NOTITIE

Aan	:	Betrokkenen bij de testaanpak DigiD –assessments
Datum	:	12 juni 2018
Van		NOREA Werkgroep DigiD assessments
Status	:	Definitief
Betreft	:	Update 2018 Handreiking bij DigiD–assessments 2.0, onderdeel testaanpak

---

Toelichting

Deze update betreft alleen de testaanpak bij het normenkader voor het DigiD assessment 2018. De update van overige teksten en bijlagen volgt later. Het normenkader voor het DigiD assessment, zoals gepubliceerd op de Logius web site onder 'Norm ICT-beveiligingsassessments DigiD, Versie 2.0. Datum 16 december 2016. Status Definitief.' blijft ongewijzigd.

De update is besproken in de NOREA werkgroep DigiD assessments van 23 mei 2018 en afgestemd met Logius. De testaanpak is de verantwoordelijkheid van de NOREA.

Naast een beperkt aantal tekstuele verbeteringen en verduidelijkingen zijn de belangrijkste wijzigingen:

- Betrokken partij(en) wordt Betrokken rol(len). De verschillende rollen kunnen ook bij één partij (bijvoorbeeld de houderorganisatie) uitgevoerd worden.
- U/TV.01: Toevoegen autorisatie proces (verschuift van U/WA.02 naar U/TV.01).

- U/WA.02: Toevoegen security incident afhandeling. Dit is een herstelactie. Per abuis is dit proces weggevallen in de eerste versie van DigiD 2.0. Het autorisatieproces is verplaatst naar U/TV.01.
- U/WA.05: Toevoegen dat TLS veilige en minder veilige instellingen kent . Het NCSC maakt onderscheid in ‘Goede’, ‘Voldoende’ en ‘Onvoldoende’ instellingen. Voor de DigiD webserver geldt dat minimaal de op dat moment als ‘Voldoende’ bestempelde instellingen vereist zijn.
- U/NW.04: Verplicht stellen dat het IDS/IPS geplaatst wordt na decryptie van het oorspronkelijk versleuteld netwerkverkeer. Dit is een verzwaring van de beveiligingseis die overeenkomt met wat in de markt nu gebruikelijk is.
- U/NW.06: Hardening netwerk: Deze norm wordt ook getoetst bij de houder van de DigiD aansluiting, in verband met het verplicht gebruik van DNSSEC.

Wij komen nog met een separaat voorstel om voor een aantal normen met ingang van 2019 tevens de werking over een periode van een heel jaar te testen. Vooralsnog denken wij in ieder geval aan: U/WA.02 Afhandeling security incidenten, C.08 Doorvoeren wijzigingen en testen, C.07 monitoring van loggingsinformatie IDS/IPS en C.09 Doorvoeren patches.

Bijlage 2. Guidance bij de te onderzoeken normen

Tabel beveiligingsrichtlijnen met aandachtspunten (Richtlijnen uit: ICT-Beveiligingsrichtlijnen voor Webapplicaties. Versie VERDIEPING. Nationaal Cyber Security Centrum. September 2015)

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
B.05	In een contract met een derde partij voor de uitbestede levering of beheer van een webapplicatie (als dienst) zijn de beveiligingseisen en -wensen vastgelegd en op het juiste (organisatorische) niveau vastgesteld. Doelstelling: Het handhaven van het beveiligingsniveau, wanneer de verantwoordelijkheid voor de ontwikkeling en/of het beheer van de webapplicatie is uitbesteed aan een andere organisatie.	Governance	Betrokken rol(len): • Applicatie-, hosting- of SAAS leverancier. • Houder van de DigiD-aansluiting. Scope: • De contracten en/of Service Level Agreements voor de levering hosting-, applicatie- of SAAS diensten. Nadere toelichting: De organisatie dient een, door beide partijen ondertekend, contract te hebben waarin tenminste de volgende zaken zijn opgenomen: • een beschrijving van de te leveren diensten die onder het contract vallen; • de van toepassing zijnde leveringsvoorwaarden; • informatiebeveiligingseisen met de relevante eisen vanuit het beveiligingsbeleid; • het melden van beveiligingsincidenten; • de behandeling van gevoelige gegevens; • wanneer en hoe de leverancier toegang tot de systemen / data van de gebruikersorganisatie mag hebben; • Service Level Reporting; • het jaarlijks uitvoeren van audits bij de leverancier(s); • beding dat deze voorwaarden back-to-back worden doorgegeven aan mogelijke sub-leveranciers. Test aanpak: • Interview de verantwoordelijke functionarissen. • Inspectie van het beveiligingsbeleid. • Inspectie van contracten met leveranciers, SLA's en andere gerelateerde documenten.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
U/TV.01	De inzet van identiteit- en toegangsmiddelen levert betrouwbare en effectieve mechanismen voor het vastleggen en vaststellen van de identiteit van gebruikers, het toekennen van de rechten aan gebruikers, het controleerbaar maken van het gebruik van deze middelen en het automatiseren van arbeidsintensieve taken.[1] Doelstelling: Het efficiënter maken van het identiteit- en toegangsbeheer en zorgen dat functies en gegevens uitsluitend beschikbaar worden gesteld aan diegenen waarvoor deze bedoeld zijn als waarborg voor vertrouwelijkheid en integriteit.	Applicatie Infrastructuur Proces	Betrokken rol(len): • Applicatie-, hosting- of SAAS leverancier. • Houder van de DigiD-aansluiting. Scope: • De DigiD webapplicatie, DigiD webservers en de firewalls, IDS/IPS, etc. Nadere toelichting: De focus ligt op de beheerprocessen. Dit betreft enerzijds toegang tot de DigiD-applicatie en anderzijds toegang tot de DigiD webservers en de firewalls, IDS/IPS, etc. die een koppeling hebben met de DigiD omgeving. Aandachtspunten hierbij zijn: • Toekennen, controleren en intrekken van autorisaties • Eisen aan wachtwoordinstellingen. • Aantoonbare controle op joiners/movers/leavers. • Wijzigen van de standaard wachtwoorden van administrator accounts. • Beperken eventuele shared accounts. • Uitvoeren periodieke reviews. Specifieke aandacht gaat uit naar wachtwoorden die leveranciers hebben om toegang tot de systemen of data van de houder van de DigiD aansluiting te krijgen (wie hebben die wachtwoorden, hoe worden die opgeslagen en wie hebben toegang. Hoe vaak worden ze gewijzigd, etc.). Test aanpak: • Interview de verantwoordelijke functionarissen. • Inspecteer het beveiligingsbeleid, joiners/movers/leavers procedure, de autorisatieprocedure, afspraken met leveranciers met betrekking tot toegang tot systemen en data en andere gerelateerde documenten. • Stel voor elk van deze processen en systemen, het bestaan vast met een deelwaarneming van tenminste één. • de toegekende autorisaties en de resultaten en opvolging van de periodieke review.

[1] In het document ICT-Beveiligingsrichtlijnen versie RICHTLIJNEN van september 2015 van het NCSC staat een afwijkende omschrijving. Deze is onjuist.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
U/WA.02	Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten. Doelstelling: Effectief en veilig realiseren van de dienstverlening.	Applicatie Proces	Betrokken rol(len): • Applicatie of SAAS leverancier. • Houder van de DigiD-aansluiting. Scope: • De DigiD webapplicatie. Nadere toelichting: Deze norm richt zich meer op de procesmatige aspecten van het functioneel en het applicatiebeheer. Aandachtspunten hierbij zijn: • Beschrijving van taken, verantwoordelijkheden en bevoegdheden van de verschillende beheerrollen. • Een incidentenprocedure is opgesteld. • Meldingen van het NCSC of IBD of Z-CERT of andere CERTS worden geanalyseerd en zo nodig opgevolgd. • Incidenten worden geregistreerd, geanalyseerd, opgevolgd en afgehandeld. • Er is een periodieke rapportage aan het management inzake beveiligingsincidenten. Test aanpak: • Interview de verantwoordelijke functionarissen. • Inspecteer de functie/taakbeschrijvingen van beheerders. • Inspecteer het incidentproces, de uitgevoerde analyse, de managementrapportage en opvolging van beveiligingsincidenten.
U/WA.03	De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt. Doelstelling: Voorkom (on)opzettelijke manipulatie van de webapplicatie, waardoor de vertrouwelijkheid, integriteit en/of beschikbaarheid van de webapplicatie aangetast worden.	Applicatie	Betrokken rol(len): • Applicatie- of SAAS leverancier. Scope: • De DigiD webapplicatie en webserver. Nadere toelichting: Ongecontroleerde (ongevalideerde) invoer van gebruikers is een belangrijke dreiging voor een webapplicatie. Als invoer van gebruikers rechtstreeks wordt gebruikt in HTML-uitvoer, cookie-waarden, SQL-queries, etc., bestaat er een (grote) kans dat een kwaadwillende de webapplicatie compromitteert. Een gebrek aan invoervalidatie kan tot kwetsbaarheden zoals XSS, commando- en

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
			SQL-injectie leiden. • HTTP request voor alle invoermethodes zoals gespecificeerd in de ICT-Beveiligingsrichtlijnen van NCSC moeten worden gevalideerd (testen op type, lengte, formaat en karakters van invoer en speciale tekens (bv. <, >, ', ", & , /, --, etc.). Test aanpak: Om deze beveiligingsrichtlijn volledig te testen is een source code review nodig. Er is echter niet gekozen voor een verplichte code review als onderdeel van de DigiD assessment. Deze wordt wel aanbevolen. • Observeer het gedrag van de webapplicatie op ongeldige invoer. Voer hierbij een representatieve deelwaarneming uit op de invoermogelijkheden die de applicatie biedt.
U/WA.04	De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren. Doelstelling: Voorkom manipulatie van het systeem van andere gebruikers	Applicatie	Betrokken rol(len): • Applicatie- of SAAS leverancier. Scope: • De DigiD webapplicatie. Nadere toelichting: Als een webapplicatie onvoldoende controles uitvoert op de uitvoer die het terugstuurt naar de gebruiker, kan het gebeuren dat er zich onbedoelde of ongewenste inhoud in de uitvoer bevindt. Uitvoervalidatie voorkomt dat de webapplicatie ongewenste opdrachten geeft aan de client, bijvoorbeeld in het geval van XSS. • De webapplicatie codeert dynamische onderdelen in de uitvoer waarbij mogelijke gevaarlijke tekens (bv. <, >, ', ", & , /, --, etc.) worden genormaliseerd. Test aanpak: Om deze beveiligingsrichtlijn volledig te testen is een source code review nodig. Er is echter niet gekozen voor een verplichte code review als onderdeel van de DigiD assessment. Deze wordt wel aanbevolen. • Observeer het gedrag van de webapplicatie op voor wat betreft onveilige uitvoer. Voer hierbij een representatieve deelwaarneming uit op de uitvoervelden van de applicatie.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
U/WA.05	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken. <u>Doelstelling:</u> Gegevens in opslag en transport beschermen tegen ongeautoriseerde kennisname en manipulatie	Applicatie Infrastructuur Proces	<u>Betrokken rol(len):</u> • Applicatie-, hosting- of SAAS leverancier. • Houder van de DigiD-aansluiting. <u>Scope:</u> • De DigiD webapplicatie en webserver en bijbehorende infrastructuur. <u>Nadere toelichting</u> Deze norm raakt diverse aspecten van privacybevorderende en cryptografische technieken. Dit betreft de classificatie van gegevens, de encryptie van gevoelige gegevens tijdens de opslag en de encryptie van gegevens tijdens transport. Aandachtspunten hierbij zijn: • de classificatie van gegevens door de houder van de DigiD aansluiting op basis van een risico analyse; • mogelijke versleuteling of hashing van gevoelige gegevens. Het gaat hier in ieder geval om het BSN als bijzonder persoonsgegeven. Overigens geldt dit alleen voor gegevens die in dezelfde DMZ worden opgeslagen als waar de webapplicatie draait. Gegevens in de backoffice vallen buiten de scope van dit onderzoek; • de HTTPS configuratie en de TLS configuratie. TLS kent veilige en minder veilige instellingen. Het NCSC maakt onderscheid in 'Goede', 'Voldoende' en 'Onvoldoende' instellingen[2]. Voor de DigiD webserver geldt dat minimaal de op dat moment als 'Voldoende' bestempelde instellingen vereist zijn. <u>Test aanpak</u>: • Interview de verantwoordelijke functionarissen. • Inspecteer de classificatie van gegevens en daaraan gerelateerde risico analyse, de netwerkarchitectuur en het inrichtingsdocument waar de encryptie van gegevens in staat beschreven. • Observeer de encryptie van gegevens. Inspecteer de HTTPS en TLS configuraties.
U/PW.02	De webserver garandeert specifieke kenmerken van de inhoud van de protocollen.	Applicatie	<u>Betrokken rol(len):</u> • Applicatie-, hosting- of SAAS leverancier.

[2] Een overzicht van de TLS-configuraties is te vinden op https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls.html

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
	Doelstelling: Voorkom inzage, wijziging of verlies van gegevens door manipulatie van de logica van de webserver of webapplicatie.		Scope: • De webserver. Nadere toelichting: HTTP headers moeten de risico's beperken van inzage, wijziging of verlies van gegevens door manipulatie van de logica van de webserver of webapplicatie. Aandachtspunten hierbij zijn: • behandel alleen HTTP-requests waarvan de gegevens een correct type, lengte, formaat, tekens en patronen hebben; • behandel alleen HTTP-requests van initiators met een correcte authenticatie en autorisatie; • sta alleen de voor de ondersteunde webapplicaties benodigde HTTP-requestmethoden (GET, POST, etc.) toe en blokkeer de overige niet noodzakelijke HTTP-requestmethoden; • verstuur alleen HTTP-headers die voor het functioneren van HTTP van belang zijn; • toon in HTTP-headers alleen de hoogst noodzakelijke informatie die voor het functioneren van belang is; • bij het optreden van een fout wordt de informatie in een HTTP-response tot een minimum beperkt. Een eventuele foutmelding zegt wel dat er iets is fout gegaan, maar niet hoe het is fout gegaan. Test aanpak: • Observeer het gedrag van de HTTP headers en responses. Voer hierbij een representatieve deelwaarneming uit op de invoer- en uitvoermogelijkheden die de applicatie biedt.
U/PW.03	De webserver is ingericht volgens een configuratie-baseline. Doelstelling: Ongewenste vrijgave van informatie tot een minimum beperken, met name waar het gaat om informatie die inzicht geeft in de opbouw van de beveiliging.	Applicatie Infrastructuur	Betrokken rol(len): • Applicatie-, hosting- of SAAS leverancier. Scope: • De webserver. Nadere toelichting Deze norm richt zich enerzijds op de aanwezigheid van een configuratie-baseline voor de webserver en op de feitelijke configuratie van de webserver. Aandachtspunten hierbij zijn: • directory listings worden niet ondersteund;

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
			• cookie flags staan op 'HttpOnly' en 'Secure'; • bij alle HTTP-responses worden zowel de HTTP-headers 'Content-Security-Policy: frame-ancestors' als de 'X-Frame-Options' verstuurd. Test aanpak: • Interview de verantwoordelijke functionarissen. • Inspecteer de configuratie-baseline van de webserver. • Observeer de mogelijk tot het maken van directory listings, de cookies flags en de HTTP response headers 'Content-Security-Policy: frame-ancestors' en 'X-Frame-Options'.

U/PW.05	Het beheer van platformen maakt gebruik van veilige (communicatie)protocollen voor het ontsluiten van beheermechanismen en wordt uitgevoerd conform het operationeel beleid voor platformen.
	
	Doelstelling:
	Voorkomen van misbruik van beheervoorzieningen.
		Infrastructuur
		Proces
			Betrokken rol(len):
			• Hosting- of SAAS leverancier.
			
			Scope:
			• De webserver en andere servers in de DMZ.
			
			Nadere toelichting:
			• Dit betreft het gebruik van veilige netwerkprotocollen. Indien beheerinterfaces via het internet te benaderen zijn moet dit door middel van twee factor authenticatie, zoals de combinatie van een wachtwoord en source IP filtering, in combinatie met een veilig (communicatie) protocol worden afgehandeld. Er mag geen gebruik worden gemaakt van backdoors om de systemen te benaderen (ook niet voor noodtoegang). Daarnaast wordt een beknopt operationeel beleid verwacht.
			• Aandachtspunten voor deze norm zijn:
			  ○ Het gebruik van veilige protocollen (conform industrie standaarden) voor het benaderen van beheermechanismen (beheerinterfaces).
			  ○ Het gebruik van sterke authenticatie voor zowel technisch als functioneel beheerders.
			
			Test aanpak:
			• Interview de verantwoordelijke functionarissen.
			• Inspecteer het operationele beleid met betrekking tot het gebruik van beheervoorzieningen en de daarbij vereiste authenticatie.
			• Observeer de protocollen die kunnen worden gebruikt voor het benaderen van beheerinterfaces en de authenticatiemethoden die daarbij worden afgedwongen, Inspecteer de configuratie ten aanzien van de wachtwoordvereisten van de

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
			webserver en voor een deelwaarneming van minimaal één van de andere servers in de DMZ.
U/PW.07	Voor het configureren van platformen is een hardeningsrichtlijn beschikbaar. <u>Doelstellingen:</u> Beperken van de functionaliteit tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.	Infrastructuur Proces	<u>Betrokken rol(len):</u> • Hosting- of SAAS leverancier. <u>Scope:</u> De webserver en andere ICT componenten binnen de DMZ. <u>Nadere toelichting</u>: Voor het configureren van platformen is een hardeningsrichtlijn beschikbaar. Hierbij kan worden verwezen naar actuele hardenings-richtlijnen van de leverancier(s)/SANS/NIST/CIS met een vermelding van "pas toe of leg uit". Hierbij spelen de geïdentificeerde risico's in de "pas toe of leg uit" afweging een bepalende rol. Het gaat echter niet alleen om de hardeningsrichtlijn zelf, maar ook om het concreet toepassen ervan. De hardening van de DigiD webomgeving dient stringent te zijn geregeld: alles wat open staat moet een reden hebben en alles wat open staat moet secure worden aangeboden. De hardening van interne systemen mag minder stringent. Wel moeten de beheer functies secure zijn en mogen er geen onveilige protocollen worden gebruikt, moeten standaard wachtwoorden zijn gewijzigd. Voorbeeld applicaties moeten zijn verwijderd als deze niet daadwerkelijk worden gebruikt. Aandachtspunten hierbij zijn: • Inrichting van ICT-componenten (aantoonbaar) volgens de instructies en procedures van de leverancier. • Bijhouden van een actueel overzicht bij van de noodzakelijke protocollen, services en accounts voor de op het platform geïnstalleerde applicaties. • Deactiveren of verwijderen van alle protocollen, services en accounts op het platform als die niet volgens het ontwerp noodzakelijk zijn. • Periodiek toetsen of de in productie zijnde ICT-componenten niet meer dan de vanuit het ontwerp noodzakelijke functies bieden (statusopname). Afwijkingen worden hersteld. <u>Test aanpak</u>: • Interview de verantwoordelijke functionarissen. • Inspecteer de architectuur en hardeningsstandaarden. • Inspecteer de configuratiebestanden en de uitkomsten van de penetratietest.
U/NW.03	Het netwerk is gescheiden in fysieke en logische domeinen (zones), in het bijzonder is er een DMZ die tussen het	Infrastructuur	<u>Betrokken rol(len):</u> • Hosting- of SAAS leverancier.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
	interne netwerk en het internet gepositioneerd is. Doelstelling: Een beveiligde (of robuuste) netwerkinfrastructuur bieden voor de bedrijfstoepassingen.		Scope: • De DMZ van de DigiD webapplicatie. Nadere toelichting: DMZ en compartimentering d.m.v. (2 virtuele) firewalls. Deze eis zowel materieel (feitelijk bestaan en inrichting van DMZ) als formeel qua opzet (netwerkschema of tekening) beoordelen, eventueel op basis van een adequate beschrijving. Overigens zal de organisatie moeten aantonen dat zij voldoende inzicht heeft in de architectuur, zowel van de DMZ als van de systemen die zich daarin bevinden. Test aanpak: • Interview de verantwoordelijke functionarissen. • Inspecteer het netwerkarchitectuur schema inclusief de toegestane verkeersstromen tussen netwerksegmenten. • Inspectie van configuratie files, firewall regels en de uitkomsten van de penetratietest.
U/NW.04	De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van detectie- en protectiemechanismen. Doelstelling: Het detecteren van aanvallen (onder andere (D)DoS) om te voorkomen dat de vertrouwelijkheid, integriteit en/of beschikbaarheid van geleverde services negatief wordt beïnvloed.	Infrastructuur	Betrokken rol(len): • Hosting- of SAAS leverancier. Scope: • De DMZ van de DigiD webapplicatie. Nadere toelichting Beveiligingsrichtlijnen NW.04, C.06 en C.07 hangen nauw met elkaar samen: - NW.04 richt zich op de implementatie en het gebruik van IDS/IPS - C.06 richt zich op het tijdig signaleren van aanvallen - C.07 richt zich op periodieke analyse van de logging. Inkomend en uitgaand verkeer moet worden gemonitord om mogelijke aanvallen tijdig te detecteren en hier acties op te kunnen ondernemen. Hiervoor zal de organisatie een Intrusion Detection Systeem (IDS) moeten implementeren. Aanbevolen wordt om tevens gebruik te maken van een Intrusion Prevention Systeem (IPS) dat automatisch preventieve maatregelen neemt tegen bedreigingen of een gecombineerde IDS/IPS. Het IDS of IPS dient geplaatst te worden **na** decryptie van het oorspronkelijk versleuteld netwerkverkeer omdat anders de inhoud van de berichten niet afdoende kan worden beoordeeld door het systeem.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
			Aandachtpunten hierbij zijn: • Het gebruik van een IDS of IPS waarmee netwerkverkeer naar / van de DMZ van de DigiD webapplicatie wordt gemonitord. • Een inrichtingsdocument en een beheerprocedure waarin is vastgelegd waar en hoe de IDS / IPS ingezet. • Het gebruik van een adequate ruleset (b.v. Snort, Suricata, ETPro, etc.) die periodiek (= minimaal wekelijks) wordt geactualiseerd. Test aanpak: • Interview de verantwoordelijke functionarissen. • Inspecteer het netwerkarchitectuur schema, de inrichtingsdocumentatie en de beheerprocedure van de IDS/IPS. • Inspecteer de configuratiefiles van het IDS/IPS en de signature datum van de regel-set.
U/NW.05	Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd. Doelstelling: Het voorkomen van misbruik van de beheervoorzieningen vanaf het internet.	Infrastructuur Proces	Betrokken rol(len): • Hosting- of SAAS leverancier. Scope: • Het netwerksegment met de webservers die een koppeling hebben met de DigiD omgeving van Logius inclusief de toegang vanuit internet. Nadere toelichting: Door middel van fysieke scheiding, veilige VPN verbindingen (zoals IPSec) of VLANs is het beheer- en productieverkeer van elkaar gescheiden. Deze beveiligingsrichtlijn is nauw verbonden met U/PW.05 omdat de voor het beheer uitsluitend veilige netwerkprotocollen mogen worden gebruikt. • Er is een inrichtingsdocument waaruit blijkt op welke wijze content beheer (web- en database-content), applicatiebeheer en technisch beheer worden uitgeoefend. • Het gebruik van fysieke scheiding, veilige VPN verbindingen (zoals IPSec) of VLANs het beheer- en productieverkeer van elkaar gescheiden. Test aanpak: • Interview de verantwoordelijke functionarissen. • Inspecteer het netwerkarchitectuurschema inclusief de toegestane verkeersstromen tussen netwerksegmenten. • Inspecteer de configuratie files, firewall regels en de uitkomsten van de penetratietest.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
U/NW.06	Voor het configureren van netwerken is een hardeningrichtlijn beschikbaar. Doelstelling Beperken van het netwerkverkeer tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.	Infrastructuur Proces	Betrokken rol(len): • Hosting- of SAAS leverancier. • Houder van de DigiD-aansluiting. Scope: • De webserver en andere ICT componenten binnen de DMZ. Nadere toelichting: Voor het configureren van netwerkcomponenten is een hardeningrichtlijn beschikbaar. Hierbij kan worden verwezen naar actuele hardeningrichtlijnen van de leverancier(s)/SANS/NIST/CIS met een vermelding van "pas toe of leg uit". Hierbij spelen de geïdentificeerde risico's in de "pas toe of leg uit" afweging een bepalende rol. Het gaat echter niet alleen om de hardeningrichtlijn zelf, maar ook om het concreet toepassen ervan. De hardening van de DigiD omgeving dient stringent te zijn geregeld: alles wat open staat moet een reden hebben en alles wat open staat moet secure worden aangeboden. De hardening van interne systemen mag minder stringent. Wel moeten de beheer functies secure zijn en mogen er geen onveilige protocollen worden gebruikt, moeten standaard wachtwoorden zijn gewijzigd. Voorbeeld applicaties moeten zijn verwijderd als deze niet daadwerkelijk worden gebruikt. Door de vitale rol die het Domain Name System speelt in het bereikbaar houden van webapplicaties, verdient de beveiliging van DNS-services extra aandacht. Onder deze beveiligingsrichtlijn valt dan ook het *verplicht* gebruik van DNSSEC (DNS Security Extensions) voor de URL van het object van onderzoek. Met DNSSEC wordt de authenticiteit van DNS-antwoorden geverifieerd om misbruik te voorkomen. Aandachtspunten hierbij zijn: • Bijhouden van een actueel overzicht van de noodzakelijke netwerkprotocollen, -poorten en -services. • Uitschakel op de netwerkcomponenten alle netwerkprotocollen, -poorten en –services uit, behalve de noodzakelijke. • Aanpassen de (beveiligings)configuraties van netwerkprotocollen, -poorten en -services op de netwerkcomponenten aan conform richtlijnen. Test aanpak: • Interview de verantwoordelijke functionarissen. • Inspecteer de netwerkarchitectuur schema en hardeningrichtlijnen. • Inspecteer de configuratiebestanden en de uitkomsten van de penetratietest.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
C.03	Vulnerability assessments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie (scope). Doelstelling: Identificeren van de kwetsbaarheden en zwakheden in de ICT-componenten van de webapplicatie zodat tijdig de juiste beschermende maatregelen kunnen worden getroffen.	Infrastructuur Proces	Betrokken rol(len): • Hosting- of SAAS leverancier. Scope: • De infrastructuur voor het netwerksegment met de DigiD webapplicatie. Nadere toelichting: Deze netwerk based scan dient zich ten minste gericht te hebben op de hardening en patching van de infrastructuur en het detecteren van mogelijke kwetsbaarheden op de infrastructuur. • Vulnerability assessments vinden intern plaats minimaal een keer per jaar en vaker op basis van een risicoafweging zoals bijvoorbeeld bij wijziging van de configuratie van de DMZ. • De scope van het vulnerability assessment omvat tenminste de infrastructuur voor het netwerksegment met de DigiD webapplicatie. • Naar aanleiding van de resultaten van de vulnerability assessment is een actieplan opgesteld om de tekortkomingen op te heffen. • Er is voldoende voortgang geboekt in het opvolgen van bevindingen gezien de aard en complexiteit van de bevindingen. Test aanpak: • Interview de verantwoordelijke functionarissen. • Inspecteer het netwerkarchitectuur schema en de opdracht tot het uitvoeren van vulnerability assessment. • Inspecteer het vulnerability assessment rapport, het actieplan naar aanleiding van de vulnerability assessment en het statusrapport met betrekking tot de bevindingen.
C.04	Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope). Doelstelling: Het verkrijgen van inzicht in de weerstand die een webapplicatie kan bieden aan pogingen om het te compromitteren (binnendringen of	Applicatie Infrastructuur Proces	Betrokken rol(len): • Applicatie-, hosting- of SAAS leverancier. Scope: • De DigiD webapplicatie, de webserver en andere servers in de DMZ van de DigiD webapplicatie. Nadere toelichting: De voorkeur heeft het op basis van een risicoafweging enkele keren per jaar een penetratietest te laten uitvoeren, zodat ingespeeld kan worden op nieuwe bedreigingen.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
	misbruiken van webapplicatie).		• De penetratietest dient minimaal eenmaal per jaar te worden uitgevoerd en na significante wijzigingen, zoals vervanging applicatie, nieuwe versie, migratie webservers, database migratie, etc.. • De scope van de penetratietest omvat tenminste de webapplicatie en de infrastructuur voor het netwerksegment met de DigiD webapplicatie. • Naar aanleiding van de resultaten van de penetratietest is een actieplan opgesteld om de tekortkomingen op te heffen. • Er is voldoende voortgang geboekt in het opvolgen van bevindingen gezien de aard en complexiteit van de bevindingen. <u>Testaanpak:</u> • Interview de verantwoordelijke functionarissen. • Inspecteer het netwerkarchitectuur schema en de opdracht tot het uitvoeren van de penetratie test. • Inspecteer het penetratietest rapport, het actieplan naar aanleiding van de penetratietest en het statusrapport met betrekking tot de bevindingen.
C.06	In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht. <u>Doelstelling:</u> Het maakt mogelijk eventuele schendingen van functionele en beveiligingseisen te kunnen detecteren en achteraf de juistheid van de uitgevoerde acties, zowel op strategisch als operationeel niveau te kunnen vaststellen.	Infrastructuur Proces	<u>Betrokken rol(len):</u> • Hosting- of SAAS leverancier. <u>Scope:</u> • De infrastructuur voor het netwerksegment met de DigiD webapplicatie. <u>Nadere toelichting</u> Beveiligingsrichtlijnen NW.04, C.06 en C.07 hangen nauw met elkaar samen: - NW.04 richt zich op de implementatie en het gebruik van IDS/IPS - C.06 richt zich op het tijdig signaleren van aanvallen - C.07 richt zich op periodieke analyse van de logging. Hoewel deze richtlijn een brede reikwijdte heeft, is zij - in overleg met Logius – ingeperkt tot het detecteren van aanvallen met detectiesystemen in de webapplicatie-infrastructuur. Aandachtspunten zijn: • Het definiëren van alarm situaties en drempelwaarden. • Het configureren van de alarm situaties en drempelwaarden in het IDS/IPS en het genereren van de bijbehorende alerts. • De inbedding van alert afhandeling in het incidentenbeheerproces inclusief escalatieprocedure.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
			Test aanpak: • Interview de verantwoordelijke functionarissen. • Inspectie van de Use Cases en drempelwaarden. • Inspectie van alerts en de opvolging daarvan.
C.07	De loggings- en detectie-informatie (registraties en alarmeringen) en de condities van de beveiliging van ICT-systemen worden regelmatig gemonitord (bewaakt, geanalyseerd) en de bevindingen gerapporteerd. Doelstelling: Tijdig inzetten van correctieve maatregelen en informatie verschaffen over activiteiten van gebruikers en beheerders van de ICT-diensten en de status van de componenten waarmee deze worden voortgebracht.	Infrastructuur Proces	Betrokken rol(len): • Hosting- of SAAS leverancier. Scope: • De infrastructuur voor het netwerksegment met de DigiD webapplicatie. Nadere toelichting Beveiligingsrichtlijnen NW.04, C.06 en C.07 hangen nauw met elkaar samen: - NW.04 richt zich op de implementatie en het gebruik van IDS/IPS; - C.06 richt zich op het tijdig signaleren van aanvallen; - C.07 richt zich op periodieke analyse van de logging. De logging- en detectie-informatie en de conditie van de beveiliging van ICT-systemen worden regelmatig gemonitord (bewaakt, geanalyseerd) en de bevindingen gerapporteerd. Aandachtpunten hierbij zijn: • Procedurebeschrijving met daarin beschreven op welke wijze en wanneer controles op logging moeten plaatsvinden en hoe taken op dit gebied belegd zijn. • Het uitvoeren van periodieke controles op: - wijzigingen aan de configuratie van webapplicaties; - optreden van verdachte gebeurtenissen en eventuele schendingen van de beveiligingseisen; - ongeautoriseerde toegang tot en wijzigingen/verwijderen van logbestanden; - toegangslogs. • Periodieke analyse op ongebruikelijke situaties (incidenten) die de werking van webapplicaties kunnen beïnvloeden. • Periodiek rapportage van de geanalyseerde en beoordeelde gelogde gegevens aan de systeemeigenaren en/of aan het management. • Opvolging van bevindingen naar aanleiding van de analyse. Test aanpak: • Interview de verantwoordelijke functionarissen. • Inspectie van de procedurebeschrijving met betrekking tot de logging. • Inspectie van de vastlegging van de periodiek review van de logging, periodieke

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
			rapportage aan het management en follow-up acties naar aanleiding van review en analyse van de logging.
C.08	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd. <u>Doelstelling:</u> Zeker stellen dat wijzigingen op een correcte en gecontroleerde wijze worden doorgevoerd waardoor de veilige werking van ICT-voorziening wordt gegarandeerd.	Applicatie Infrastructuur Proces	<u>Betrokken rol(len):</u> • Applicatie-, hosting- of SAAS leverancier. • Houder van DigiD aansluiting. <u>Scope:</u> • De DigiD webapplicatie en de infrastructuur voor het netwerksegment met de DigiD webapplicatie. <u>Nadere toelichting:</u> De focus ligt op het vaststellen dat het proces wijzigingsbeheer zodanig is opgezet en geïmplementeerd dat alle wijzigingen altijd eerst worden getest voordat deze in productie worden genomen en via wijzigingsbeheer worden doorgevoerd. In sommige gevallen kunnen formulieren worden gebouwd die beveiligingsrisico's introduceren en valt wijzigingenbeheer met betrekking tot formulieren wel in scope van de DigiD-assessment. Is dit niet het geval dan valt wijzigingenbeheer met betrekking tot formulieren niet in scope. Welke specifieke situatie zich voordoet hangt af van de applicatie (formulierengenerator) en de wijze waarop deze wordt gebruikt. Het is aan de auditor om te bepalen of er aanleiding is om wijzigingenbeheer ten aanzien van de formulieren in de DigiD-scope op te nemen. Ingeval van SAAS-toepassingen ligt de verantwoordelijkheid voor het testen van wijzigingen aan de applicatie doorgaans bij de leverancier en/of gebruikersgroep. Aandachtspunten hierbij zijn: • Wijzigingsbeheer procedure, waarbij zo nodig onderscheid wordt gemaakt tussen wijzigingen op de applicatie, de servers en de netwerkcomponenten. • Het inrichten van een OTAP omgeving zodat wijzigingen eerst in een testomgeving worden getest voordat zij in productie kunnen worden genomen (n.b. voor netwerk wijzigingen is een testomgeving vaak niet mogelijk). • Het hanteren van een testscript en de vastlegging van de testresultaten. • Een formele acceptatie voor het in productie nemen van de wijziging. • Het beperken van het aantal personen die wijzigingen in productie kunnen nemen. • Bij het uitbrengen van een nieuwe release van de applicatie of een grote upgrade van het onderliggende platform moet, bij voorkeur door middel van een penetratietest, worden onderzocht of er geen nieuwe kwetsbaarheden zijn geïntroduceerd. <u>Test aanpak:</u> • Interview de verantwoordelijke functionarissen.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
			• Inspecteer de wijzigingsprocedure en de inrichting van de OTAP omgeving. • Inspecteer, voor elk type wijziging (applicatie, servers, netwerk), één wijziging en de daaraan gerelateerde documentatie.
C.09	Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT voorzieningen. Doelstelling: Zeker stellen dat technische en software kwetsbaarheden tijdig en effectief worden aangepakt en zo een stabiele omgeving wordt gecreëerd.	Applicatie Infrastructuur Proces	Betrokken rol(len): • Applicatie-,Hosting- of SAAS leverancier. Scope: • Hypervisor (VM Ware, etc.). • Operating system (Windows, etc.). • Databases. • Netwerk componenten. • Firewall. • Webapplicatie en daarvoor benodigde software componenten Nadere toelichting: De focus is op het patching proces. Dit proces kan gedifferentieerd zijn naar bijvoorbeeld het OS, DBMS en netwerk. Applicaties en systemen dienen periodiek gepatcht te worden. Een maandelijks patching cyclus is aanvaardbaar tenzij er security alerts zijn. Voor internet facing systemen dienen de laatste stabiele beveiligingspatches te zijn geïnstalleerd. Indien patching niet mogelijk is in verband met een legacy applicatie die niet meer zou functioneren na patching, zal dit risico aantoonbaar moeten zijn afgewogen. Aandachtpunten hierbij zijn: • Het beschrijven van patchmanagementbeleid waarin is aangegeven hoe de organisatie omgaat met updates: hoe snel implementeert de organisatie een kritieke patch en welke stadia moet de patch doorlopen. • Registratie van patches met vastlegging of de patches niet, wel of versneld worden doorgevoerd. • Het tijdig doorvoeren van patches. Test aanpak: • Interview de verantwoordelijke functionarissen. • Inspectie van het patchmanagementbeleid. • Inspectie van configuratie files en de uitkomsten van de penetratietest.