Aansluitvoorwaarden en inzetregels

JuBIT3

Justitie Beveiligde Internet Toegang (JuBIT)

Versie 1.2
Datum 3 augustus 2023

Colofon

Projectnaam	JuBIT3
Versienummer	1.2
Afzendgegevens	**Ministerie van Justitie en Veiligheid** **Directie Informatisering en Inkoop** Turfmarkt 147 2511 DP Den Haag Postbus 20301 2500 EH Den Haag
Contactpersonen	Projectgroep JuBIT3
Auteur	Projectgroep JuBIT3

Versiebeheer

Versie	Datum	Wijzigingen
0.1	16 maart 2022	Initiele versie door projectteam
0.2	30 maart 2022	Diverse aanvullingen en concept versie
0.21	4 april 2022	Correcties in de tekst
0.22	4 april 2022	Correcties in de tekst
0.3	5 april 2022	Laatste wijzigingen na interne bespreking door de werkgroep IB en het projectteam
0.4	25 mei 2022	Commentaar verwerkt uit de eerste review ronde
0.5	1 juni 2022	Commentaar verwerkt uit de tweede review ronde
0.51	16 juni 2022	Inzetregels bij 5.2 aangescherpt en commentaar uit de werkgroep
0.9	6 juli 2022	Afstemming met architecten
0.91	6 juli 2022	Toevoegen van open standaarden van Forum Standaardisatie
0.92	11 oktober 2022	Aanvullingen Solvinity architecten en collegiale review.
1.0	Definitief (Concept)	Laatste commentaar verwerkt uit interne review rondes.
1.1	Definitief (Concept)	Verwijziging naar BIO maatregelen opgenomen n.a.v. behandeling in CISO raad.
1.2	Definitief (Concept)	PTR records voor DNS opgenomen, volgt uit actie 4 JuBIT3 Archtitectuur overleg.

Inhoudsopgave

1 Inleiding

Justitie Beveiligde Internet Toegang (JuBIT) is het beveiligd koppelvlak tussen het interne vertrouwde landelijke datacommunicatie netwerk (Justitienet) dat Justitie en Veiligheid (MinJenV) in gebruik heeft en externe netwerken zoals internet, partnernetwerken (Publieke partijen en semi-overheidspartijen) en overheidsnetwerken (Haagse Ring, Diginetwerk, Rijksoverheidsnetwerk).

Met de digitale overheid neemt digitale communicatie tussen burgers, bedrijven en instellingen en de overheid toe.
JuBIT3 speelt een belangrijke rol in deze digitale communicatie, enerzijds om te voorzien in de (business) behoefte aan communicatie met de buitenwereld van individuele Deelnemers, applicaties en toepassingen, anderzijds om te zorgen dat de belangen van MinJenV als geheel beschermd worden.

Belangrijke doelstellingen voor JuBIT3 zijn:
- Veiligheid
- Stabiliteit en continuïteit
- Innovatie
- Flexibiliteit

De doelstellingen voor JuBIT3 zijn omgezet in het plan van eisen en wensen[1]. Verplichte- en aanbevolen standaarden van Forum Standaardisatie worden gevolgd bij de inrichting van JuBIT3.

Om de doelstellingen te halen voor het gebruik van JuBIT3, zijn spelregels nodig; Inzetregels en Aansluitvoorwaarden. Dit document bevat de verschillende inzetregels en aansluitvoorwaarden. Deze zijn dynamisch van aard en zullen meegroeien met de innovatie van JuBIT, de mogelijk veranderende behoefte van de Deelnemers en de beveiligings eisen die de omgeving aan JuBIT stelt. Hoe wijzigingen tot stand komen staat beschreven in procesbeschrijving Beheersen uitzonderingen en wijzigingen.
Alle brondocumenten die als referentie zijn gebruikt bij het opstellen van dit document, zijn ook te vinden in een subfolder Referentie stukken in de SWF.

1 Zie Samenwerkingsruimte JuBITmigratie Bijlage 3 Programma van Eisen en Wensen v1.0 (inloggen met SSO is noodzakelijk)

2 Begrippen

Begrip	Definitie
Aansluitvoorwaarde	Aansluitvoorwaarden geven de minimale set van eisen waaraan een Deelnemer moet voldoen om van JuBIT3 diensten gebruik te maken.
Deelnemer	Een dienstonderdeel van het ministerie van Justitie en Veiligheid of een ander organisatieonderdeel zoals vermeld in paragraaf 1.3 van de Selectieleidraad, die van JuBIT3 gebruik zal maken.
DKIM	Domain Keys Identified Mail; een methode voor een ontvanger om vast te stellen dat de mail afkomstig is van een domein welke bij de houder in eigendom is.
DMARC	Domain-based Message Authentication, Reporting and Conformance; instructies voor de ontvanger wat met phishing mail gedaan moet worden en waar misbruik gemeld kan worden.
Forum Standaardisatie	Forum Standaardisatie ondersteund de publieke sector bij het gebruik van ICT-standaarden. Overheidsorganisaties zijn verplicht om, bij aanschaf van ICT-producten of ICT-diensten van € 50.000,- of meer, te kiezen voor de relevante standaarden die op de 'Pas toe of leg uit'-lijst staan.
Inzetregels	Inzetregels geven aan hoe de JuBIT3 diensten gebruikt kunnen worden, waarbij niet alles wat (technisch) mogelijk is vanuit oogpunt van veiligheid en/of stabiliteit wordt toegestaan.
JuBIT	Justitie Beveiligde Internet Toegang.
SPF	Sender Policy Framework; een lijst met mailservers die e-mail mogen versturen voor een domein. SPF is onderdeel van een set maatregelen gericht op voorkomen en detecteren van phishing mail.
Tanium	Gemeenschappelijk dienst voor Asset management, Vulnerability management, Baseline configuratie management en Threat hunting.
Zonering	Groepering van onderdelen met een gelijk vertrouweijkheidsniveau. JuBIT kent verschillende vertrouwelijkheidsniveaus: Onvertrouwd, Semi-vertrouwd en Vertrouwd (Departementaal Vertrouwelijk of DV).
Zoneovergang	Overgang naar een zone met een hoger of lager vertrouwelijkheidsniveau.

3 Algemene beleidsuitgangspunten

JuBIT is de Security Perimeter van MinJenV en vormt de grens tussen het MinJenV security domein en de buitenwereld. Binnen het MinJenV security domein is er een groot onderling vertrouwen mogelijk door het hanteren van een gemeenschappelijk informatiebeveiligings- en aansluitbeleid:

- Binnen MinJenV wordt de BIO als ondergrens gehanteerd voor JuBIT, JustitieNet en het eigen ICT domein van de Deelnemer.
- Elke Deelnemer kan aanvullend informatiebeveiligingsbeleid hanteren.
- Dit document beschrijft de gemeenschappelijke JuBIT aansluitvoorwaarden en inzetregels en is gebaseerd op staande afspraken/beleid.

JuBIT heeft als centrale opgang van JustitieNet naar de buitenwereld, de functie om zoneovergangen op een veilige manier mogelijk te maken. Alle verkeer van en naar de buitenwereld of zoneovergangen binnen MinJenV loopt via JuBIT.

Zero trust en hardening vormen in de basis het uitgangspunt voor JuBIT3. Dit betekent dat verkeer door de firewall van en naar de buitenwereld standaard uit staat op alle poorten behalve diegene die gebruikt moet worden. Security by obscurity wordt niet toegepast, applicaties gebruiken in principe de standaard poort[2], er is geen noodzaak om een applicatie bewust op een afwijkende poort te configureren voor veiligheidsoverwegingen.
Dit document beschrijft de standaard Inzetregels en Aansluitvoorwaarden. Eventuele afwijkingen hierop zijn mogelijk. Zie hiervoor de procesbeschrijving Beheersen uitzonderingen en wijzigingen.

2 List of TCP and UDP port numbers - Wikipedia

4 Aansluitvoorwaarden

De Aansluitvoorwaarden geven de minimale set van eisen waaraan een Deelnemer moet voldoen om van JuBIT3 diensten gebruik te maken. Onderstaande tabel geeft een overzicht van alle Aansluitvoorwaarden, de achterliggende paragraven geven een toelichting daarop.

Nr	Aansluitvoorwaarden	Paragraaf
1	Alle verkeersstromen tussen JustitieNet en internet of partnernetwerken dienen in JuBIT ontkoppeld te worden zodat verkeer geïnspecteerd kan worden.	4.1
2	Sectorale proxies van een Deelnemer kennen geen andere externe koppelingen dan met de JuBIT dienst Veilig Browsen (Centrale Proxy).	4.1.1
3	MinJenV diensten die aangeboden worden aan externe partijen worden middels een reverse proxy, web application gateway of soortgelijke device/service ontsloten.	4.1.2
4	Alle inkomende en uitgaande mail van interne mailservers op Justitienet wordt langs de JuBIT dienst Veilig Mailen (mailrelay) geleid en geinspecteerd	4.1.3
5	Anti-Phishing maatregelen voor domeinen van de Deelnemers zijn aanwezig en voldoen aan de eisen van Forum Standaardisatie.	4.1.3
6	Instellingen van SPAM filters en actie zijn herleidbaar naar een eigenaar en zijn onderbouwd.	4.1.3
7	De Deelnemer sluit de eigen DNS aan op DNS router in JubIT3 voor resolving van eigen diensten door andere deelnemers en de forwarding van DNS vragen.	4.1.4
8	De Deelnemer implementert tenminste SOA, NS, A, MX en PTR records op de eigen DNS.	4.1.4
9	Domeinnamen volgen de naamconventie.	4.1.4
10	De Deelnemer gebruikt de JuBIT NTP voor de tijdsynchronisatie van de eigen systemen gehost in JuBIT3.	4.1.5
11	JenV Trusted Cloud is alleen te benaderen langs de daarvoor aangewezen ontsluiting in JuBIT3 (expressroute).	4.1.6
12	Voor elk informatiesysteem in JuBIT3 is de verantwoordelijke lijnmanager bekend.	4.2
13	Alle instellingen en security policies voor het betreffende informatiesysteem zijn herleidbaar naar de eigenaar (=lijnmanager).	4.2
14	Communicatie tussen verschillende veiligheidszones, al dan niet van verschillend niveau, verloopt via het beveiligd koppelvlak JuBIT.	4.3

4.1 Verkeersstromen

JuBIT heeft als centrale opgang van JustitieNet naar de buitenwereld de functie om zoneovergangen op een veilige manier mogelijk te maken. Het is daarom een eis van JenV dat verkeersstromen ontkoppeld worden in JuBIT. Ontkoppeling van verkeersstromen biedt de mogelijkheid om dit verkeer te inspecteren en vanuit een beheer perspectief de verkeersstroom toe te kennen aan een bepaalde toepassing/applicatie. Om deze onkoppeling te faciliteren, zijn in JuBIT centrale voorzieningen aanwezig waar een Deelnemer op aan dient te sluiten:

- Centrale proxy voor toegang tot webdiensten (o.a. veilig browsen)
- Reverse proxy voor het ontsluiten van MinJenV diensten
- Mailrelay voor verzenden en ontvangen van e-mail
- DNS voor resolving van IP adressen
- NTP voor synchronisatie van systeemklokken
- JenV Trusted cloud

Nr	Aansluitvoorwaarden
1	Alle verkeersstromen tussen JustitieNet en internet of partnernetwerken dienen in JuBIT ontkoppeld te worden zodat verkeer geïnspecteerd kan worden.

4.1.1 Centrale Proxy

De toepassing Veilig browsen stelt gebruikers binnen MinJenV in staat om op een veilige wijze gebruik te maken en toegang te krijgen tot websites en informatiebronnen op het internet en extranetten. Deze toegang omvat naast gebruikers via browsers ook applicatie koppelingen. In de toepassing Veilig browsen zijn beveiligingsmechanismes actief die schadelijke content detecteren, blokkeren en verwijderen. Ook biedt Veilig browsen door URL-filtering de mogelijkheid om beleid te implementeren voor "Acceptabel internetgebruik". Gebruik van SaaS diensten op internet wordt centraal gemonitored met CASB.

De huidige inrichting van deze toepassing voorziet hierin door middel van proxies. Een centrale proxy (CP) voorziet in content filtering (virus/malware scanning), URL-filtering (malware/schadelijk) en mogelijkheden om versleuteld (TLS/SSL) verkeer te inspecteren. Elke Deelnemer heeft minimaal één sectorale proxy (SP), welke voorziet in de herleidbaarheid door koppeling naar de sectorale identiteiten van gebruikers. Voor de juiste werking zijn de sectorale proxies van een Deelnemer aangesloten op de Centrale Proxy. Andere koppelingen zijn niet toegestaan met uitzondering van verkeer met bestemming binnen Justitienet.

Afwijken is mogelijk voor datastromen waarvan inspectie onwenselijk is gelet de gevoeligheid van de gegevens, vanwege het real-time karakter en de gevoeligheid voor latency of jitter of datastromen waarbij TLS interceptie niet mogelijk is of sterk wordt afgeraden.

Nr	Aansluitvoorwaarden
2	Sectorale proxies van een Deelnemer kennen geen andere externe koppelingen dan met de JuBIT dienst Veilig Browsen (Centrale Proxy).

4.1.2 Reverse proxy

Om diensten binnen het netwerk van MinJenV ter beschikking te stellen aan externe partijen, wordt een reverse proxy ter beschikking gesteld die verbindingen vanaf de externe zones doorzet naar de front-end servers binnen JuBIT, welke uiteindelijk connectie hebben naar de back-end servers op JustitieNet. De reverse proxy kan ook worden gebruikt voor diensten van de verschillende Deelnemers onderling.

De reverse proxy voorziet in content filtering (virus/malware scanning) en mogelijkheden om versleuteld (TLS/SSL/FTPS) en onversleuteld (http/FTP) verkeer te inspecteren. Een reverse proxy wordt ingezet voor alle verkeerstromen die een zone-overgang hebben (Zie ook 4.3 Zonering).

Nr	Aansluitvoorwaarden
3	MinJenV diensten die aangeboden worden aan andere Deelnemers of externe partijen worden middels een reverse proxy ontsloten.

4.1.3 Mailrelay

De mailrelay zorgt voor het routeren van de e-mail berichten tussen Deelnemers onderling, tussen Deelnemers en partners en tussen de Deelnemer en de buitenwereld, internet. De belangrijkste taak van de JuBIT3 mailrelay is te zorgen voor een veilige e-mail omgeving voor MinJenV, de Deelnemers en haar medewerkers.

Technisch voorziet de mailrelay in het ontvangen, het bufferen, het schonen, routeren en afleveren van e-mail. Deze mailrelay heeft een externe en interne mailrelay functie. De externe mailrelay functie zorgt dat interne mailservers van Deelnemers mail naar internet of ketenpartijen kunnen routeren. Omgekeerd zorgt de externe mailrelay dat mail van internet en ketenpartijen, op basis van domeinen en subdomeinen, naar de juiste interne mailserver van Deelnemers wordt gerouteerd. De interne mailrelay functie zorgt voor routeren van onderling e-mailverkeer tussen de interne mailservers van Deelnemers. Externe aansluitingen van de interne mailservers van een Deelnemer anders dan de Mailrelay, zijn niet toegestaan.

De mailrelay filtert inkomende mail op Spam en Phishing. Spam wordt in quaraintaine geplaatst. Phishing mail wordt gedetecteerd aan de hand van kenmerken van de zendende mailserver (SPF/DKIM/DMARC) en inhoud. Phishing mail wordt in lijn met instructies van het zendende domein verwerkt (verwijderen of quarantaine) en afwijkingen worden door de ontvangende mailserver gerapporteerd naar de zendende mailserver. Uitgaande mail van de Deelnemers wordt door de mailrelay voorzien van basis anti-phishing maatregelen. De Deelnemer is verantwoordelijk voor de aanvulling en actualiteit van uitgaande mailservers (SPF) en acties voor Phishing mail (DMARC).
De antimalware software scant alle binnenkomende en uitgaande mails op virussen en malware, zowel externe als interne mailrelay. Ook bijlagen worden gecontroleerd. Als controleren van een bijlage niet mogelijk is, dan wordt de mail in quarantaine geplaatst. Van verdachte, geïnfecteerde of geblokkeerde e-mail of bestanden, ontvangt de beoogde ontvanger een meldingen.

Nr	Aansluitvoorwaarden
4	Alle inkomende en uitgaande mail van mailservers op Justitienet wordt langs de JuBIT dienst Veilig Mailen (mailrelay) geleid en geinspecteerd.
5	Anti-Phishing maatregelen voor domeinen van de Deelnemers zijn aanwezig en voldoen aan de eisen van Forum Standaardisatie.
6	Instellingen van SPAM filters en actie zijn herleidbaar naar een eigenaar en zijn onderbouwd.

4.1.4 DNS

De JuBIT DNS dienst bestaat uit een JuBIT DNS Router die verkeer naar de Interne Autorative (IA) DNS, Internet, Rijksweb, etc routeert en een Externe Publieke DNS dienst. MinJenV Deelnemers gebruiken de JuBIT DNS router voor resolving van intern gerichte DNS domeinen (JustitieNet). Tevens zorgt deze Interne DNS ook voor forwarding van DNS vragen richting Internet of Rijkweb. DNS ondersteunt ook reverse-loopup op niveau 1, 2 en 3[3].

De JuBIT publieke DNS fungeert als domein host/registrar en bevat de administratie van de DNS records die door internet systemen opgevraagd moeten kunnen worden.

De richtlijn voor naamconventie[4] voor domeinnamen van DNS-en voor Justitie en Veiligheid wordt gevolgd om complexe en foutgevoelige configuraties te voorkomen.

Nr	Aansluitvoorwaarden
7	De Deelnemer sluit de eigen DNS aan op DNS router in JuBIT3 voor resolving van eigen diensten voor andere deelnemers en de forwarding van alle interne DNS vragen.
8	De Deelnemer implementert tenminste SOA, NS, A, MX en PTR records op de eigen DNS[5].
9	Domeinnamen volgen de naamconventie.

4.1.5 NTP

JuBIT NTP heeft tot doel om Deelnemers te voorzien van een bron voor nauwkeurige tijdsynchronisatie. Om logging van verschillende systemen goed te kunnen vergelijken, is het belangrijk dat systemen van de Deelnemers en van Opdrachtnemer gebruik maken van de NTP in JuBIT3.

Nr	Aansluitvoorwaarden
10	De Deelnemer gebruikt de JuBIT NTP voor de tijdsynchronisatie van de eigen systemen gehost in JuBIT3.

3 Zie paragraaf 3.3 van Conventies voor Naamgeving en ICT gerelateerde adressering
4 Zie hoofdstuk 3 van Conventies voor Naamgeving en ICT gerelateerde adressering
5 https://www.cloudflare.com/learning/dns/dns-records/

4.1.6 JenV Trusted cloud

De JenV Trusted cloud is een bijzondere vorm van de publieke cloud en zorgt ervoor dat de onafhankelijkheid, zelfbeschikking en beveiliging van JenV met inzet van de publieke clouddiensten kan worden vormgegeven. De implementatie van een JenV Trusted cloud bestaat uit de inzet van eigen security controls in de publieke cloud op zowel het gebied van netwerkbeveiliging, identiteitscontrole en data-encryptie. JenV Trusted cloud kent eigen aansluitvoorwaarden en inzetregels. Deze vallen buiten de scope van dit document.
Toegang tot de JenV Trusted Cloud is alleen mogelijk langs een dedicated ontsluiting in JuBIT3[6].
Onderdeel van de ontsluiting is inspectie van het verkeer van en naar de JenV trusted cloud wanneer er sprake is van zone overgangen, zie ook 4.3 Zonering.

Nr	Aansluitvoorwaarden
11	JenV Trusted Cloud is alleen te benaderen langs de dedicated ontsluiting in JuBIT3.

4.2 Security policies / Configuratie

Het beheer van security policies (o.a firewall regels, Spam filters, anti-phishing) kan naar verloop van tijd een uitdagende klus worden, zeker wanneer onduidelijk is waarom policies in het verleden zijn geactiveerd. Het verwijderen van oude en niet langer gebruikte policies is wat doorgaans niet of onvoldoende gebeurt. Verouderde en onbeheerde policies vormen een risico omdat deze door kwaadwillenden misbruikt kunnen worden. Conform de BIO zijn lijnmanagers verantwoordelijk voor beveiliging van informatie systemen. Security policies moeten herleidbaar zijn naar toepassing/applicatie. Toepassingen/applicaties zijn herleidbaar naar business eigenaren.

Nr	Aansluitvoorwaarden
12	Voor elk informatiesysteem in JuBIT3 is de verantwoordelijke lijnmanager bekend.
13	Alle instellingen en security policies voor het betreffende informatiesysteem zijn herleidbaar naar de eigenaar (=lijnmanager).

4.3 Zonering

Communicatie tussen verschillende veiligheidszones, al dan niet van verschillend niveau, verloopt via het beveiligd koppelvlak 'JuBIT'[7]. Binnen JuBIT zijn passende maatregelen beschikbaar voor de overgang tussen Onvertrouwd, Vertrouwd en Semi-vertrouwd.

De JuBIT3 omgeving in haar geheel wordt als 'Vertrouwd' beschouwd, met daar binnen de JuBIT3 hosting zones TL1, AL1 en TL2 waarmee informatie op een veilige manier ontsloten wordt.
TL1 is voor toegang vanaf publieke systemen (inclusief externe systemen in de onvertrouwde zone.
AL1 voor toegang vanaf Semi-Vertrouwde partners & overheden of eigen veiligheidszones, terwijl TL2 voor ondersteuning dient van de omgevingen binnen trustlevels TL1 en AL1. Zie “Zonerings Architectuur JustitieNet v1.1. d.d. 22 Maart 2018” voor verdere informatie over zonering.

Nr	Aansluitvoorwaarden
14	Communicatie tussen verschillende veiligheidszones, al dan niet van verschillend niveau, verloopt via het beveiligd koppelvlak JuBIT.

6 Zie Cloud uitgangspunten JenV, hoofdstuk 3 d.d. 19 september 2019
7 Zie Zonerings Architectuur JustitieNet, parageaaf 3.4

5 Inzetregels

Inzetregels geven aan hoe Deelnemers JuBIT3 diensten kunnen gebruiken, waarbij niet alles wat (technisch) mogelijk is vanuit oogpunt van veiligheid en/of stabiliteit wordt toegestaan. Onderstaande tabel geeft een overzicht van alle Inzetregels, de achterliggende paragrafen geven een toelichting daarop.

Nr	Voorwaarde	Paragraaf
1	Objecten binnen JuBIT kennen een eigenaar (=lijnmanager).	5.1
2	Gebruikte hardware, operating systemen en soft/firmware binnen JuBIT is gedekt door een actueel support contract met de leverancier.	5.2
3	Elke host binnen JuBIT3 (hosting of housing) is voorzien van een Tanium agent en is aangesloten op de Centrale Tanium Omgeving.	5.3
4	Hosts zonder Tanium agent worden in in quarantaine geplaatst.	5.3
5	Hosts in quarantaine zonder eigenaar, worden opgeruimd.	5.3
6	Afwijkingen van de JenV baseline worden door de Deelnemer opgelost volgens de KPI's Baseline Configuratie Management	5.3.1
7	Systemen zijn gehard volgens de relevante CIS baseline.	5.3.1
8	Kwetsbare plekken worden door de Deelnemer opgelost volgens de KPI's Vulnerability Management	5.3.2
9	Systemen met Soft- en firmware die niet (langer) voldoet aan de inzetregel voor kwetsbare plekken, worden in quarantaine geplaatst.	5.3.2
10	Bij migratie is Lift-and-shift van VM en storage toegestaan wanneer aan alle Inzetregels is voldaan.	5.4

5.1 Eigenaarschap en herleidbaarheid

Conform de BIO zijn lijnmanagers verantwoordelijk voor beveiliging van informatie systemen. Alle objecten, waaronder systemen die door een Deelnemers in JuBIT3 wordt geplaatst (hosting of housing) en daar gekoppelde (aangepaste) Security policies zijn herleidbaar zijn naar toepassing/applicatie. Elke toepassing/applicatie is herleidbaar naar business eigenaren (=lijnmanager).

Nr	Inzetregels
1	Objecten binnen JuBIT kennen een eigenaar (=lijnmanager).

5.2 Support van hard-, software, firmware en besturingssystemen

Alle componten (hardwarde, software, firmware, besturingssytemen, databases, etc.) moeten door de desbetreffende leverancier gesupport worden, zodat eventuele (security) issues tijdig opgelost kunnen worden. Systemen zonder geldig supportcontract worden binnen JuBIT3 in quarantaine geplaatst. Eventuele hieruit voortvloeiende kosten komen voor rekening van de eigenaar.

De tabel op de volgende pagina is niet uitputtend en beschrijft van veel voorkomende besturingsystemen welke versies ingezet kunnen worden in JuBIT. Oudere versies worden niet ondersteund.

Besturingsysteem	Full-support eind datum	Extended-support eind datum	Ondersteund in JuBIT3 Hosting & Colo	Ondersteund in JuBIT3 Hosting + TAB
Windows server 2008	13-01-2015	14-01-2020	Nee	Nee
Windows Server 2012	09-10-2018	10-10-2023	Ja	Ja
Windows Server 2016	11-01-2022	12-01-2027	Ja	Ja
Windows Server 2022	3-10-2026	14-10-2031	Ja	Ja
Windows Server 2019	9-1-2024	9-1-2029	Ja	Ja
Oracle Linux 8	1-7-2029	TBA	Ja	Ja
Oracle Linux 7	1-7-2024	TBA	Ja	Ja
Redhat Enterprise Linux 8	31-5-2024	31-5-2031	Ja	Ja
Redhat Enterprise Linux 7	6-8-2019	30-6-2026	Ja	Ja

Nr	Inzetregels
2	Gebruikte hardware, operating systemen en soft/firmware binnen JuBIT is gedekt door een actueel support contract met de leverancier.

5.3 Tanium Agent

Elke host (VM of hardware) is minimaal voorzien van een Tanium agent. Deze agent is gekoppeld aan een Zone server van de centrale JenV Tanium dienst. De agent op de host wordt ingezet voor Asset management, Vulnerability management, Baseline configuratie managment en Threat hunting (zie Dienstenbeschrijving SOC JenV, hoofdstuk 4, 5 en 6). Informatie uit de verschillende diensten is inzichtelijk in Tanium voor geautoriseerde medewerkers van de Deelnemer en SOC JenV.

Nieuwe hosts worden bij de start voorzien van een Tanium agent. Een host zonder een Tanium agent wordt behandeld als een onbeheerde/onbekende host en in quarantaine geplaatst en daarmee effectief buiten gebruik gesteld. Wanneer een eigenaar bekend is, wordt de quarantaine opgeheven ná installatie van een Tanium agent. Wanneer geen eigenaar gevonden of bekend is (Zie Eigenaarschap en herleidbaarheid), dan wordt de host opgeruimd.

Nr	Inzetregels
3	Elke host binnen JuBIT3 (hosting of housing) is voorzien van een Tanium agent en is aangesloten op de Centrale Tanium Omgeving.
4	Hosts zonder Tanium agent worden in in quarantaine geplaatst.
5	Hosts in quarantaine zonder eigenaar worden opgeruimd.

5.3.1 Hardening van soft- en firmware

Hardening van Soft- en firmware is gericht op het voorkomen van onvoldoende veilige configuratie van soft- en firmware. Hardening gebeurt zo veel mogelijk op basis van de relevante standaarden van CIS (zie Dienstenbeschrijving SOC JenV, hoofdstuk 6). Soft- en firmware in JuBIT3 is geconfigureerd volgens CIS baseline[8] en wordt periodiek gecontroleerd met Tanium.

8 Voorstel voor CIS baseline is in de maak als onderdeel van PvA IB2.0.

Geconstateerde afwijkingen worden door de Deelnemer opgelost volgens de KPI's Baseline Configuratie Management, zie Dienstenbeschrijving SOC JenV, paragraaf 6.3). Soft- en firmware met één of meer onvoldoende veilige configuraties die niet volgens de KPI's opgelost zijn, worden in quarantaine geplaatst. Extra kosten zijn voor rekening van de Deelnemer. Wanneer de Deelnemer geconstateerde onvoldoende veilige configuraties heeft gecorrigeerd, wordt de quarantaine opgeheven.

Nr	Inzetregels
6	Afwijkingen van de JenV baseline worden door de Deelnemer opgelost volgens de KPI's Baseline Configuratie Management
7	Systemen zijn gehard volgens de relevante CIS baseline.

5.3.2 Kwetsbare plekken

Kwetsbare plekken in soft- en firmware vormen afhankelijk van de ernst[9] een bedreiging voor de beveiliging van MinJenV. SOC JenV controleert periodiek alle gebruikte soft- en firmware op kwetsbare plekken met Tanium.

Geconstateerde afwijkingen worden door de Deelnemer opgelost volgens de KPI's Vulnerability Management (Zie dienstenbeschrijving SOC JenV, paragraaf 6.4). Soft- en firmware met kwetsbaarheden die niet volgens de KPI's opgelost zijn, worden in quarantine geplaatst. Extra kosten zijn voor rekening van de Deelnemer.

Nr	Inzetregels
8	Kwetsbare plekken worden door de Deelnemer opgelost volgens de KPI's Vulnerability Management
9	Systemen met Soft- en firmware die niet (langer) voldoet aan de inzetregel voor kwetsbare plekken, worden in quarantaine geplaatst.

5.4 Migratie

Tijdens de migratie van JuBIT2 naar JUBIT3 is het lift-and-shift principe voor bestaande VM's en storage toegestaan mits aan alle JuBIT3 inzetregels is voldaan.

Nr	Inzetregels
10	Bij migratie is Lift-and-shift van VM en storage toegestaan wanneer aan alle Inzetregels is voldaan.

9 https://www.ncsc.nl/documenten/publicaties/2019/juli/02/inschalingsmatrix