zoals de gratis software Malwarebytes zet een antihacking vergrendeling, of voert regelmatig scans uit om de aanwezigheid van een hacker of malware in het computernetwerk te detecteren. Deze software kan gebruikt worden voor de systemen waarop virtuele machines draaien, en ook op de laptops van de studenten.
Bij computers met NAW-gegevens dient realtime bescherming toegepast te worden
Dit valt onder een betaalde versie van Malwarebytes, maar daarmee voorkom je onder andere dat kwaadwilligen doormiddel van een RAT, stiekem meekijken in de computer.

1.4 Aanbeveling 4: Gebruik een wachtwoord manager.

Binnen de organisatie wordt gebruik gemaakt van sterke wachtwoorden, cijfers, speciale tekens en hoofdletters.
Zoals 096#Zaandam
Het gebruik van zwakke wachtwoorden kan ertoe leiden dat cybercriminelen toegang krijgen tot het bedrijfsnetwerk en persoonlijke data.
Dit kan ervoor zorgen dat er virussen en malware geïnstalleerd worden en een datalek plaatsvindt. Om dit te voorkomen is een wachtwoordmanager aan te raden.
Met een wachtwoordmanager kunnen wachtwoorden veilig en centraal beheerd worden. Tevens genereert de wachtwoordmanager zelf sterke wachtwoorden zodat dit niet zelf bedacht en onthouden moet worden. Daarnaast bieden sommige wachtwoordmanagers ook nog eens de mogelijkheid om andere gegevens zoals notities, adresgegevens en softwarelicenties veilig te bewaren. De wachtwoordmanager die wordt aangeraden is Bitwarden. Dit is een uitstekende wachtwoordmanager en is ook nog eens gratis. Een meerwaarde van Bitwarden is dat het opensource is en dus niets kan verbergen behalve natuurlijk de zorgvuldig versleutelde wachtwoorden.



Bitwarden · GitHub

1.5 Aanbeveling 5: ISO 27001 certificering.

Bedrijven wordt aangeraden zich te certificeren volgens de ISO 27001 standaard. Dit is een wereldwijd erkende norm op het gebied van informatiebeveiliging. Met deze certificering wordt aangetoond dat het bedrijf voldoet aan alle eisen rondom informatiebeveiliging. Tevens is het zo dat er met de ingang van de Algemene Verordening Persoonsgegevens (AVG) de regels in Europa rondom gegevensbescherming flink zijn aangescherpt. Als organisatie betekent dit dat het managementsysteem voor informatiebeveiliging goed op orde dient te zijn.

ISO 27001 helpt u bij het opstellen van een managementsysteem voor informatiebeveiliging. Het opstellen van zo'n systeem en het behalen van het ISO 27001 certificaat levert de organisatie verscheidene voordelen op:

- Met ISO 27001 laat het bedrijf zien dat het voldoet aan de strenge normeisen rondom informatiebeveiliging. Steeds meer klanten eisen dat partners waarmee zij samenwerken hun informatiebeveiliging goed op orde hebben. Met ISO 27001 certificering wordt aangetoond dat het bedrijf voldoet aan alle eisen rondom informatiebeveiliging. Zo kan het certificaat commerciële kansen voor de organisatie creëren.
- Het ISO 27001 certificaat helpt informatiebeveiligingsrisico's te verkleinen en incidenten te voorkomen. Hierdoor de reputatie van de organisatie beschermt.
- Met het ISO 27001 certificaat op zak kan ervan worden uitgegaan dat er voldoende is gedaan om te voldoen aan wet- en regelgeving rondom informatiebeveiliging.

1.6 Aanbeveling 6 Best practice voor PXE en Pre-boot OS beveiliging

Beveiligingsproblemen beginnen bij toegang tot het netwerk. De volgende aanbevelingen dienen worden opgevolgd om risico's tot een minimum te beperken bij verdere potentiële inbreuken op het netwerk via de PXE-server.

Tijdens het maken van de automatiseringsomgeving wordt een gebruikersnaam en wachtwoord gebruikt om toegang te verlenen tot gedeelde netwerkmappen en -locaties, inclusief toegang tot het deelpunt en de netwerklocatie van opgeslagen imagebestanden. Het is sterk aanbevolen dat dit nooit een domeinaccount is. Maak één lokale gebruikersaccount aan op elke gedeelde netwerklocatie en geef deze gebruikersaccount minimale gebruikersrechten (meestal alleen lees-/schrijfrechten) en uitsluitend toegang tot specifieke mappen binnen de deellocatie (meestal de PXE folder genaamd "images" en eventuele vereiste mappen).

Opmerking: Bijzondere aandacht dient te worden besteed aan beveiliging van locatie en bescherming van opgeslagen bestanden om te voorkomen dat onbevoegden met de PXE-boot bestanden knoeien.

- Beperk de beschikbaarheid van PXE-diensten door MAC-adresfiltering te gebruiken via het PXE-configuratiehulpprogramma.
- Beperk de beschikbaarheid van poorten voor netwerkcommunicatie tot UDP-poorten 67, 68, 69 en 4011, die worden gebruikt in het opstartproces van de PXE-server.

1.7 Aanbeveling 7: Beveiligingsinrichting Azure volgens best-practice

De cursisten horen een Azure virtuele machine volgens beveiligingsrichtlijnen in te richten. Daarvoor zijn standaardinstellingen die zich baseren op de best-practice uit het Microsoft handboek. Azure Virtual Desktop heeft veel ingebouwde beveiligingsmaatregelen. In deze sectie vindt je informatie over beveiligingscontroles die je kan gebruiken om de gebruikers en gegevens veilig te houden.

1) Multi-Factor Authentication

De verificatie voor gebruikers en beheerders in Azure Virtual Desktop verbetert de beveiliging van de hele implementatie. Zie Azure AD Multi-Factor Authentication inschakelen voor Azure Virtual Desktop voor meer informatie.

2) Voorwaardelijke toegang inschakelen

Als voorwaardelijke toegang wordt ingeschakeld, kunnen risico's beheerd worden alvorens de gebruikers toegang wordt verleent tot de Azure Virtual Desktop-omgeving. Bij het bepalen aan welke gebruikers toegang wordt verleent, is het aan te raden we te overwegen wie de gebruiker is, hoe ze zich aanmelden en welk apparaat ze gebruiken.

3) Auditlogboeken verzamelen

Als het verzamelen van auditlogboek wordt ingeschakeld, zijn de gebruikers- en beheerdersactiviteiten te bekijken. Enkele voorbeelden van belangrijke auditlogboeken zijn:

- Azure-activiteitenlogboek
- Azure Active Directory activiteitenlogboek
- Azure Active Directory
- Sessiehosts
- Diagnostisch logboek van Azure Virtual Desktop
- Key Vault logboeken

4) RemoteApps gebruiken

Bij het kiezen van een implementatiemodel, wordt externe gebruikers toegang verleend tot volledige virtuele desktops of specifieke applicaties. Remote applicaties, of RemoteApps, bieden een soepele ervaring bij interactie van gebruikers met applicaties op hun virtuele desktop. RemoteApps beperken het risico omdat de gebruiker alleen werkt met een subset van de externe computer die beschikbaar wordt gemaakt door de applicatie.

5) Gebruik bewaken met Azure Monitor

Controleer het gebruik en de beschikbaarheid van uw Azure Virtual Desktop-service met Azure Monitor. Overweeg service health-waarschuwingen te maken voor de Azure Virtual Desktop-service om meldingen te ontvangen wanneer er een gebeurtenis is die van invloed is op de service.

Aanbevolen procedures voor beveiliging

6) Schakel Azure Security Center

Het wordt aangeraden Azure Security Center Standard in te stellen voor abonnementen, virtuele machines, sleutelkluizen en opslagaccounts.

Azure Security Center Standard kan het volgende gedaan worden:

- Beveiligingsproblemen beheren.
- Evalueer de naleving van algemene frameworks zoals PCI.
- De algehele beveiliging van uw omgeving verbeteren.

Zie your Azure subscription to Security Center Standard (Uw Azure-abonnement onboarden naar Security Center Standard) voor meer informatie.

7) De veiligheidsscore verbeteren

Beveiligingsscore biedt aanbevelingen en best practice om de algehele beveiliging te verbeteren. Deze aanbevelingen krijgen prioriteit om te helpen kiezen welke het belangrijkst zijn, en de snelle oplossingen helpen om potentiële beveiligingsproblemen snel op te lossen. Deze aanbevelingen worden ook na een bepaalde periode bijgewerkt, zodat men op de hoogte blijft van de beste manieren om de beveiliging van die omgeving te onderhouden. Zie Improve your Secure Score in Azure Security Center (De beveiligde score verbeteren in Azure Security Center) voor meer Azure Security Center.

8) Gebruik bewaken met Azure Monitor

Controleer het gebruik en de beschikbaarheid van de Azure Virtual Desktop-service met Azure Monitor. Overweeg service health-waarschuwingen te maken voor de Azure Virtual Desktop-service om meldingen te ontvangen wanneer er een gebeurtenis is die van invloed is op de service.

1.8 Aanbeveling 8: Best practices voor Azure beveiliging van sessiehosts

Sessiehosts zijn virtuele machines die worden uitgevoerd binnen een Azure-abonnement en virtueel netwerk. De algehele beveiliging van de Azure Virtual Desktop-implementatie is afhankelijk van de beveiligingscontroles die u op de sessiehosts zijn geïmplementeerd. In deze sectie worden de best practices beschreven voor het beveiligen van sessiehosts.

1) Endpoint Protection inschakelen

Om de implementatie te beschermen tegen bekende schadelijke software, wordt aangeraden endpoint protection in te stellen op alle sessiehosts. Er kan een Windows Defender Antivirus programma van derden gebruikt wordenn. Zie Implementatiehandleiding voor Windows Defender Antivirus in een VDI-omgeving voor meer informatie.

Voor profieloplossingen zoals FSLogix of andere oplossingen waarmee VHD-bestanden worden bevestigd, wordt aangeraden de VHD-bestandsextensies uit te sluiten.

2) Een eindpuntdetectie- en -responsproduct installeren

Het wordt aangeraden een EDR-product (eindpuntdetectie en -respons) te installeren om geavanceerde detectie- en responsmogelijkheden te bieden. Voor serverbesturingssystemen Azure Security Center ingeschakeld, wordt Defender ATP geïmplementeerd door een EDR-product te installeren. Voor clientbesturingssystemen kunt u Defender ATP of een product van derden implementeren op deze eindpunten.

3)Bedreigings- en vulnerability management inschakelen

Het identificeren van beveiligingsproblemen van software die voorkomen in besturingssystemen en toepassingen is essentieel om de omgeving veilig te houden. Azure Security Center kan problemen identificeren door middel van evaluaties van beveiligingsleeds voor serverbesturingssystemen. Ook door Defender ATP gebruiken. Dit biedt bedreigingen en vulnerability management voor desktopbesturingssystemen. Er kunnen ook producten van derden gebruikt worden, maar het is aan te bevelen om Azure Security Center Defender ATP te gebruiken.
Wat is ATP?

English
https://www.techzine.eu/news/security/47703/microsoft-defender-atp-gets-built-in-firmware-protection/

4)Beveiligingsproblemen met software in de omgeving patchen

Zodra een beveiligingsprobleem is gevonden, moet je dat gaan patchen. Dit geldt ook voor virtuele omgevingen, waaronder de besturingssystemen die worden uitgevoerd, de toepassingen die erin zijn geïmplementeerd en de afbeeldingen van waaruit nieuwe machines worden gemaakt. Volg de meldingen van de leverancier en pas patches tijdig toe. We raden aan om de basisafbeeldingen maandelijks te patchen om ervoor te zorgen dat nieuw geïmplementeerde machines zo veilig mogelijk zijn.

Best practices voor beveiliging van sessiehosts

6) Maximumaantal inactieve tijd en beleid voor verbreken van verbinding vaststellen

Door gebruikers af te melden wanneer ze inactief zijn, blijven resources behouden en wordt de toegang door onbevoegde gebruikers voorkomen. We raden aan dat time-outs een goede balans bieden tussen de productiviteit van gebruikers en het resourcegebruik. Voor gebruikers die met staatloze toepassingen werken, kan je een agressiever beleid overwegen om machines uit te schakelen en resources te behouden. Het verbreken van de verbinding van langlopende toepassingen die nog steeds worden uitgevoerd als een gebruiker niet actief is, zoals een simulatie of CAD-rendering, kan het werk van de gebruiker onderbreken en kan zelfs het opnieuw opstarten van de computer vereisen.

7) Schermvergrendelingen instellen voor niet-actieve sessies

Je kan ongewenste systeemtoegang voorkomen door Azure Virtual Desktop te configureren om het scherm van een machine te vergrendelen tijdens niet-actieve tijd en verificatie te vereisen om deze te ontgrendelen.

8) Gelaagde beheerderstoegang tot stand

Het wordt aangeraden de gebruikers geen beheerderstoegang te verlenen tot virtuele bureaubladen. Als je softwarepakketten nodig hebt, kan je deze beschikbaar te maken via hulpprogramma's voor configuratiebeheer, zoals Microsoft Endpoint Manager. In een omgeving met meerdere sessies wordt aangeraden gebruikers geen software rechtstreeks te laten installeren.

9) Bedenk welke gebruikers toegang moeten hebben tot welke resources

Overweeg sessiehosts als een uitbreiding van de bestaande desktopimplementatie. Er wordt aangeraden de toegang tot netwerkbronnen op dezelfde manier te beheren als voor andere bureaubladen in die omgeving, zoals het gebruik van netwerksegmentatie en filteren. Sessiehosts kunnen standaard verbinding maken met elke resource op internet. Er zijn verschillende manieren waarop je het verkeer kan beperken, Azure Firewall, virtuele netwerkapparaten of -perxies. Als je het verkeer wilt beperken, moet je ervoor zorgen dat de juiste regels worden toegevoegd zodat Azure Virtual Desktop goed werkt.

10) Office Pro Plus-beveiliging beheren

Naast het beveiligen van diesessiehosts is het belangrijk dat je ook de toepassingen beveiligt die erin worden uitgevoerd. Office Pro Plus is een van de meest voorkomende toepassingen die worden geïmplementeerd in sessiehosts. Om de beveiliging van de Office-implementatie te verbeteren, is het raadzaam om security policy advisor voor Microsoft 365 apps voor bedrijven te gebruiken. Dit hulpprogramma identificeert beleidsregels die je kan toepassen op de implementatie voor meer beveiliging. Security Policy Advisor raadt ook beleidsregels aan op basis van hun invloed op uw beveiliging en productiviteit.

11) Andere beveiligingstips voor sessiehosts

Door de mogelijkheden van het besturingssysteem te beperken, kan je de beveiliging van die sessiehosts verbeteren. Hier zijn enkele dingen die je kan doen:

- Beheer apparaatomleiding door stations, printers en USB-apparaten om te leiden naar het lokale apparaat van een gebruiker in een extern bureaublad-sessie. er wordt aangeraden de beveiligingsvereisten te evalueren en te controleren of deze functies al dan niet moeten worden uitgeschakeld.
- Beperk Windows Verkenner toegang door toewijzingen van lokale en externe station te verbergen. Dit voorkomt dat gebruikers ongewenste informatie over systeemconfiguratie en gebruikers detecteren.
- Vermijd directe RDP-toegang tot sessiehosts in die omgeving. Als je directe RDP-toegang nodig hebt voor beheer of probleemoplossing, moet je Just-In-Time-toegang inschakelen om de potentiële aanvalsmogelijkheden op een sessiehost te beperken.
- Verleen gebruikers beperkte machtigingen wanneer ze toegang hebben tot lokale en externe bestandssystemen. Je kan machtigingen beperken door ervoor te zorgen dat de lokale en externe bestandssystemen toegangsbeheerlijsten met de minste bevoegdheden gebruiken. Op deze manier hebben gebruikers alleen toegang tot wat ze nodig hebben en kunnen ze kritieke resources niet wijzigen of verwijderen.
- Voorkomen dat ongewenste software wordt uitgevoerd op sessiehosts. Je kan App Locker inschakelen voor extra beveiliging op sessiehosts, zodat alleen de apps die je toestaat op de host kunnen worden uitgevoerd.

11) Ondersteuning voor Azure Virtual Desktop voor vertrouwd starten

Vertrouwde introductie zijn Virtuele Gen2-VM's van Azure met verbeterde beveiligingsfuncties die zijn gericht op bescherming tegen bedreigingen op 'de onderkant van de stack' via aanvalsvectoren zoals rootkits, boot kits en malware op kernelniveau. Hier volgen de verbeterde beveiligingsfuncties van de vertrouwde start, die allemaal worden ondersteund in Azure Virtual Desktop. Ga naar Vertrouwde start voor virtuele Azure-machines (preview)voor meer informatie over een vertrouwde start.

12) Secure Boot

Beveiligd opstarten is een modus die door platformfirmware wordt ondersteund en die je firmware beschermt tegen rootkits en opstartkits op basis van malware. Met deze modus kunnen alleen ondertekende BESe's en stuurprogramma's de machine starten.

13) Opstartintegriteit bewaken met Remote Attestation

Externe attestation is een uitstekende manier om de status van de VM's te controleren. Externe attestation controleert of Measured Boot records aanwezig en legitiem zijn en afkomstig zijn van de virtuele Trusted Platform Module (vTPM). Als statuscontrole biedt het cryptografische zekerheid dat een platform goed is opgestart.

14) vTPM

Een vTPM is een gevirtualiseerde versie van een hardware Trusted Platform Module (TPM), met een virtueel exemplaar van een TPM per VM. vTPM maakt externe attestation mogelijk door integriteitsmeting uit te voeren van de volledige opstartketen van de VM (UEFI, besturingssysteem, systeem en stuurprogramma's).

Het wordt aangeraden vTPM in te stellen voor het gebruik van externe attestation op de VM's. Als vTPM is ingeschakeld, kan je ook BitLocker-functionaliteit inschakelen, die versleuteling op volledige volumes biedt om data-at-rest te beveiligen. Alle functies die vTPM gebruiken, resulteren in geheimen die zijn gebonden aan de specifieke VM. Wanneer gebruikers verbinding maken met de Azure Virtual Desktop-service in een poolscenario, kunnen gebruikers worden omgeleid naar elke virtuele machine in de hostgroep. Afhankelijk van hoe de functie is ontworpen, kan dit van invloed zijn.

15) Notitie

BitLocker mag niet worden gebruikt voor het versleutelen van de specifieke schijf waarop je de FSLogix-profielgegevens opslaat.

16) Beveiliging op basis van virtualisatie

Beveiliging op basis van virtualisatie (VBS) maakt gebruik van de hypervisor om een beveiligde geheugenregio te maken en te isoleren die niet toegankelijk is voor het besturingssysteem. Hypervisor-Protected code-integriteit (HVCI) en Windows Defender Credential Guard gebruiken beide VBS om betere beveiliging tegen beveiligingsproblemen te bieden.

17) Hypervisor-Protected code-integriteit

HVCI is een krachtige systeembeperking die gebruikmaakt van VBS om processen in de Windows-kernelmodus te beschermen tegen injectie en uitvoering van schadelijke of niet-geverifieerde code.

18) Windows Defender Credential Guard

Windows Defender Credential Guard maakt gebruik van VBS om geheimen te isoleren en te beveiligen, zodat alleen bevoegde systeemsoftware er toegang toe heeft. Dit voorkomt onbevoegde toegang tot deze geheimen en diefstal van referenties, zoals Pass-the-Hash-aanvallen.

19) Vertrouwde start implementeren in uw Azure Virtual Desktop-omgeving

Azure Virtual Desktop biedt momenteel geen ondersteuning voor het automatisch configureren van Vertrouwd starten tijdens het installatieproces van de hostgroep. Als je vertrouwd starten in uw Azure Virtual Desktop-omgeving wil gebruiken, moet je Vertrouwd starten normaal implementeren en vervolgens handmatig de virtuele machine toevoegen aan de gewenste hostgroep.