Remote beheer richtlijn voor leveranciers

Afdeling: ICT Expertisecentrum
Datum: 30-09-2024
Auteur: Bas Rabeling
Versie: 1.0

www.hetcak.nl

Wijzigingshistorie

VERSIE	DATUM	AUTEUR	OMSCHRIJVING	VERZONDEN AAN	STATUS
0.9	09-07-2024	Bas Rabeling	Eerste versie nieuwe document	Linda Dellouche	Draft
0.91	11-07-2024	Bas Rabeling	Review opmerkingen verwerkt	Linda Dellouche Dirkjan Joor	Draft
0.92	18-09-2024	Bas Rabeling	Review opmerkingen verwerkt	Walter van Oostrum	Draft
1.0	30-09-2024	Bas Rabeling	Kleine aanpassing + vastgesteld	DWO	Final

Goedkeuringshistorie

VERSIE	DATUM	AUTORISATIE	J/N	TOELICHTING
1.0	30-09-2024	Walter van Oostrum	J	

Bijlagen en verwijzingen

VERSIE	DATUM

Inhoudsopgave

Inleiding

Het doel van dit document is om aan te geven op welke wijze leveranciers beheer op afstand kunnen uitvoeren binnen de CAK omgeving, aan welke eisen de leveranciers moeten voldoen en welke afspraken er met de leveranciers gemaakt moeten worden. Deze richtlijn is van toepassing op zowel de on premise omgeving(en) als om cloudomgeving(en) van het CAK.

1. Soorten beheer

1.1. Inleiding

Dit hoofdstuk beschrijft welke soorten beheer door externe partijen kunnen worden uitgevoerd op CAK netwerken.

1.2. Incidentele support & ondersteuning

In dit scenario wordt het beheer door het CAK uitgevoerd maar moet de leverancier toegang krijgen tot de applicatie in geval van support verzoeken of incidenten.

1.3. Functioneel beheer door leverancier

In dit scenario wordt het functioneel beheer door de externe leverancier verzorgd, het technisch beheer blijft hierbij bij het CAK.

1.4. Technisch beheer door leverancier

In dit geval wordt het technisch beheer door de leverancier uitgevoerd, functioneel beheer wordt door het CAK uitgevoerd.

2. Soorten toegang

2.1. Inleiding

Dit hoofdstuk beschrijft welke soorten toegang het CAK leveranciers biedt voor het uitvoeren van werkzaamheden op het netwerk.

2.2. Schermovername

Hoewel de standaard werkwijze is dat er Remote Beheer afspraken zijn met een firma om ondersteuning te leveren aan het CAK, is het soms noodzakelijk om een externe partij het scherm over te laten nemen voor incidenteel support en ondersteuning.

2.3. VDI toegang

Wanneer voor het beheer of ondersteuning van een CAK systeem een externe leverancier is gekozen kan deze de dienst invullen met Remote Beheer. De standaard oplossing hiervoor is dat toegang verkregen kan worden tot de CAK systemen middels het Remote Desktop portaal met 2-factor authenticatie.

Hierbij logt de externe partij in op de CAK omgeving op een KA account voor externen (met minimale rechten). Vanuit de KA VDI kan met een ADM account worden ingelogd op de AppBeheer VDI. Deze moet zodanig worden ingericht dat de externe partij alleen toegang heeft tot de applicaties die door deze partij beheerd moeten worden.

In dit geval worden de accounts en 2FA uitgegeven door het CAK. Dit heeft als voordeel dat indien de leverancier wordt gecompromitteerd dit geen gevolgen voor het CAK hoeft te hebben.

2.4. VPN tunnel monitoring

Wanneer voor de dienstverlening VPN toegang nodig is voor monitoring (24x7) kan een Site-to-Site VPN verbinding worden ingericht voor de monitoring protocollen. De VPN verbinding is uitsluitend voor monitoring en kan zowel voor functioneel als technisch beheer worden gebruikt. Het is niet toegestaan om beheerwerkzaamheden over deze VPN verbinding uit te voeren.

2.5. VPN toegang beheer

Wanneer VDI toegang niet werkbaar is voor de leverancier kan er ook gekozen worden voor een directe VPN connectie tussen de leverancier en het netwerk van het CAK. In dat geval gelden er aanvullende security eisen voor de leverancier (zie paragraaf 4.5). Aan de kant van het CAK is het belangrijk dat de leverancier op een eigen VLAN binnenkomt binnen het CAK netwerk via een stepping stone server. De leverancier moet hierbij alleen toegang krijgen tot de systemen die hij moet beheren en geen andere CAK systemen kunnen benaderen.

3. Toegang per type beheer

3.1. Inleiding

Dit hoofdstuk beschrijft per type beheer welke soort toegang is toegestaan. Hierbij wordt het type beheer uit hoofdstuk 1 gelinkt aan de soorten toegang uit hoofdstuk 2.

3.2. Toegang voor support en ondersteuning bij incidenten

Wanneer de leverancier toegang nodig heeft tot de CAK omgeving voor support of ondersteuning bij incidenten dan zijn er een aantal mogelijkheden op basis van de afspraken met de leverancier die zijn vastgelegd in de overeenkomst. Uitzonderingen op gemaakte afspraken moeten vooraf getoetst worden door de Information Security Officer.

3.3. Incidenteel ad hoc beheer

Indien er sprake is van incidenteel ad hoc beheer zonder beheerafspraken met de leverancier, dan is schermovername de aangewezen werkwijze. Denk hierbij aan de situatie waarbij een leverancier toegang tot onze omgeving nodig heeft om een incident te onderzoeken zonder dat deze leverancier verantwoordelijk is voor het beheer. Zie paragraaf 2.2 voor meer informatie.

3.4. Toegang voor functioneel beheer

Voor het uitvoeren van functioneel beheer werkzaamheden binnen de CAK omgeving is VDI toegang (paragraaf 2.3) de aangewezen methode. Eventueel aangevuld met VPN tunnel monitoring (paragraaf 2.4) wanneer de omgeving van het CAK moet worden gemonitord door de leverancier.

3.5. Toegang voor technisch beheer

Wanneer de leverancier het technisch beheer gaat uitvoeren binnen de CAK omgeving dan zijn er 2 mogelijkheden waarop dit kan worden uitgevoerd:

1. Met VDI toegang (paragraaf 2.3), eventueel aangevuld met VPN tunnel monitoring (paragraaf 2.4). Deze vorm van toegang is de voorkeursoplossing voor het CAK;
2. Met VPN toegang tot de CAK omgeving (paragraaf 2.5). Hiervoor gelden aanvullende security eisen (zie paragraaf 4.5). Deze vorm van toegang wordt in principe alleen ingezet wanneer VDI toegang niet voldoet, dit ter beoordeling door de Information Security Officers. Denk bijvoorbeeld aan een situatie waarbij 24*7 technisch beheer wordt geleverd.

4. Security vereisten

4.1. Inleiding

In dit hoofdstuk worden de security eisen per type toegang aangegeven. Deze gelden bovenop de security eisen uit de Richtlijn uitbesteding ICT- en Clouddiensten.

4.2. Schermovername

Voor schermovername gelden de volgende voorwaarden:

1. De CAK beheerder is verantwoordelijk voor de uitgevoerde handelingen;
2. De CAK beheerder houdt gedurende de schermovername toezicht op de handelingen van de remote beheerder. Bij het (tijdelijk) verlaten van de werkplek moet de remote beheer sessie afgebroken zijn;
3. Het delen van vertrouwelijke- en bijzonder vertrouwelijke data gebeurt conform de “Richtlijn Omgang met CAK data”. Voor het delen van persoonsgegevens is een ook verwerkingsovereenkomst noodzakelijk.
4. Het CAK neemt het initiatief voor het overnemen van het scherm. De beheer partij kan niet zelfstandig een scherm overname sessie starten;
5. Software of plug-ins installeren voor schermovername is niet toegestaan;
6. Het maken van schermopnames en screenshots door de leverancier is niet toegestaan. Hierover moeten contractuele afspraken worden gemaakt.

4.3. VDI toegang

Uitgangspunt voor informatiebeveiliging, ten aanzien van dit document voor u (RemoteBeheer Security Richtlijn Leverancier:

1) Alle beveiligingsmaatregelen die gelden voor de CAK medewerkers of inhuur voor toegang tot de betreffende informatie gelden ook voor de personen die op basis van remote beheer toegang hebben tot de informatie. Denk hierbij bijvoorbeeld aan de eis om alleen met 2FA toegang tot de CAK omgeving te kunnen krijgen.
2) De toegang is beperkt tot de noodzakelijke systemen;
3) De afspraak wordt bevestigd met een getekende overeenkomst (Contract/SLA) met de remote beheer partij dat deze instemt met de afspraken over informatiebeveiliging. Zonder deze overeenkomst krijgt een beheer partij geen toegang tot de CAK omgeving.

Overige bepalingen, in aanvulling op de eisen uit de ‘Richtlijn uitbesteding ICT- en Clouddiensten:

1) Toegang wordt alleen geautoriseerd op basis van een melding gedaan bij het ServiceCenter CAK en geaccordeerd door het CAK changeproces;
2) Wanneer toegang tot (productie) data uit de beheerde systemen noodzakelijk is voor het beheer zal een verwerkersovereenkomst afgesloten worden die de juridische basis vormt voor toegang tot deze systemen;
3) Toegang tot systemen wordt verstrekt op een persoonlijk ‘named’ account. Anonieme accounts zijn niet toegestaan. Persoonlijke accounts mogen niet gedeeld worden;
4) De leverancier is verantwoordelijk voor het aanmelden van nieuwe remote beheer medewerkers en het afmelden van de medewerkers die niet langer betrokken zijn bij het remote beheer of niet langer in dienst bij de leverancier. Het afmelden van medewerkers moet uiterlijke 2 dagen voor de uit dienst treding worden gemeld bij het CAK. Hierop wordt periodiek door het CAK een controle op uitgevoerd;
5) Het aantal personen met toegang tot de CAK omgeving dient zo beperkt mogelijk te zijn;
6) Toegang is beperkt tot alleen de systemen die benoemd zijn in de SLA middels een specifiek profiel;
7) Door leverancier geconstateerde datalekken worden binnen 24 uur aan ServiceCenter CAK gemeld;
8) Medewerkers van de leverancier moeten een Verklaring Omtrent Gedrag (VOG) aanleveren aan het CAK om toegang te krijgen tot de VDI. De VOG screening vindt plaats op profiel 95, Financiële dienstverlening. De verantwoordelijkheid voor de controle hierop kan ook worden uitgevoerd door de leverancier zelf in samenspraak met het CAK.
9) Medewerkers van de leverancier moeten een geheimhoudingsverklaring tekenen en aanleveren aan het CAK. Dit ook contractueel tussen het CAK en de leverancier worden geregeld;
10) Medewerkers van leverancier moeten de periodieke interne security en privacy awareness training met goed gevolg afleggen via de website van de CAK academie of aantoonbaar een soortgelijke periodieke training met goed gevolg afleggen via de leverancier;
11) Medewerkers van de leverancier moeten op de hoogte worden gesteld van de locatie van het security beleid en de inhoud van het e-mail en internet protocol.
12) Beheerwerkzaamheden mogen alleen worden uitgevoerd uit de Europese Economische Ruimte;
13) Significante security incidenten [1]moeten binnen 4 uur worden gemeld aan het CAK.

[1] Een “significant” incident is een incident dat ernstige operationele onderbreking van de service of financiële verliezen heeft veroorzaakt of kan veroorzaken, of als het incident aanzienlijke verliezen heeft veroorzaakt of kan veroorzaken voor anderen.

4.4. VPN tunnel monitoring

1) De VPN tunnel voor monitoring mag alleen gebruikt worden voor monitoring en niet voor beheerwerkzaamheden;
2) Er mogen geen persoonsgegevens worden gebruikt in de monitoring naar de leverancier;
3) De versleuteling vindt plaats door middel van encryptie algoritmes en ciphers die door het Nationaal Cyber Security Center (NCSC) minimaal als voldoende zijn aangemerkt;
4) De verdere inrichting moet worden afgestemd met security en netwerkbeheer van het CAK.

4.5. VPN tunnel beheer

1) De leverancier moet beschikken over een SOC2 type II verklaring welke van toepassing is op de aan het CAK te leveren diensten en aantoonbaar betrekking heeft op de CAK omgeving. Deze wordt beoordeeld door security. Eventuele bevindingen worden door security beoordeeld en moeten door de business worden geaccepteerd.
2) Er dient een aan de CAK regie organisatie gelieerde governancestructuur ingericht te zijn met aanspreekpunten en periodiek service review overleg, waar ook eventuele bevindingen uit de SOC 2 en de opvolging daarop besproken worden.
3) Een Dossier Afspraken en Procedures (DAP) te zijn overeengekomen waarin de onderwerpen aan bod komen van ‘algemene beheersing van ICT- diensten’ van NOREA en PvIB.
4) Ter goedkeuring van security van het CAK moet uit de aangeleverde documentatie van de leverancier blijken op welke wijze de leverancier de toegang tot de CAK omgeving heeft beperkt en beveiligd. Den hierbij bijvoorbeeld aan het gebruik van 2FA en het beperken van het aantal personen dat toegang tot de omgeving krijgt.
5) De leverancier moet een netwerkplaat aanleveren voor de wijze waarop men verbinding met het CAK wil maken. Deze moet goedgekeurd worden door security en netwerkbeheer van het CAK;
6) De versleuteling vindt plaats door middel van encryptie algoritmes en ciphers die door het Nationaal Cyber Security Center (NCSC) minimaal als voldoende zijn aangemerkt;
7) Het aantal personen met toegang tot de CAK omgeving dient zo beperkt mogelijk te zijn;
8) Door leverancier geconstateerde datalekken worden binnen 24 uur aan ServiceCenter CAK gemeld;
9) De leverancier is er voor verantwoordelijk dat medewerkers die werkzaamheden op het CAK netwerk uitvoeren beschikken over een VOG (profiel 95, Financiële dienstverlening) en geheimhoudingsverklaring. Hierover moeten afspraken met de leverancier worden gemaakt. De verantwoordelijkheid voor de controle hierop kan ook worden uitgevoerd door de leverancier zelf in samenspraak met het CAK.
10) Medewerkers van leverancier moeten via de leverancier een periodieke (minimaal jaarlijks) security en privacy awareness training met goed gevolg hebben afgelegd;
11) Voor het uitvoeren van werkzaamheden op het CAK netwerk moet een verwerkingsovereenkomst worden afgesloten.
12) Significante security incidenten[2] moeten binnen 4 uur worden gemeld aan het CAK;
13) Toegang tot systemen wordt verstrekt op een persoonlijk ‘named’ account. Anonieme accounts zijn niet toegestaan. Persoonlijke accounts mogen niet gedeeld worden;
14) Beheerwerkzaamheden mogen alleen worden uitgevoerd uit de Europese Economische Ruimte.

[2] Een “significant” incident is een incident dat ernstige operationele onderbreking van de service of financiële verliezen heeft veroorzaakt of kan veroorzaken, of als het incident aanzienlijke verliezen heeft veroorzaakt of kan veroorzaken voor anderen.

5. Afspraken met leverancier

5.1. Inleiding

Dit hoofdstuk beschrijft de afspraken die met de leverancier moeten worden gemaakt en vastgelegd. Dit zodat ieders verantwoordelijkheden duidelijk zijn.

5.2. Afspraken met leveranciers

In de onderstaande tabel staat een overzicht van afspraken die met leveranciers moeten worden gemaakt in het geval van beheer op afstand. Deze lijst is niet uitputtend.

Type afspraak	Schermovername	VDI toegang	VPN monitoring	VPN Beheer
Afspraken informatiebeveiliging		Ja	Ja	Ja
Aan- en afmelden medewerkers		Ja		
Afspraken over VOG en geheimhoudingsverklaring		Ja		Ja
Afspraken over de locatie van de werkzaamheden		Ja		Ja
Afspraken over toegang medewerkers leverancier (aantal en wijze)				Ja
Afspraken over kwetsbaarheden scanning		Ja		Ja
Afspraken over patching		Ja		Ja
Afspraken over maken backups		Ja		Ja
Afspraken technische inrichting VPN tunnel			Ja	Ja
Afspraken over melden datalekken		Ja		Ja
Afspraken over het melden van significante security incidenten		Ja		Ja
Afspraken periodiek aanleveren SOC2 type II				Ja