Informatiebeveiliging bij remote beheer

14 december 2018

Lars Hoogendijk

In een eerdere editie van de IT-Auditor heb ik geschreven over informatiebeveiliging bij telewerken, oftewel werken op afstand. [HOOG11a] Een bijzondere vorm van werken op afstand is remote (IT-)beheer, dat inherente risico's kent vanwege de aard van het beheerwerk. In dit artikel beschrijf ik deze risico's en een aantal specifieke beveiligingsprincipes als handreiking die de IT-auditor kan helpen bij het agenderen en uitvoeren van IT-audits op de beveiliging van remote beheer.

Men spreekt van remote beheer als een organisatie delen van haar automatisering op afstand beheert of laat beheren. Van het eerste is bijvoorbeeld sprake wanneer een organisatie haar IT-infrastructuur huisvest in een extern rekencentrum en zelf beheer vanaf haar kantoorpand uitvoert. In het tweede geval bevindt de IT-infrastructuur zich bijvoorbeeld in het pand van de organisatie, maar is het beheer ervan uitbesteed aan een externe partij. Er zijn meer varianten denkbaar. In de paragraaf 'Wat is remote beheer?' behandel ik het begrip remote beheer vanuit een breed perspectief.

Uit een onderzoek onder ruim 500 IT-professionals blijkt dat remote beheer in potentie een aantal voordelen heeft, zoals afname van het aantal bezoeken aan het rekencentrum, verbeterde beschikbaarheid van IT-voorzieningen en kortere hersteltijd na incidenten. [COMM05] Meer in het algemeen kan remote beheer kosten verlagend werken en de productiviteit van IT-personeel en IT-voorzieningen verbeteren.

Een randvoorwaarde voor remote beheer is een goede informatiebeveiliging. Remote beheer brengt, net als telewerken in het algemeen, andersoortige bedreigingen met zich mee, omdat het voor een deel buiten de beheersbare bedrijfsomgeving plaatsvindt. Dat laatste betekent dat een organisatie mogelijk minder invloed heeft op de beveiliging van (niet vertrouwde) werkstations en (externe) werkplekken van beheerders. Hetzelfde geldt voor de beveiliging van het (publieke) netwerk waarover beheertoegang plaatsvindt. Verder is de impact van incidenten relatief groot. Zo worden er potentieel veel gebruikers getroffen als beheerders in geval van storingen geen beheer op afstand kunnen uitvoeren. Bovendien kan misbruik van beheeraccounts veel schade veroorzaken, omdat deze accounts doorgaans ruime bevoegdheden hebben.

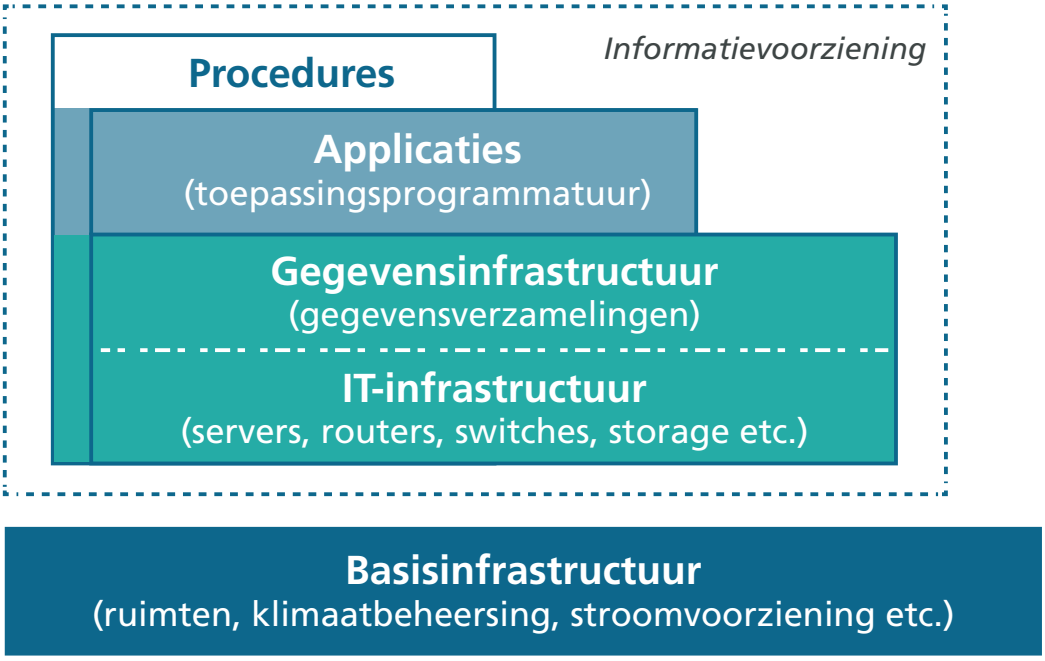
In het vervolg van dit artikel omschrijf ik eerst het begrip 'remote beheer'. Daarna ga ik in op de beveiliging ervan. Ik sluit af met tips voor het uitvoeren van een IT-audit op de beveiliging van remote beheer.

Wat is remote beheer?

Publicaties over remote beheer gaan meestal over specifieke vormen ervan, zoals 'remote support', of over technische oplossingen, zoals 'SSH'. In dit artikel belicht ik remote beheer vanuit een breder perspectief. Als vertrekpunt hiervoor neem ik Wikipedia, waarop staat dat remote beheer verwijst naar de verschillende 'methodes' om een 'computer' te 'besturen' vanaf een 'locatie op afstand'. [WIKI18] De gearceerde onderdelen uit deze omschrijving werk ik hierna verder uit.

Computer: de informatievoorziening

Binnen de context van een organisatie spreekt men meestal niet van 'computers' maar van 'de informatievoorziening'. [OVER00] Deze bestaat uit hard- en software en de daarop van toepassing zijnde procedures en documentatie. De afzonderlijke onderdelen van de informatievoorziening zijn weergegeven in figuur 1.



Figuur 1: de informatievoorziening

Per onderdeel staan tussen haakjes voorbeelden van objecten die daarbij horen. De onderdelen Applicaties en Gegevensinfrastructuur zijn software. De onderdelen IT-infrastructuur en Basisinfrastructuur zijn vaak een combinatie van hard- en software. Deze software wordt basisprogrammatuur genoemd en bestaat uit besturingssystemen, virtualisatiesoftware, firmware en dergelijke. De basisinfrastructuur valt buiten het

gestippelde kader van de figuur, omdat deze volgens Overbeek [OVER00] geen deel uitmaakt van de informatievoorziening. De basisinfrastructuur schept wel de noodzakelijke voorwaarden voor het functioneren ervan en kan ook object van IT-beheer zijn. Daarom maak ik geen hard onderscheid tussen beide begrippen.

Om een object van de informatievoorziening te beheren, heeft een beheerder toegang tot dat object nodig. Deze toegang kan fysiek of logisch (softwarematig) zijn. Voor fysieke toegang moet een beheerder zich bij het object bevinden. Beheer op afstand kan dus uitsluitend via logische toegang worden uitgevoerd. Daaruit volgt dat applicaties en gegevensinfrastructuur in beginsel remote te beheren zijn. Hetzelfde geldt voor objecten uit de IT- en basisinfrastructuur, mits deze voorzien zijn van basisprogrammatuur. Een *unmanaged switch* is een voorbeeld van een object uit de IT-infrastructuur, dat niet op afstand is te beheren. Dat komt doordat dit type switch niet via programmatuur kan worden ingesteld. Dit in tegenstelling tot een *managed switch*.

Besturen: IT-beheer

Het besturen van een computer kan worden beschouwd als 'IT-beheer'. Looijen brengt de IT-beheertaken onder in drie beheereenheden, te weten functioneel beheer, applicatiebeheer en technisch beheer. [LOOI04] Looijen onderscheidt daarnaast drie niveaus waarop IT-beheertaken worden uitgevoerd: strategisch, tactisch en operationeel.

De daadwerkelijke uitvoering van het beheer gebeurt op operationeel niveau. Uitsluitend de operationele IT-beheertaken die via logische toegang worden verricht, zijn remote uitvoerbaar. Dit kunnen taken zijn uit alle drie de beheereenheden. Voorbeelden hiervan staan in de onderstaande tabel. Beheertaken die fysieke toegang vereisen, zoals het vervangen van hardware, kunnen niet op afstand worden uitgevoerd.

Technisch beheer	Applicatiebeheer	Functioneel beheer
Opstarten en bewaken van (batch)verwerking	Beheren van applicatieparameters	Beheren van autorisatie van gegevensgebruik
Installeren en verwijderen van programmatuur	Onderhouden van gegevensbankstructuren	Testen van programmatuur

Tabel 1: Voorbeelden van remote beheertaken per IT-beheereenheid

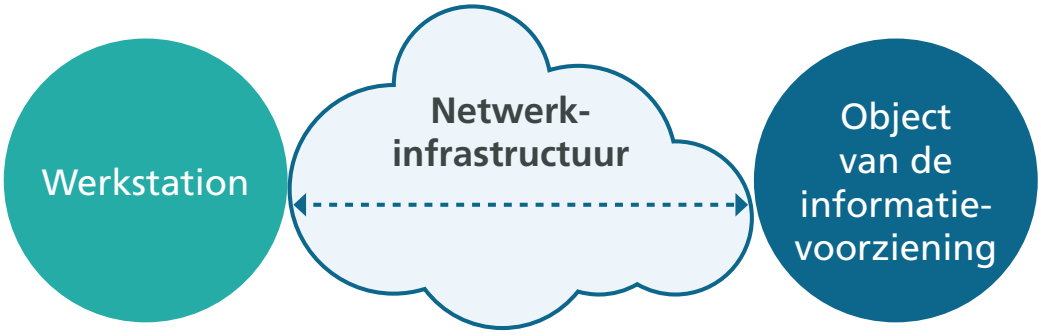
Locatie op afstand

Remote beheer vindt plaats vanaf een locatie op afstand, die kan variëren van een kamer naast de fysieke IT- en basisinfrastructuur tot een plek aan de andere kant van de wereld. De werkplek van een beheerder is vast of flexibel. In het laatste geval werkt de beheerder vanaf wisselende locaties en niet alleen vanuit bijvoorbeeld zijn woning of een satellietkantoor.

Methodes

Remote beheer gebeurt via elk werkstation dat in verbinding staat met een object van de informatievoorziening. Dit is conceptueel weergegeven in figuur 2. Het werkstation kan vast of mobiel zijn. Voorbeelden van mobiele werkstations zijn laptops, tablets en smartphones. De verbinding tussen het werkstation en de informatievoorziening verloopt bij remote beheer via een netwerkinfrastructuur, bijvoorbeeld een *leased line* of internet. Beheer vanaf een console dat rechtstreeks op hardware is aangesloten, is 'lokaal' en niet 'remote'. De beheerder bevindt zich dan immers in de fysieke nabijheid van het te beheren object.

Het te beheren object is met de netwerkinfrastructuur verbonden via een netwerkinterface zoals een fysieke netwerkkaart. Via deze interface wordt software voor het uitvoeren van beheertaken ontsloten. Deze combinatie van software en netwerkinterface noem ik hierna kortweg beheerinterface.



Figuur 2: methode voor remote beheer

Definitie remote beheer

Het voorafgaande samenvattend is remote beheer: het uitvoeren van operationele IT-beheertaken met behulp van een werkstation dat via een netwerkinfrastructuur in verbinding staat met toepassingsprogrammatuur, gegevensverzamelingen of basisprogrammatuur vanaf een locatie op afstand van de onderliggende fysieke IT- of basisinfrastructuur. Deze definitie vormt het uitgangspunt voor de volgende paragraaf.

Beveiliging van remote beheer

In de introductie heb ik het belang aangegeven van beveiliging van remote beheer. De kern is dat remote beheer – ondanks de vele voordelen die het biedt – ook inherent risicovol is en de gevolgen van (a) misbruik van beheerrechten en (b) uitval van beheertoegang groot kunnen zijn. Het is dus van belang om dat te voorkomen. In lijn daarmee onderscheid ik de volgende twee beveiligingsdoelstellingen voor remote beheer.

A Remote beheer is veilig

Uitsluitend geautoriseerde beheerders kunnen op afstand beheertaken uitvoeren op de objecten van de informatievoorziening. Dit betreft de kwaliteitsaspecten vertrouwelijkheid en integriteit.

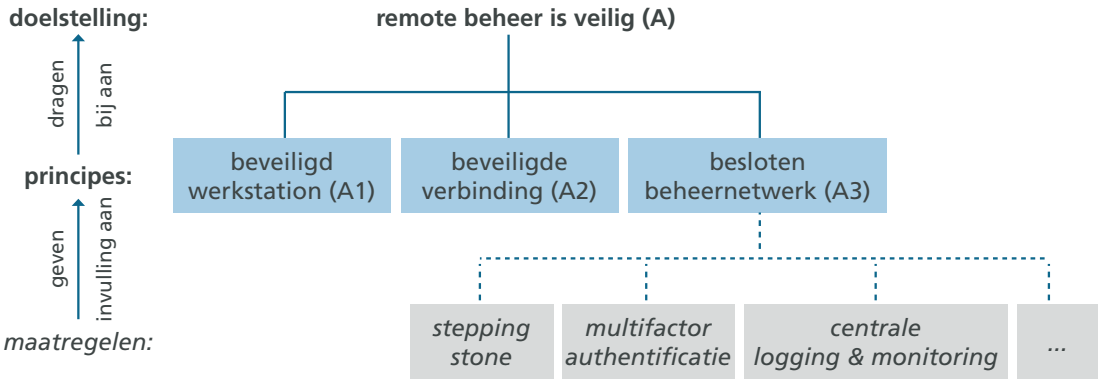
B Remote beheer is mogelijk

De objecten van de informatievoorziening zijn op afstand toegankelijk voor het uitvoeren van IT-beheertaken. Dit betreft het kwaliteitsaspect beschikbaarheid.

Hierna beschrijf ik voor beide doelstellingen de beveiligingsprincipes die bijdragen aan het behalen van deze doelstellingen.[1] Tevens geef ik voorbeelden van beveiligingsmaatregelen. De principes kunnen in combinatie worden toegepast. Dit geeft meer zekerheid dat de betreffende doelstelling wordt behaald. Tussen de twee doelstellingen zelf bestaat echter een spanningsveld, dat ik aan het einde van deze paragraaf behandel. De doelstellingen en principes zijn bruikbaar als uitgangspunt voor de inrichting van beveiliging bij remote beheer, maar ook als referentiekader voor de beoordeling van de adequaatheid ervan.

Doelstelling A: remote beheer is veilig

Figuur 3 geeft de drie beveiligingsprincipes voor doelstelling A weer en enkele voorbeelden van beveiligingsmaatregelen bij het derde principe. Links in de figuur is weergegeven dat de beveiligingsprincipes bijdragen aan de doelstelling dat remote beheer veilig is en dat deze principes worden ingevuld met beveiligingsmaatregelen.



Figuur 3: beveiligingsprincipes bij doelstelling A

Principe A.1: beveiligd werkstation

Het werkstation van de beheerder is via tal van maatregelen te beschermen tegen ongeautoriseerde toegang. Voorbeelden van logische maatregelen zijn identificatie en authenticatie mechanismen, versleuteling van gegevens, anti-malwaresoftware, firewalls en automatisch locken bij inactiviteit. Fysieke beveiliging tegen verlies en met name diefstal is ook denkbaar. Zo kunnen onopvallende tassen worden gebruikt voor het opbergen en transporteren van werkstations. Daarnaast kunnen werkstations worden voorzien

van kabelsloten. Degelijke fysieke maatregelen zijn met name toepasbaar bij de grotere werkstations, zoals laptops en tablets, en minder bij handheld devices, zoals smartphones. Een organisatie heeft meer invloed op de beveiliging van werkstations als ze deze zelf verstrekt en beheert. Om te zorgen dat die beveiliging effectief blijft, is het raadzaam om rechten van gebruikers op de werkstations te beperken. Dat kan bij beheerders een uitdaging zijn, omdat zij vanwege hun functie vaak hoge bevoegdheden nodig hebben.

Principe A.2: beveiligde verbinding

In de vorige paragraaf is aangegeven dat remote beheer plaatsvindt via een netwerkinfrastructuur. De invloed die een organisatie heeft op de (fysieke) beveiliging en het beheer hiervan wisselt. Bij een eigen netwerkinfrastructuur, zoals een leased line, is deze invloed per definitie groter dan bij een publieke infrastructuur, zoals het internet. Met behulp van cryptografie kan de organisatie echter ook invloed uitoefenen op de beveiliging van gegevens die via meer publieke infrastructuren uitgewisseld worden. Zo kan de datacommunicatie tussen het werkstation van de beheerder en het te beheren objecten (end-to-end) worden versleuteld. Als het werkstation van de beheerder gecompromitteerd is, bestaat echter het risico dat via dat werkstation een kwaadwillende alsnog meekijkt of de besturing overneemt. Daarom is het sterker om dit principe toe te passen in combinatie met het voorgaande principe en/of de 'stepping stone' onder het volgende principe.

Principe A.3: besloten beheernetwerk

Dit principe houdt in dat beheerinterfaces van objecten uitsluitend benaderbaar zijn via besloten netwerksegmenten die we beheernetwerken noemen. Om een beheerinterface te benaderen moet een beheerder eerst toegang hebben tot het beheernetwerk. Vanaf een publiek netwerk kan dat bijvoorbeeld door het opzetten van een VPN-tunnel. Bij grotere beheerorganisaties kunnen er verschillende beheernetwerken zijn. Individuele beheerders krijgen dan toegang tot een of meer beheernetwerken, afhankelijk van hun functieprofiel. Toegang tot een beheernetwerk gebeurt uitsluitend op basis van persoonsgebonden accounts. Om brute-force aanvallen te voorkomen is het aantal toegestane foutieve aanmeldpogingen gemaximeerd.

Het besloten karakter van het beheernetwerk helpt voorkomen dat derden kwetsbaarheden in individuele beheerinterfaces uitbuiten. Die kwetsbaarheden ontstaan bijvoorbeeld als gevolg van ontoereikende hardening of patching, lokale beheeraccounts die niet tijdig zijn ingetrokken of waarvan de wachtwoorden bij teveel mensen bekend zijn. Het beveiligingsniveau van het beheernetwerk kan worden vergroot door extra maatregelen te treffen. Zie het tekstkader voor enkele voorbeelden daarvan.

Drie voorbeeldmaatregelen voor een besloten beheernetwerk

Stepping stone

Een stepping stone is een schakel tussen het werkstation van de beheerder en het beheernetwerk. Het beheernetwerk is alleen via deze schakel te benaderen en niet rechtstreeks via het werkstation. Het voordeel hiervan is dat de beveiliging zich kan concentreren op de stepping stone in plaats van op het werkstation. Bij principe A.1 merkte ik op dat het lastig kan zijn om het werkstation goed te beveiligen, omdat de organisatie hier niet altijd invloed op heeft. Dat laatste is bij de stepping stone wel het geval. Een ander voordeel is dat de stepping stone kan worden voorzien van specifieke software die de beheerder nodig heeft. Een stepping stone kan verschillende verschijningsvormen hebben, zoals een opstapserver of een gevirtualiseerde desktop.[2]

Multi-factor authenticatie

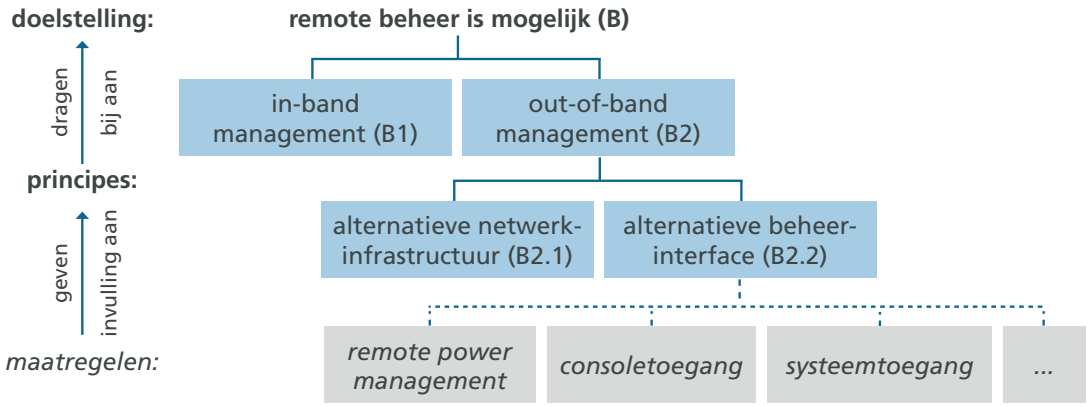
Toegang tot het beheernetwerk vindt plaats na identificatie en authenticatie van de beheerder. Authenticatie op basis van kennis alleen is meestal niet acceptabel, omdat verlies van gebruikersnaam en wachtwoord dan direct tot ongeautoriseerde toegang kan leiden. Daarom is aanvullende authenticatie op basis van bezit (een token, een door de organisatie uitgegeven werkstation e.d.) of biometrische kenmerken van de beheerder (een vingerafdruk e.d.) raadzaam. Als onderdeel van de authenticatie kan ook het beveiligingsniveau van het werkstation worden gecontroleerd, denk bijvoorbeeld aan een firewall, antivirus, logische toegangsbeveiliging, encryptie etc.

Logging en monitoring

Een beheernetwerk geeft de mogelijkheid om beveiligingsgebeurtenissen, zoals aanmeldpogingen met beheeraccounts, meer gecentraliseerd en in samenhang te loggen en monitoren, in plaats van gefragmenteerd per beheerinterface. Dat helpt om verbanden te leggen en patronen te herkennen.

Doelstelling B: remote beheer is mogelijk

De onderstaande afbeelding geeft de beveiligingsprincipes voor doelstelling B weer. Hierin is zichtbaar dat ik twee hoofdprincipes onderscheid. Het eerste principe is gericht op het waarborgen van de continuïteit van het reguliere, ofwel 'in-band', toegangspad voor remote beheer. Het tweede principe gaat uit van een of meer alternatieve, ofwel 'out-of-band', toegangspaden.[3] Dit laatste principe kent op zijn beurt weer twee deelprincipes. Voor deelprincipe B2.2 werk ik enkele voorbeelden van beveiligingsmaatregelen uit.



Figuur 4: beveiligingsprincipes bij doelstelling B

Principe B.1: in-band management

Dit principe heeft betrekking op het waarborgen van de continuïteit van het (reguliere) toegangspad voor remote beheer. Dit toegangspad kan bestaan uit diverse objecten, waaronder routers, switches, firewalls en servers. Er is een breed scala aan maatregelen denkbaar om de beschikbaarheid en performance van het gehele toegangspad te regelen. Voorbeelden hiervan zijn het redundant uitvoeren van objecten in het toegangspad, objecten betrekken van gerenommeerde leveranciers en inrichten volgens hun specificaties, het implementeren van netwerkmonitoring, enzovoorts. Om remote beheer mogelijk te maken is het in ieder geval van belang om single-points-of-failure in het pad zoveel mogelijke te voorkomen. Als er bijvoorbeeld een centraal toegangspunt tot de te beheren objecten is, zoals een stepping stone, dan kan deze worden ingericht als 'high availability' omgeving.

Principe B.2: out-of-band management

Dit principe is gericht op alternatieve toegangspaden voor remote beheer. Dat zorgt ervoor dat het te beheren object ook toegankelijk blijft als het reguliere toegangspad daarvoor is uitgevallen of als er in het te beheren object zelf storingen optreden. In dat kader onderscheid ik twee deelprincipes, te weten een alternatieve netwerkinfrastructuur en een alternatieve beheerinterface. Deze deelprincipes kunnen, net als beide hoofdprincipes, in combinatie worden toegepast.

- *Principe B.2.1: alternatieve netwerkinfrastructuur*
  Volgens dit principe is een te beheren object toegankelijk via verschillende netwerkinfrastructuren. Als de in-band netwerkinfrastructuur uitvalt, bijvoorbeeld door storingen in haar objecten (routers, switches, bekabeling, etc.), dan kan remote beheer via een out-of-band netwerkinfrastructuur plaatsvinden. Er zijn verschillende combinaties van in-band en out-of-band netwerkinfrastructuren denkbaar, waaronder internet, leased lines en inbellen.
- *Principe B.2.2: alternatieve beheerinterface*
  Door storingen in hard- of software kan een beheerinterface uitvallen. Een alternatieve beheerinterface kan ervoor zorgen dat het object dan toch, geheel of gedeeltelijk, beschikbaar blijft voor remote beheer. Door een alternatieve beheerinterface op een alternatieve

netwerkinfrastructuur aan te sluiten, is een 'end-to-end' alternatief toegangspad voor remote beheer te realiseren. Er zijn verschillende manieren om een alternatieve beheerinterface te implementeren. Ik geef hierna drie voorbeelden. Deze staan op volgorde van de mogelijkheden die ze bieden voor het uitvoeren van beheer op afstand (oplopend).

Drie voorbeeldmaatregelen voor een alternatieve beheerinterface

Stroomvoorziening schakelen via remote power management

Remote power management maakt het mogelijk om objecten op afstand via de stroomvoorziening te herstarten als deze zijn vastgelopen. Dit kan automatisch of door tussenkomst van de beheerder. Er zijn diverse methoden voor remote power management. Een beheerder kan bijvoorbeeld inloggen op de UPS en vervolgens kiezen welke server moet worden herstart. Een andere mogelijkheid is dat de UPS zelf luistert naar heartbeat software op het object. Als er geen heartbeat is dan zorgt de UPS automatisch voor een power reset.

Consoletoegang via een consoleserver of KVM-switch

Een consoleserver of KVM-switch[4] biedt toegang tot de systeemconsole van de daarop aangesloten objecten (bijvoorbeeld servers). Hierdoor zijn deze ook benaderbaar wanneer de software, zoals het OS, vastloopt. Consoletoegang stelt de beheerder in staat om BIOS-instellingen te beheren en het gehele opstartproces te monitoren. Een consoleserver of KVM-switch is aangesloten op de fysieke poorten, zoals KVM-poorten of seriële poorten en bereikbaar via een netwerkinterface. Meestal wordt terminal emulator software (bijv. SSH of telnet) of een webbrowser gebruikt om in te loggen op de console server of KVM-switch.

Systeemtoegang via service processor

Een service processor biedt niet alleen toegang tot de systeemconsole van een object maar ook de mogelijkheid tot remote power cycling en het uitlezen van sensorinformatie zoals temperatuur en stroomverbruik. Service processors zijn ook bij software- en hardwarematige storingen benaderbaar, omdat ze gescheiden zijn van CPU, besturingssysteem en applicaties. Ze worden vaak geïmplementeerd als een geïntegreerde processor, een dochterkaart van het moederbord of een volledig gescheiden PCI kaart. Service processors hebben een eigen netwerkinterface of een fysieke poort. In het eerste geval kunnen ze rechtstreeks op een computernetwerk worden aangesloten en in het laatste geval kan dat via bijvoorbeeld een console server.

Spanningsveld tussen veiligheid en toegankelijkheid

Voor iedere doelstelling afzonderlijk geldt dat de zekerheid dat deze wordt behaald, toeneemt naarmate de bijbehorende beveiligingsprincipes meer worden ingevuld. Tussen de twee doelstellingen zelf is echter een spanningsveld. Als het voorkomen van ongeautoriseerde toegang (doelstelling A) zwaar weegt, dan is out-of-band management wellicht minder wenselijk. Meer toegangspaden kunnen immers ook meer potentiële kwetsbaarheden creëren. Andersom geldt dat, als beschikbaarheid van beheertoegang (doelstelling B) zwaar weegt, een bepaald risico op ongeautoriseerde toegang moet worden aanvaard. Veiligheid en toegankelijkheid staan, zoals wel vaker, op gespannen voet met elkaar. Het gaat erom hierin een juiste balans te vinden.

Tot slot

De beveiliging van remote beheer is een interessant onderwerp voor een IT-audit, niet in de laatste plaats omdat remote beheer inherent risicovol is. Dit artikel kan bijdragen aan de opzet en uitvoering van zo'n audit. Het eerste deel van dit artikel waarin ik het begrip 'remote beheer' heb ontleed in een aantal onderdelen, kan de IT-auditor gebruiken om zijn eigen onderzoeksobject systematisch af te bakenen en te bepalen wat de inherente risico's zijn. Relevante aspecten hierbij zijn onder andere welke objecten remote worden beheerd, vanaf welke locaties de beheerders werken en via welke computernetwerken het beheer wordt uitgevoerd. Het tweede deel van dit artikel kan de IT-auditor gebruiken om te onderzoeken of de beveiliging van remote beheer adequaat is. Hiertoe kijkt hij met welke maatregelen in de praktijk invulling wordt gegeven aan de beveiligingsprincipes. Vervolgens weegt hij af in hoeverre dat toereikend is om de bijbehorende beveiligingsdoelstellingen te realiseren. Deze oordeelsvorming blijft maatwerk, maar de aanwijzingen in dit artikel – en eventueel verdere uitwerkingen van beheersingsmaatregelen in beveiligingsstandaarden zoals de NEN-ISO/IEC 27001/2 en de ICT-Beveiligingsrichtlijnen voor Webapplicaties van het NCSC – kunnen de IT-auditor wel houvast bieden.

Literatuur

[COMM05] Communication News: Where's the remote? *Communication News*, 2005.

[HOOG11a] Hoogendijk, L., Schajik van, J.: Beveiliging van telewerken: een praktische aanpak, in: de *IT-auditor*, 2 (2011), pp. 7-14.

[HOOG11b] Hoogendijk, L.: *Beveiliging van Remote Beheer Een 'Good Practice Guidance'*. Afstudeerscriptie Post Graduate IT-audit opleiding Vrije Universiteit Amsterdam, 14 september 2011.

[LOOI04] Looijen, M.: *Beheer van Informatiesystemen.* ten Hagen & Stam uitgevers, 2004.

[OVER00] Overbeek, P., Lindgreen, E.R., Spruit, M.: *Informatiebeveiliging onder controle*. Pearson, 2000.

[WIKI18] Wikipedia: Remote administration. Online beschikbaar via http://en.wikipedia.org/wiki/Remote_administration. Geraadpleegd op 7 november 2018.

Noten

[1] De beveiligingsprincipes en voorbeelden van -maatregelen zijn gebaseerd op literatuurstudie en een meervoudige case study bij vijf organisaties. Dit is uitgevoerd in het kader van een afstudeeronderzoek voor de Post Graduate IT-audit opleiding van de Vrije Universiteit Amsterdam. [HOOG11b]

[2] Opstapserver: de beheerder logt in op het besturingssysteem van een server om van daaruit andere objecten te kunnen beheren. Bij een gevirtualiseerde desktop is het besturingssysteem van het werkstation verplaatst van het lokale werkstation naar het datacenter.

[3] Op Wikipedia worden de begrippen out-of-band en in-band management nader omschreven. De essentie staat in de eerste alinea: 'In computer networks, out-of-band management involves the use of a dedicated channel for managing network devices. This allows the network operator to establish trust boundaries in accessing the management function to apply it to network resources. It also can be used to ensure management connectivity (including the ability to determine the status of any network component) independent of the status of other in-band network components.'

[4] Een KVM-switch is een stuk hardware om meerdere computers te bedienen via een enkel toetsenbord, monitor en muis.

C.H. (Lars) Hoogendijk MSc RE CISA | Senior Auditor bij *Provincie Zuid-Holland*

C.H. (Lars) Hoogendijk MSc RE CISA | Senior Auditor bij Provincie Zuid-Holland

Lars Hoogendijk werkt sinds vier jaar bij de Eenheid Audit en Advies van de provincie Zuid-Holland. Hier verricht hij onder andere onderzoek op het gebied van informatiebeveiliging en privacy. Daarvoor was Lars ruim zeven jaar werkzaam als IT-auditor bij BDO. Hier richtte hij zich voornamelijk op assurance-opdrachten bij IT-dienstverleners. Lars heeft de IT-auditopleiding van de Vrije Universiteit afgerond. Zijn afstudeerscriptie ligt aan de basis van dit artikel. Dit artikel is op persoonlijke titel geschreven.