Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

ICT-Beveiligingsrichtlijnen voor Webapplicaties

RICHTLIJNEN

ICT-Beveiligingsrichtlijnen voor Webapplicaties

RICHTLIJNEN

INHOUDSOPGAVE

Inleiding

Aanleiding voor de Beveiligingsrichtlijnen

Digitale informatie-uitwisseling is een essentieel onderdeel geworden voor het functioneren van de Nederlandse samenleving. Betrouwbare digitale communicatie is van wezenlijk belang en vraagt om voortdurende zorg. Dat dit geen makkelijke opgave is blijkt wel uit het veelvoud van incidenten. De Beveiligingsrichtlijnen bieden een leidraad naar een veiliger dienstverlening.

Deze ICT-Beveiligingsrichtlijnen voor Webapplicaties (hierna Richtlijnen genoemd) bestaan uit twee documenten die na implementatie bijdragen aan een betere beveiliging van webapplicaties bij organisaties en de (rijks)overheid. Dit document (Richtlijnen) beschrijft de beveiligingsrichtlijnen voor webapplicaties op hoofdniveau, bijbehorend beleid, uitvoering en beheersing. Het document Verdieping vormt een ondersteunend document en beschrijft de beveiligingsrichtlijnen op detailniveau en geeft richting (handelingsperspectief) met betrekking tot de implementatie en controleerbaarheid van de beveiligingsrichtlijnen. Waar mogelijk worden concrete adviezen geven. Met de adviezen in het document Verdieping kan worden voldaan aan de beveiligingsrichtlijnen in dit document.

Webapplicaties

Wanneer dit document spreekt over een webapplicatie, dan gaat het om een applicatie die bereikbaar is met een webbrowser of een andere client, die ondersteuning biedt voor het Hypertext Transfer Protocol (http). Kern van deze definitie is dat een webapplicatie altijd bereikbaar is op basis van http of de met versleuteling beveiligde vorm hiervan: https (http secure). De functionaliteit die een webapplicatie kan bieden is onbeperkt. De techniek is echter altijd gebaseerd op de http-standaard zoals gedefinieerd in 'Request for Comments' (RFC) 1945[1], 2616[2], 2617[3], 2817[4], 6265[5], 6585[6] en 7540[7].

Ook bijbehorende infrastructuur, het koppelvlak met internet, de opslag van de gegevens en de netwerkservices worden in dit document beschouwd als aandachtsgebied. Voorbeelden van applicaties, die volgens deze definitie onder de noemer 'webapplicatie' vallen, zijn internetsites, extranetten, intranetten, software-as-a-service (SaaS)-applicaties, webservices en web-api's.

Doelgroep

Dit document heeft drie primaire doelgroepen:

» De eerste doelgroep bestaat uit partijen die verantwoordelijk zijn voor het stellen van beveiligingskaders en de controle op naleving hiervan. Hierbij kan worden gedacht aan securitymanagers en systeemeigenaren van de te leveren ICT-diensten.
» De tweede doelgroep bestaat uit diegenen die betrokken zijn bij het ontwerp- en ontwikkelproces, de implementatie en het beheer van webapplicaties. Deze doelgroep moet de beveiligingsrichtlijnen implementeren. Bij deze doelgroep zijn drie partijen te onderscheiden:
  › interne afdelingen.
  › externe leveranciers van software.
  › externe webhostingpartijen.
» De derde doelgroep bestaat uit de controlerende instanties (IT-auditors) die op basis van deze richtlijnen een objectieve ICT-beveiligingsassessment uitvoeren.

Doelstelling

Deze Richtlijnen geven een overzicht van beveiligingsmaatregelen die aanbieders van webapplicaties kunnen nemen om een bepaalde mate van veiligheid te bereiken. De beveiligingsmaatregelen hebben niet alleen betrekking op de webapplicatie, maar ook op de beheeromgeving en de omringende hard- en softwareomgeving die noodzakelijk is om de webapplicatie te laten functioneren.

Toepassing van de Richtlijnen

Organisaties kunnen (een deel van) deze Richtlijnen voor bepaalde toepassingsgebieden verheffen tot een normenkader. In tegenstelling tot de beveiligingsrichtlijnen, die adviserend van aard zijn, is een normenkader dwingend voor het toepassingsgebied. Ook kunnen de Richtlijnen worden gebruikt in aanbestedingen, het uitbesteden van dienstverlening en in onderlinge afspraken bij ketenprocessen. Afhankelijk van de aard en de specifieke kenmerken van de betreffende dienst kunnen beveiligingsrichtlijnen worden geselecteerd en kunnen de wegingsfactoren van de individuele beveiligingsrichtlijnen worden aangepast om de gewenste situatie te weerspiegelen.

Prioriteit

De prioriteit van elke beveiligingsrichtlijn wordt in algemene zin gewaardeerd volgens de classificatie Hoog, Midden of Laag. Deze

1 RFC 1945: Hypertext Transfer Protocol -- HTTP/1.0: http://www.ietf.org/rfc/rfc1945.txt
2 RFC 2616: Hypertext Transfer Protocol -- HTTP/1.1: http://www.ietf.org/rfc/rfc2616.txt
3 RFC 2617: HTTP Authentication (Basic and Digest): http://www.ietf.org/rfc/rfc2617.txt
4 RFC 2817: Upgrading to TLS Within HTTP/1.1: http://www.ietf.org/rfc/rfc2817.txt
5 RFC 6265: HTTP State Management Mechanism: http://www.ietf.org/rfc/rfc6265.txt
6 RFC 6585: Additional HTTP Status Codes: http://www.ietf.org/rfc/rfc6585.txt
7 RFC 7540: Hypertext Transfer Protocol Version 2 (HTTP/2): https://tools.ietf.org/html/rfc7540

drie classificaties vormen drie punten op een continuüm van mogelijke waarden waarbij Hoog de sterkste mate van gewenstheid is (must have), Midden een redelijk sterke mate van gewenstheid is (should have) en Laag een gewenste, maar niet noodzakelijke voorwaarde vormt (nice to have). De drie waarden zijn moeilijk exact te definiëren, maar vormen een functie van kans op optreden van een bedreiging en de mogelijke schade als gevolg hiervan.

De uiteindelijke afweging voor een specifieke webapplicatie voor een specifieke organisatie is afhankelijk van de weging van risico's die uit een risicoanalyse naar voren komen. Daarbij wordt gekeken naar de kans op optreden van een bedreiging, het te verdedigen belang[8] en de mogelijke impact hiervan op de bedrijfsvoering. De beveiligingsrichtlijnen bieden de maatregelen die genomen kunnen worden om het optreden van bedreigingen terug te dringen en/of de impact in geval van optreden van een bedreiging te beperken.

Als voorbeeld van een aanpassing van de algemene classificaties in specifieke situaties kan worden gekeken naar beschikbaarheidsmaatregelen. De noodzaak van beschikbaarheidsmaatregelen kan bijvoorbeeld laag zijn in situaties waar het niet beschikbaar zijn van een webdienst weinig impact heeft op de bedrijfsvoering. De noodzaak kan juist hoog zijn in situaties waar de impact en de kans op optreden van een bedreiging groot zijn.

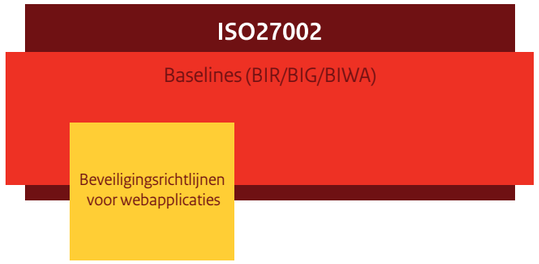
Uitgangspunten

Deze Richtlijnen:

- zijn generiek van opzet en voor een breed spectrum van dienstverlening toepasbaar;
- richten zich op de vier kernaspecten van informatiebeveiliging: beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid;
- hebben betrekking op webapplicaties en de omgeving die hiervoor benodigd is. Dit omvat de hardware waarop de software draait, het netwerk, de koppelingen tussen componenten, het beheer en alle software die noodzakelijk is om de webdienst op een veilige manier aan te bieden;
- kunnen als (toetsbare) norm worden gebruikt bij aan- en uitbestedingen van diensten en onderlinge afspraken;
- beschrijven in het document Richtlijnen vooral beveiligingsmaatregelen op hoog niveau die organisaties kunnen nemen om webapplicaties veiliger te maken;
- beschrijven in het document Verdieping op detailniveau de (deel) beveiligingsmaatregelen en hoe deze geïmplementeerd kunnen worden.

Context/scope

Deze Richtlijnen richten zich op de beveiliging van webapplicaties vanuit het oogpunt van de aanbiedende partij (de serverzijde). De Richtlijnen richten zich niet op de clientinrichting van gebruikers van de webapplicatie.[9] Er zijn daarom in deze Richtlijnen geen directe beveiligingsmaatregelen opgenomen voor de manier waarop afnemende partijen (de werkstations) veilig gebruik kunnen maken van webapplicaties.
Deze Richtlijnen zijn niet alomvattend en kunnen naast beveiligingsvoorschriften en baselines met een bredere scope (zoals BIR[10] en BIG[11]) worden gebruikt. Waar dergelijke baselines uit een deelverzameling van de maatregelen uit ISO-standaard 27002 bestaan, kennen deze Richtlijnen wel een gedeeltelijke overlap met ISO27002 en baselines, maar zijn ze op bepaalde onderdelen gedetailleerder uitgewerkt.



Figuur 1. Positionering Richtlijnen ten opzichte van ISO2700x en overheidsbaselines

De Richtlijnen bieden specifieke verdieping voor de beveiliging van webapplicaties. De beveiliging van webapplicaties moet passen binnen de beveiligingsopzet die organisaties voor hun overige processen en omgeving al ingericht zouden moeten hebben, bijvoorbeeld op basis van de ISO 27002.

Deze Richtlijnen zijn primair technisch van aard. Dit betekent dat een aantal aspecten van informatiebeveiliging geen onderdeel uitmaakt van het raamwerk dat in deze Richtlijnen wordt gehanteerd. Het raamwerk besteedt bijvoorbeeld nauwelijks tot geen aandacht aan zaken als beveiligingsorganisatie, fysieke beveiliging en personeel. Niet-technische maatregelen worden uitsluitend opgenomen wanneer deze noodzakelijk worden geacht voor de technische context of wanneer andere normenkaders of standaarden hier onvoldoende op ingaan. Indien een risicoanalyse aanleiding geeft voor het invullen van deze aanvullende beveiligingsmaatregelen dan wordt verwezen naar andere beveiligingsstandaarden zoals ISO 27001 en ISO 27002.

Deze Richtlijnen zijn het uitgangspunt voor de beveiliging van webapplicaties en een organisatie kan de beveiliging van zijn webapplicaties (laten) toetsen op basis van deze Richtlijnen. De toetsende organisaties kunnen deze Richtlijnen gebruiken om een objectief beveiligingsassessment uit te voeren. Bij het beoordelen van een specifieke situatie en bij het implementeren van de Richtlijnen (het oplossen van tekortkomingen) kan naar deze Richtlijnen verwezen worden.

Verschil tussen versie 2012 en versie 2015

De opbouw van de Richtlijnen versie 2012 was gebaseerd op het raamwerk beveiliging webapplicaties (RBW)[12] van het NCSC en onderverdeeld naar de volgende lagen:

- Algemene maatregelen
- Netwerkbeveiliging
- Beveiliging van het platform/besturingssysteem
- Beveiligen van een webapplicatie op applicatieniveau
- Afscherming van webapplicaties via authenticatie- en autorisatiemechanismen
- Implementatie van vertrouwelijkheid en onweerlegbaarheid in webapplicaties
- Integratie van de webapplicatie met de verschillende beveiligingscomponenten
- Inrichting van monitoring, auditing en alerting

De opbouw en formulering van deze Richtlijnen, versie 2015, is gebaseerd op het SIVA-raamwerk.[13] Dit raamwerk helpt bij het systematisch in kaart brengen van auditobjecten en de beschrijving van richtlijnen voor de in kaart gebrachte auditobjecten. Daarnaast zorgt het voor een betere verbinding van beleid, uitvoering en beheersing van de te nemen maatregelen.

Het SIVA-raamwerk bestaat uit vier componenten: Structuur, Inhoud, Vorm en Analysevolgorde. In de volgende paragraaf worden Structuur, Inhoud en Vorm besproken. Analysevolgorde gaat over de wijze waarop deze structuur gebruikt wordt bij het ontwikkelen van referentiekaders. Omdat we hier te maken hebben met bestaande richtlijnen voor een specifiek auditobject (webapplicatie-omgeving) is de component Analysevolgorde niet van toepassing. De opbouw van deze Richtlijnen wordt verder toegelicht in de volgende paragraaf.

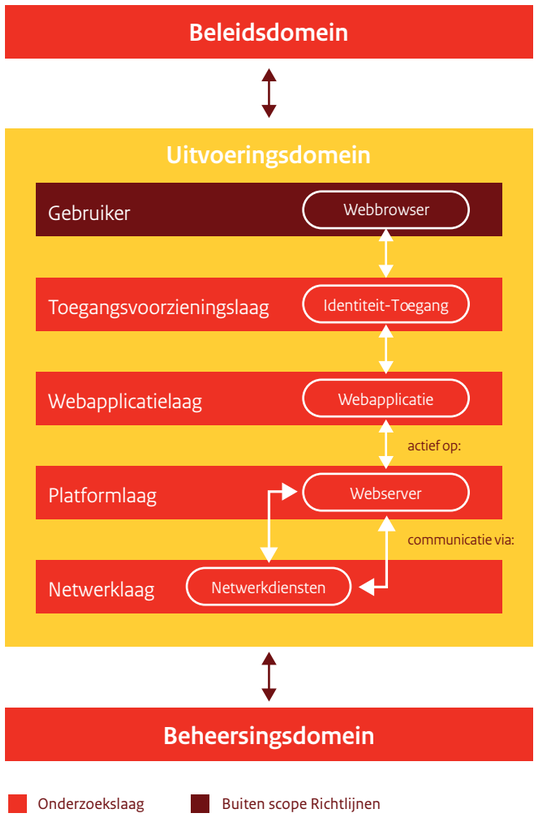
In bijlage C is een verwijzingstabel opgenomen waarin is aangegeven in welke richtlijn(en) iedere richtlijn uit 2012 is opgenomen.

Organisatie van de Richtlijnen

In deze paragraaf wordt de indeling van deze Richtlijnen toegelicht.

Indeling van de webapplicatie-omgeving op basis van domeinen (Structuur)

De beveiligingsrichtlijnen zijn, naar de gelijknamige domeinen, georganiseerd in drie hoofdstukken: beleidsdomein, uitvoeringsdomein en control- of beheersingsdomein. Deze indeling komt voort uit het SIVA-raamwerk. Figuur 2 geeft de indeling van de richtlijnen.



Figuur 2. Indeling van de beveiligingsrichtlijnen

8 Of mate van bereidheid risico's te accepteren.
9 Clientbeveiliging ligt gezien de diversiteit buiten de scope en worden qua risico geclassificeerd als een niet te beïnvloeden en niet te vertrouwen factor.
10 BIR = Baseline Informatiebeveiliging Rijksdienst
11 BIG = Baseline Informatiebeveiliging Nederlandse Gemeenten
12 https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/raamwerk-beveiliging-webapplicaties.html
13 Voor achtergronden en de wetenschappelijke basis van het SIVA-raamwerk wordt verwezen naar het proefschrift van W. Tewarie. 'SIVA – Methodiek voor de ontwikkeling van auditreferentiekaders', 2014.

Beleidsdomein
Hier bevinden zich elementen die aangeven wat in organisatiebrede zin bereikt kan worden en bevat daarom conditionele en randvoorwaardelijke elementen die van toepassing zijn op de overige lagen, zoals doelstellingen, informatiebeveiligingsbeleid, strategie en vernieuwing, organisatiestructuur en architectuur.

Uitvoeringsdomein
In dit domein wordt de implementatie van de ICT-diensten uiteengezet, zoals toegangsvoorzieningen, webapplicaties, platformen, webservers en netwerken.

Beheersingsdomein
Evaluatieaspecten en meetaspecten zijn in dit domein opgenomen. Daarnaast treffen we hier ook de beheerprocessen aan, die noodzakelijk zijn voor de instandhouding van ICT-diensten. De informatie uit de evaluaties en de beheerprocessen is niet alleen gericht op het bijsturen van de geïmplementeerde webapplicaties, maar ook om het bijsturen en/of aanpassen van de eerder geformuleerde conditionele elementen die gebaseerd zijn op “onzekere” informatie en aannames, visie en uitgestippeld beleid.
Een voorbeeld van een dergelijke aanname is een inschatting van de capaciteitsbehoefte. In de praktijk kan (en zal) het gebruik anders zijn dan oorspronkelijk verondersteld. Dan is een mechanisme nodig dat de daadwerkelijke belasting meet en een proces waarin eventueel noodzakelijke veranderingen worden vastgesteld en doorgevoerd.

Maatregelen per domein (Inhoud)
Binnen de domeinen zijn de verschillende onderwerpen benoemd. Binnen het uitvoeringsdomein is bovendien een verdere structuur aangebracht, om uitdrukking te geven aan de verschillende (technische) disciplines die hier een rol spelen. Ieder onderwerp heeft hier een eigen specifiek beleid en een eigen specifieke beheersing. Daar waar specifiek beleid meerdere onderwerpen raakt, is dit – om dubbelingen tegen te gaan – alsnog als algemeen beleid opgenomen, ook al is de inhoud vrij specifiek van aard. Op dezelfde manier zijn ook vrij specifieke beheersingsmaatregelen in de algemene beheersing terecht gekomen.

Beschrijving van de richtlijnen (Vorm)
De beveiligingsrichtlijnen zijn in dit document verkort tot een opsomming van de maatregelen. Het document Verdieping bevat een uitgebreidere structuur met een omschrijving van het risico, conformiteitsindicatoren en een nadere toelichting op de maatregel waar nodig.
Met nadruk wordt gesteld dat de beschreven doelstellingen mogelijk ook met een (deels) andere invulling bereikt kunnen worden dan door de uitwerking die in deze richtlijnen bij de maatregelen wordt aangegeven. De beschreven maatregelen zijn een handreiking aan opdrachtgevers, technici en auditors. Zij zullen zelf de eindafweging moeten maken en deze verantwoorden. Voor het verantwoorden kunnen zij dan verwijzen naar de criteria en doelstellingen, met een beschrijving hoe hieraan op andere wijze invulling is gegeven.

Over de bijlagen
Een overzicht van alle gebruikte afkortingen staat in bijlage A.
Bij het samenstellen van deze beveiligingsrichtlijnen is een aantal literatuurbronnen geraadpleegd. Op plaatsen waar informatie uit literatuurbronnen verwerkt is, wordt naar die bron verwezen in de vorm van ‘[x]’. ‘[x]’ verwijst naar een document opgenomen in bijlage B.
Bijlage C is een tabel waarin de maatregelen uit de beveiligingsrichtlijnen uit 2012 worden gerelateerd aan de overeenkomstige maatregelen uit deze richtlijn.
Tot slot gebruiken de beveiligingsrichtlijnen ook voetnoten om bepaalde termen of begrippen te verduidelijken. Deze voetnoten herkent u aan een cijfer in superscript (bijvoorbeeld: [3]).

NOOT Als dit document de naam van een product, dienst, fabrikant of leverancier noemt, betekent dit niet dat het NCSC deze op enige wijze goedkeurt, afkeurt, aanraadt, afraadt of op een andere manier hiermee verbonden is.

Onderhoud van de Richtlijnen
Het NCSC is verantwoordelijk voor het opstellen en onderhouden van deze Richtlijnen en zal ze periodiek actualiseren. Indien noodzakelijk zal het NCSC tussentijds door middel van een addendum of erratum de Richtlijnen aanpassen.
Hebt u aanvullingen op, opmerkingen over of eigen ervaringen met deze Richtlijnen? Het NCSC ontvangt ze graag via richtlijnen@ncsc.nl.

Relatie met andere documenten
Deze Richtlijnen zijn afgeleid van het ‘Raamwerk beveiliging webapplicaties (RBW)’ [1] van het NCSC. De beveiligingsadviezen uit het RBW zijn in dit document op een andere wijze gerangschikt en in sommige gevallen opgedeeld indien dit de opbouw ten goede kwam (zie bijlage F voor de verwijzingstabel).
Daarnaast wordt in beveiligingsrichtlijnen verwezen naar de volgende relevante normen, standaarden, best practices, zoals:
» Open Web Application Security Project (OWASP)[14] Top 10 2013 [2]
» OWASP Testing Guide v3 [3]
» OWASP Code Review Guide [4]
» OWASP Application Security Verification Standard (ASVS) [5]
» NEN-ISO/IEC 27001 ‘Managementsystemen voor informatiebeveiliging’ [6][15]
» NEN-ISO/IEC 27002 ‘Praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging’ [7][16]
» NEN-ISO/IEC 27005 ‘Information security risk management’ [8][17]
» Basisnormen Beveiliging en Beheer ICT-infrastructuur [9]
» Nederlandse Overheid Referentie Architectuur (NORA)[18] Dossier Informatiebeveiliging [10]

14 Het Open Web Application Security Project (OWASP) is een wereldwijde charitatieve not-profitorganisatie met als doel de beveiliging van applicatiesoftware te verbeteren. Hun missie is om applicatiebeveiliging zichtbaar te maken, zodat mensen en organisaties een weloverwogen beslissingen kunnen nemen over de veiligheidsrisico’s met betrekking tot applicaties. OWASP heeft ook een Nederlandse Chapter <https://www.owasp.org/index.php/Netherlands>.

15 NEN-ISO/IEC 27001:2013 specificeert eisen voor het vaststellen, implementeren, uitvoeren, controleren, beoordelen, bij-houden en verbeteren van een gedocumenteerd ISMS in het kader van de algemene bedrijfsrisico’s voor de organisatie. De eisen in deze internationale norm zijn algemeen en bedoeld om van toepassing te zijn voor alle organisaties, ongeacht type, omvang of aard.

16 NEN-ISO/IEC 27002:2013 geeft richtlijnen en principes voor het initiëren, het implementeren, het onderhouden en het verbe-teren van informatiebeveiliging binnen een organisatie.

17 NEN-ISO/IEC 27005 geeft richtlijnen voor risicobeheer en ondersteunt de uitvoering van informatiebeveiliging op basis van een risicomanagementaanpak.

18 De Nederlandse Overheid Referentie Architectuur (NORA) bevat principes, beschrijvingen, modellen en standaarden voor het ontwerp en de inrichting van de elektronische overheid. Het is een instrument dat door overheidsorganisaties kan wor-den benut in de verbetering van de dienstverlening aan burgers en bedrijven <http://www.e-overheid.nl/onderwerpen/e-overheid/architectuur/nora-familie/nora>.

Beleidsdomein

Doelstelling

De doelstelling van het beleidsdomein is om vast te stellen of er voldoende randvoorwaarden op het strategisch niveau zijn geschapen om webapplicaties veilig te doen functioneren, zodat de juiste ondersteuning wordt geleverd voor het bereiken van de afgesproken doelstellingen.

Risico's

Door het ontbreken van een door het management uitgevaardigd beleid bestaat het risico dat onvoldoende sturing wordt gegeven aan de veilige inrichting van de ICT-omgeving waar de webapplicatie een onderdeel van uitmaakt. Dit zal een negatieve impact hebben op de realisatie van organisatiedoelstellingen.

Beveiligingsrichtlijn B.01

Informatiebeveiligingsbeleid

Richtlijn (wie en wat)
De organisatie formuleert een informatiebeveiligingsbeleid en besteedt hierin specifiek aandacht aan webapplicatiegerelateerde onderwerpen zoals dataclassificatie, toegangsvoorziening en kwetsbaarhedenbeheer.

Doelstelling (waarom)
Hiermee wordt ervoor gezorgd dat in het beveiligingsproces specifiek aandacht is voor de webapplicaties van de organisatie.

Classificatie
Hoog

Richtlijn 2012
Bo-1

Maatregelen

01 Het informatiebeveiligingsbeleid voldoet aan de eisen die in ISO-standaard 27002[19] of een voor de organisatie geldende baseline worden gesteld.
02 Laat het informatiebeveiligingsbeleid vaststellen door verantwoordelijk hoger management (CxO–niveau).
03 Stel een dataclassificatieschema op.
04 Formuleer specifiek beleid voor het verlenen van toegang tot functies en gegevens aan personen en systemen.
05 Formuleer voorschriften om de risico's van kwetsbaarheden in ICT-componenten te verminderen.
06 Voer een responsible-disclosurebeleid[20] in.

Beveiligingsrichtlijn B.02

Toegangsvoorzieningsbeleid

Richtlijn (wie en wat)
Het toegangsvoorzieningsbeleid formuleert, op basis van eisen en wensen van de organisatie, richtlijnen voor de organisatorische en technische inrichting (ontwerp) van de processen en middelen, waarmee de toegang en het gebruik van ICT-diensten gereguleerd wordt.

Doelstelling (waarom)
De effectieve toegang tot informatiesystemen voor bevoegde

19 ISO/IEC 27002:2013: Chapter 5. Information Security Policies.
20 Voor meer informatie, zie: https://www.ncsc.nl/actueel/nieuwsberichten/leidraad-responsiblediscl osure.html.

gebruikers bewerkstelligen en de integriteit, vertrouwelijkheid en controleerbaarheid van de gegevens binnen informatiesystemen garanderen.

Classificatie
Hoog

Richtlijn 2012
Bo-12

Maatregelen

01 Documenteer zakelijke behoeften en beveiligingseisen voor de toegangsvoorzieningen en stel deze vast.
02 Identificeer gebruikersgroepen, -profielen en/of –rollen.
03 Leg alleen de hoogst noodzakelijke gegevens van gebruikers vast.
04 Leg de relatie vast tussen gebruikersgroepen, -profielen en/of -rollen en het dataclassificatieschema.
05 Leg vast welke combinaties van functies, taken en/of rollen ongewenst zijn (functiescheiding).
06 Stel eisen aan de toegestane authenticators.
07 Stel eisen aan de inzet van technische middelen voor identificatie, authenticatie en autorisatie.
08 Stel richtlijnen en procedures op voor de technische inrichting van toegangsvoorzieningen (identificatie, authenticatie en autorisatie) in informatiesystemen, besturingssystemen en netwerken.
09 Stel eisen aan:
   » de uniformiteit en flexibiliteit van authenticatiemechanismen;
   » de rechten voor platformaccounts;
   » het automatisch verbreken van de sessie (zie ook richtlijn U/WA.08);
   » de identificatie/authenticatie(mechanismen) om voldoende sterke wachtwoorden af te dwingen.
10 Baseer de inrichting van het identiteit- en toegangsbeheer op een vastgesteld ontwerp.

Beveiligingsrichtlijn B.03

Risicomanagement

Richtlijn (wie en wat)
Voor de webapplicatieomgeving wordt risicomanagement uitgevoerd waarbij (web)applicaties en hun ondersteunende infrastructuur zowel tijdens ontwikkeling als tijdens operationeel gebruik periodiek worden onderworpen aan een (informatie) risicoanalyse.

Doelstelling (waarom)
Bepalen of de risico's (nog) binnen de voor de organisatie acceptabele grenzen liggen en verantwoordelijken informatie verschaffen voor het treffen van eventuele (aanvullende) maatregelen.

Classificatie
Hoog

Richtlijn 2012
Bo-2

Maatregelen

01 Maak gebruik van een breed toegepaste risicoanalyse-methode.
02 Voer voor (nieuwe) webapplicaties een risicoanalyse uit en herhaal deze risicoanalyses periodiek.
03 Houd van elke uitgevoerde risicoanalyse de rapportage beschikbaar en stel er een informatiebeveiligingsplan bij op.
04 Volg aantoonbaar de aanbevelingen/verbetervoorstellen uit de risicoanalyses op.

Beveiligingsrichtlijn B.04

Cryptografiebeleid

Richtlijn (wie en wat)
Het cryptografiebeleid formuleert eisen die worden gesteld aan processen en procedures rond het beheer van cryptografisch materiaal en de opslag en distributie van dit materiaal.

Doelstelling (waarom)
Beschermen van cryptografische sleutels op een manier die past bij de aard van de cryptografisch beschermde gegevens (dataclassificatie B.01/03).

Classificatie
Hoog

Richtlijn 2012
B5-1, B5-7

Maatregelen

01 Stel eisen aan processen en procedures voor aanvraag, creatie, hernieuwing, intrekken en beheer van sleutelmateriaal en certificaten.
02 Stel eisen aan procedures voor beheer om te zorgen voor een 'soepele' migratie wanneer een patch een certificaat van de lijst met vertrouwde certificaten verwijdert.
03 Stel eisen aan opslag van sleutelmateriaal.
04 Stel eisen aan distributie van sleutelmateriaal.

Beveiligingsrichtlijn B.05

Contractmanagement

Richtlijn (wie en wat)
In een contract met een derde partij voor de uitbestede levering of beheer van een web-applicatie (als dienst) zijn de beveiligingseisen en -wensen vastgelegd en op het juiste (organisatorische) niveau vastgesteld.

Doelstelling (waarom)
Het handhaven van het beveiligingsniveau, wanneer de verantwoordelijkheid voor de ontwikkeling en/of het beheer van de webapplicatie is uitbesteed aan een andere organisatie.

Classificatie
Hoog

Richtlijn 2012
Bo-14

Maatregelen

01 Laat het (beveiligings)beleid onderdeel zijn van het pakket beveiligingseisen en -wensen dat is opgesteld bij de verwerving van webdiensten en middelen.
02 Laat de requirements en specificaties voor de webdienst onderdeel zijn van het eisenpakket dat is opgesteld bij de verwerving van diensten en middelen.

Beveiligingsrichtlijn B.06

ICT-landschap

Richtlijn (wie en wat)
De organisatie heeft de actuele documentatie van het ICT-landschap vastgelegd, met daarin de bedrijfsprocessen, de technische componenten, hun onderlinge samenhang en de ICT-beveiligingsarchitectuur.

Doelstelling (waarom)
Het geven van inzicht geven in de relatie tussen techniek en bedrijfsprocessen en de manier waarop en mate waarin deze op elkaar aansluiten. Hiernaast geeft het ICT-landschap inzicht in de interactie en relaties tussen webapplicaties en andere componenten in de ICT-infrastructuur.

Classificatie
Midden

Richtlijn 2012
Bo-3, B6-1

Maatregelen

01 Inventariseer en karakteriseer de bedrijfsprocessen, functies, rollen, et cetera die bij het aanbieden, gebruiken en onderhouden van een webapplicatie betrokken zijn.
02 Benoem en beschrijf de technische componenten (waaronder infrastructuur en software) die bij het aanbieden, gebruiken en onderhouden van een webapplicatie betrokken zijn.
03 Benoem en beschrijf de koppelingen met externe netwerken die bij het aanbieden, gebruiken en onderhouden van een webapplicatie betrokken zijn.
04 Benoem en beschrijf de beveiligingsmaatregelen die hun weerslag hebben (in componenten) in het ICT-landschap.
05 Benoem en beschrijf de onderlinge samenhang tussen technische componenten (waaronder infrastructuur en software) die bij het aanbieden, gebruiken en onderhouden van een webapplicatie betrokken zijn.
06 Benoem en beschrijf de functionele relaties tussen de applicaties die bij het aanbieden, gebruiken en onderhouden van een webapplicatie betrokken zijn.
07 Benoem en beschrijf de onderlinge samenhang tussen bedrijfsprocessen die bij het aanbieden, gebruiken en onderhouden van een webapplicatie betrokken zijn.
08 Benoem en beschrijf de samenhang tussen bedrijfsprocessen en technische componenten die bij het aanbieden, gebruiken en onderhouden van een webapplicatie betrokken zijn.
09 Geef met behulp van de ICT-beveiligingsarchitectuur inzicht in de relatie tussen de toegangsvoorzieningen en het gehele ICT-landschap (inclusief beveiligingsservices).

Uitvoeringsdomein

Doelstelling

Vanuit de klant- en organisatie-invalshoek is het doel van de diensten op de ICT-lagen betrouwbare diensten te leveren. Vanuit de assessmentinvalshoek is het doel om vast te stellen of de geleverde diensten adequaat en veilig zijn ingericht.

Domeinen

Binnen het uitvoeringsdomein worden richtlijnen voor de ICT-lagen geformuleerd. De lagen die uitgewerkt worden zijn:

» toegangsvoorzieningsmiddelen;
» webapplicaties;
» platformen en webservers;
» netwerken.

De betrokken maatregelen zullen binnen de specifieke lagen worden uitgewerkt.

UITVOERINGSDOMEIN
» TOEGANGSVOORZIENINGSMIDDELEN

Doelstelling
De doelstelling van de laag "Toegangsvoorzieningsmiddelen" is om te waarborgen dat de toegang tot objecten als data, webapplicaties, computerapparatuur en netwerken ingericht is volgens specifieke beleidsuitgangspunten van de organisatie. De werking voldoet aan de eisen die door de organisatie zijn gesteld ten aanzien van de kwaliteitsaspecten vertrouwelijkheid, integriteit, beschikbaarheid en controleerbaarheid van deze objecten.[21]

Risico's
Door het ontbreken van adequate toegangsbeveiliging tot (web) applicaties, systemen en netwerken bestaat het risico dat onbevoegden zich toegang kunnen verschaffen tot deze objecten, waardoor ongewenste acties op de services kunnen plaatsvinden en/of informatie kan worden ontvreemd of verminkt.
Identiteiten zijn gevoelige persoonsgegevens. Wanneer een systeem onvoldoende bescherming biedt tegen misbruik of diefstal kan dit leiden tot identiteitsfraude (binnen het systeem of elders met misbruik van identiteiten uit het systeem).

Beveiligingsrichtlijn U/TV.01

Toegangsvoorzieningsmiddelen

Richtlijn (wie en wat)
Het toegangsvoorzieningsbeleid formuleert, op basis van eisen en wensen van de organisatie, richtlijnen voor de organisatorische en technische inrichting (ontwerp) van de processen en middelen, waarmee de toegang en het gebruik van ICT-diensten gereguleerd wordt.

Doelstelling (waarom)
De effectieve toegang tot informatiesystemen voor bevoegde gebruikers bewerkstelligen en de integriteit, vertrouwelijkheid en controleerbaarheid van de gegevens binnen informatiesystemen garanderen.

Classificatie
Hoog

Richtlijn 2012
B0-12, B04-1

Maatregelen
01 Ondersteun de initiële vaststelling en vastlegging van de identiteit van personen met het toegangsvoorzieningsmiddel.
02 Bied adequate bescherming van de vastgelegde gebruikers- en toegangsgegevens met het toegangsvoorzieningsmiddel.
03 Ondersteun in voldoende mate het vaststellen van de identiteit van natuurlijke personen met het authenticatiemiddel.
04 Ondersteun het wachtwoordbeleid met het authenticatiemiddel.
05 Wijs rechten toe op basis van het toegangsvoorzieningsbeleid.
06 Houd een actueel overzicht bij van accounts en de personen die daar gebruik van maken:
» service-accounts;
» beheeraccounts;
» gebruikersaccount;
» (web)applicatie-accounts.
07 Trek de rechten direct in en blokkeer direct het account wanneer een gebruiker geen recht op toegang meer heeft.
08 Voer periodiek een audit uit op de uitgedeelde autorisaties.
09 Registreer het beheren en onderhouden van identiteiten en autorisatie onweerlegbaar.
10 Registreer het verkrijgen van autorisatie en het gebruik van functionaliteit onweerlegbaar.
11 Ondersteun met het ingezette identiteits- en toegangsmanagementtool conform het toegangsvoorzieningsbeleid de complete levenscyclus van identiteiten en autorisaties:
» aanvragen;
» toekennen;
» wijzigen;
» intrekken/schorsen/verwijderen;
» conform voorgeschreven procedures.

21 Vaak ook aangeduid als CIAA (Confidentiality, Integrity, Availability en Auditability).

UITVOERINGSDOMEIN
» WEBAPPLICATIES

Doelstelling
De doelstelling van de laag "Webapplicaties" is om te waarborgen dat webapplicaties functioneren zoals is beoogd, ingericht zijn volgens specifieke beleidsuitgangspunten van de organisatie en voldoen aan de eisen die door de organisatie zijn gesteld ten aanzien van de kwaliteitsaspecten vertrouwelijkheid, integriteit, beschikbaarheid en controleerbaarheid.

Risico's
De ervaren of veronderstelde betrouwbaarheid van de webapplicatie wordt ondermijnd door derden, doordat zij in staat zijn de (inhoud van de) webapplicatie te manipuleren of verstoren. Oorzaken kunnen gelegen zijn in het niet (correct) of onvolledig toepassen van bekende richtlijnen en beveiligingstechnieken in zowel de ontwikkel- als de productiefase.

Beveiligingsrichtlijn U/WA.01

Operationeel beleid voor webapplicaties

Richtlijn (wie en wat)
Het operationeel beleid voor webapplicaties bevat richtlijnen en instructies en procedures met betrekking tot ontwikkeling, onderhoud en uitfasering van webapplicaties.

Doelstelling (waarom)
De ontwikkeling van de webapplicatie optimaal ondersteunen en de klant betrouwbare diensten bieden.

Classificatie
Hoog

Richtlijn 2012
-

Maatregelen
01 Stel richtlijnen op voor:
» ontwikkeling, onderhoud en uitfasering van webapplicaties;
» beveiliging van webapplicaties;
» verwerking van gegevens;
» koppelingen met onderliggende systemen;
» koppelingen met achterliggende systemen.
02 Stel instructies en procedures op voor:
» het werken met gescheiden ontwikkel-, test-, acceptatie- en productie-omgevingen (OTAP);

Beveiligingsrichtlijn U/WA.02

Webapplicatiebeheer

Richtlijn (wie en wat)
Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten.

Doelstelling (waarom)
Effectief en veilig realiseren van de dienstverlening.

Classificatie
Midden

Richtlijn 2012
-

Maatregelen
01 Voer beheerwerkzaamheden uit volgens afgesproken richtlijnen en procedures.
02 Laat leidinggevenden en systeemeigenaren vooraf criteria vastleggen waaraan de operationele webapplicatie moet voldoen.
03 Voorkom dat hiertoe niet geautoriseerde gebruikers toegang krijgen tot beheerfuncties binnen de applicatie.
04 Op basis van taken, verantwoordelijkheden en bevoegdheden zijn de verschillende beheerrollen geïdentificeerd.
05 Vul in de autorisatiematrix in:
» aan welke rollen welke bevoegdheden worden toegekend;
» hoe functiescheiding tot uitdrukking komt.
06 Richt een proces in voor het definiëren en onderhouden van de rollen.

Beveiligingsrichtlijn U/WA.03

Webapplicatie-invoer

Richtlijn (wie en wat)
De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt.

Doelstelling (waarom)
Voorkom (on)opzettelijke manipulatie van de webapplicatie, waardoor de vertrouwelijkheid, integriteit en/of beschikbaarheid van de webapplicatie aangetast worden.

Classificatie
Hoog

Richtlijn 2012
B3-1, B3-3, B3-6, B3-7

Maatregelen

01 Valideer de invoer op de server.
02 Verbied of beperk het gebruik van dynamische file includes.
03 Converteer alle invoer naar een veilig formaat, waarbij risicovolle tekens uit de invoer 'onschadelijk' worden gemaakt.
04 Weiger foute, ongeldige of verboden invoer.

Beveiligingsrichtlijn U/WA.04

Webapplicatie-uitvoer

Richtlijn (wie en wat)
De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren.

Doelstelling (waarom)
Voorkom manipulatie van het systeem van andere gebruikers.

Classificatie
Hoog

Richtlijn 2012
B3-4

Maatregelen

01 Converteer alle uitvoer naar een veilig formaat.

Beveiligingsrichtlijn U/WA.05

Betrouwbaarheid van gegevens

Richtlijn (wie en wat)
De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken.

Doelstelling (waarom)
Gegevens in opslag en transport beschermen tegen ongeautoriseerde kennisname en manipulatie.

Classificatie
Hoog

Richtlijn 2012
B5-2, B5-3, B5-4, B5-5

Maatregelen

01 Pas, wanneer de webapplicatie persoonsgegevens verwerkt, de privacy-by-designprincipes toe.
02 Maak waar mogelijk gebruik van privacybevorderende technieken.
03 Versleutel of hash gevoelige gegevens in databases en bestanden.
04 Gebruik cryptografisch sterke sessie-identificerende cookies.
05 Versleutel communicatie.
06 Onderteken transacties met een digitale handtekening.

Beveiligingsrichtlijn U/WA.06

Webapplicatie-informatie

Richtlijn (wie en wat)
De webapplicatie beperkt de informatie in de uitvoer tot de informatie die voor het functioneren van belang is.

Doelstelling (waarom)
Beperk het (onnodig) vrijgeven van informatie tot een minimum.

Classificatie
Hoog

Richtlijn 2012
B3-11

Maatregelen

01 Verwijder commentaarregels uit de scripts (code).
02 Verwijder of pseudonimiseer verwijzingen naar interne bestands- of systeemnamen.

Beveiligingsrichtlijn U/WA.07

Webapplicatie-integratie

Richtlijn (wie en wat)
De webapplicatie communiceert alleen met onder- en achterliggende systemen op basis van statisch geconfigureerde (geparametriseerde) queries en commando's en uitsluitend ten behoeve van de noodzakelijke functionaliteit.

Doelstelling (waarom)
Kwetsbaarheid van de onder- en achterliggende systemen voorkomen en de integriteit en vertrouwelijkheid garanderen.

Classificatie
Hoog

Richtlijn 2012
B3-5

Maatregelen

01 Bouw commando- en queryteksten op met uitsluitend in de code reeds aanwezige vaste tekstfragmenten.
02 Geef gebruikersinvoer die gebruikt moet worden in commando's en queries op een zodanige manier door, dat de beoogde werking niet wordt gewijzigd.
03 Houd van elke webapplicatie bij welke functionaliteit van backendsystemen nodig is.
04 Verbied directe data-toegang tot backendsystemen, tenzij andere opties niet voorhanden zijn.

Beveiligingsrichtlijn U/WA.08

Webapplicatiesessie

Richtlijn (wie en wat)
De (gebruikers)sessie die ontstaat na het succesvol aanmelden van een gebruiker, kent een beperkte levensduur en de gebruiker kan deze sessie zelf beëindigen.

Doelstelling (waarom)
Voorkomen dat derden de controle over een sessie kunnen krijgen.

Classificatie
Hoog

Richtlijn 2012
B4-2

Maatregelen

01 Maak bij het aanmelden een nieuwe sessie aan en verbreek een eventueel al bestaande sessie van die gebruiker. Maak de oude sessie-identifier ongeldig.
02 Beëindig de sessie na een vooraf vastgestelde en geconfigureerde tijdspanne van inactiviteit van de gebruiker (idle-time).
03 Beëindig de sessie na een vooraf vastgestelde en geconfigureerde sessietijd (session-time).
04 Bied de gebruiker de mogelijkheid de sessie op eigen initiatief te beëindigen (uitloggen).
05 De sessie is na beëindiging niet langer geautoriseerd binnen de webapplicatie.

Beveiligingsrichtlijn U/WA.09

Webapplicatiearchitectuur

Richtlijn (wie en wat)
Voor het implementeren, integreren en onderhouden van webapplicaties zijn architectuur- en beveiligingsvoorschriften beschikbaar.

Doelstelling (waarom)
Een webapplicatie-infrastructuur bieden die een betrouwbare verwerking garandeert.

Classificatie
Hoog

Richtlijn 2012
-

Maatregelen

01 Stel architectuurvoorschriften op die actief worden onderhouden.
02 Scheid vertrouwde en niet-vertrouwde domeinen: toepassen van scheidingen in netwerken (DMZ).
03 Pas het principe van 'least privilege' toe op hoe de webapplicatie van onderliggende servers gebruikmaakt.
04 Configureer webapplicaties en onderliggende servers zodanig dat ook security-gerelateerde events worden vastgele

UITVOERINGSDOMEIN
» PLATFORMEN EN WEBSERVERS

Doelstelling

De doelstelling van de laag "Platformen en webservers" is te waarborgen dat de platformen (besturingssystemen) en webservers ingericht zijn volgens specifieke beleidsuitgangspunten van de organisatie en voldoen aan de eisen die door de organisatie zijn gesteld ten aanzien van de kwaliteitsaspecten vertrouwelijkheid, integriteit, beschikbaarheid en controleerbaarheid.

Risico's

Door gebruik te maken van kwetsbaarheden in platformen en webservers, zijn onbevoegden in staat kennis te nemen van bedrijfs- of privacygevoelige gegevens, de gegevens te manipuleren of de beschikbaarheid van de webapplicatie negatief te beïnvloeden. Bovendien bestaat het risico dat zij in staat zijn de sporen van dit gebruik te wissen of verhullen, of dit uit andermans naam doen.

Beveiligingsrichtlijn U/PW.01

Operationeel beleid voor platformen en webservers

Richtlijn (wie en wat)
Het operationeel beleid voor platformen en webservers formuleert richtlijnen, instructies en procedures voor inrichting en beheer van platformen en webservers.

Doelstelling (waarom)
Betrouwbare ondersteuning van de programmatuur die op het platform draait.

Classificatie
Hoog

Richtlijn 2012
B2-2

Maatregelen

01 Stel voorschriften (baselines) op voor de veilige configuratie van platformen en webservers.
02 Besteed in de voorschriften expliciet aandacht aan hardening van platformen en webservers.
03 Besteed in de voorschriften expliciet aandacht aan de configuratie en het gebruik van accounts.
04 Stel instructies en procedures op voor:
» het creëren en onderhouden van voorschriften voor de veilige configuratie van platformen en webservers;
» het toepassen van voorschriften voor de veilige configuratie van platformen en webservers.

Beveiligingsrichtlijn U/PW.02

Webprotocollen

Richtlijn (wie en wat)
De webserver garandeert specifieke kenmerken van de inhoud van de protocollen.

Doelstelling (waarom)
Voorkom inzage, wijziging of verlies van gegevens door manipulatie van de logica van de webserver of webapplicatie.

Classificatie
Hoog

Richtlijn 2012
B3-2, B3-8, B3-9, B3-10, B3-12

Maatregelen

01 Behandel alleen http-requests waarvan de gegevens een correct type, lengte, formaat, tekens en patronen hebben.
02 Behandel alleen http-requests van initiators met een correcte authenticatie en autorisatie.
03 Sta alleen de voor de ondersteunde webapplicaties benodigde http-requestmethoden (GET, POST, etc.) toe en blokkeer de overige niet noodzakelijke http-requestmethoden.
04 Verstuur alleen http-headers die voor het functioneren van http van belang zijn.
05 Toon in http-headers alleen de hoogst noodzakelijke informatie die voor het functioneren van belang is.
06 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.

Beveiligingsrichtlijn U/PW.03

Webserver

Richtlijn (wie en wat)
De webserver is ingericht volgens een configuratie-baseline.

Doelstelling (waarom)
Ongewenste vrijgave van informatie tot een minimum beperken, met name waar het gaat om informatie die inzicht geeft in de opbouw van de beveiliging.

Classificatie
Hoog

Richtlijn 2012
B3-13, B3-16

Maatregelen

01 Beschrijf de parametrisering van de webserver in een configuratiedocument.
02 Verbied het opvragen van de inhoud van het filesysteem van de server. Ondersteun geen directory-listings.
03 Stel voor alle cookies de flags 'secure' en 'HttpOnly' in.
04 Verstuur bij alle http-responses de http-headers 'Content-Security-Policy: frame-ancestors' en (tijdelijk) 'X-Frame-Options'.

Beveiligingsrichtlijn U/PW.04

Isolatie van processen/bestanden

Richtlijn (wie en wat)
Kritieke delen van systemen (bijv. subprocessen, bestanden) beschermen door isolatie van overige delen.

Doelstelling (waarom)
Beperk de impact bij misbruik van processen.

Classificatie
Hoog

Richtlijn 2012
B2-3

Maatregelen

01 Stel een ontwerp- en configuratiedocument vast dat beschrijft op welke wijze processen worden afgeschermd van bestanden waartoe zijn geen toegang mogen hebben.
02 Stel een ontwerp- en configuratiedocument vast dat beschrijft op welke wijze processen van elkaar worden afgeschermd.

Beveiligingsrichtlijn U/PW.05

Toegang tot beheermechanismen

Richtlijn (wie en wat)
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 (waarom)
Voorkomen van misbruik van beheervoorzieningen.

Classificatie
Hoog

Richtlijn 2012
B2-1

Maatregelen

01 Gebruik uitsluitend beveiligde (communicatie)protocollen voor de toegang tot beheermechanismen.
02 Gebruik sterke authenticatie voor de toegang tot de beheermechanismen.

Beveiligingsrichtlijn U/PW.06

Platform-netwerkkoppeling

Richtlijn (wie en wat)
Ieder platform filtert het netwerkverkeer met behulp van een lokale firewall, zodat het netwerkverkeer beperkt is tot de bekende, toegestane communicatiestromen.

Doelstelling (waarom)
Controleren van het netwerkverkeer, zowel op poort- als procesniveau, dat lokaal binnenkomt en uitgaat.

Classificatie
Hoog

Richtlijn 2012
B2-4

Maatregelen

01 Stel een (inrichtings)document op met de communicatiestromen van de op het systeem geïnstalleerde applicaties.
02 De ingestelde firewall-regels beperken communicatiestromen tot die van het (inrichtings)document.

Beveiligingsrichtlijn U/PW.07

Hardening van platformen

Richtlijn (wie en wat)
Voor het configureren van platformen is een hardeningrichtlijn beschikbaar.

Doelstelling (waarom)
Beperken van de functionaliteit tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.

Classificatie
Hoog

Richtlijn 2012
Bo-5

Maatregelen

01 Richt ICT-componenten (aantoonbaar) volgens de instructies en procedures van de leverancier in.
02 Houd een actueel overzicht bij van de noodzakelijke protocollen, services en accounts voor de op het platform geïnstalleerde applicaties.
03 Deactiveer of verwijder alle protocollen, services en accounts op het platform als die niet volgens het ontwerp noodzakelijk zijn.
04 Toets periodiek of de in productie zijnde ICT-componenten niet meer dan de vanuit het ontwerp noodzakelijke functies bieden (statusopname). Afwijkingen worden hersteld.
05 Pas de beveiligingsconfiguraties van netwerkservices en protocollen op het platform aan conform richtlijnen.

Beveiligingsrichtlijn U/PW.08

Platform- en webserverarchitectuur

Richtlijn (wie en wat)
Voor het implementeren, integreren en onderhouden van platformen en webservers zijn architectuurvoorschriften en beveiligingsvoorschriften beschikbaar.

Doelstelling (waarom)
Een platform bieden dat een betrouwbare verwerking garandeert.

Classificatie
Midden

Richtlijn 2012
-

Maatregelen

01 Stel architectuurvoorschriften op die actief worden onderhouden.
02 Stel hardeningrichtlijnen op voor platformen, aantoonbaar afgeleid uit de architectuur.
03 Leid de inrichtingsrichtlijnen voor registratie van (beveiligings) events (logging, zie richtlijn C.06) aantoonbaar af uit de architectuur.

UITVOERINGSDOMEIN » NETWERKEN

Doelstelling

De doelstelling van de laag “Netwerken” is om te waarborgen dat de netwerkinfrastructuur ingericht is overeenkomstig specifieke beleidsuitgangspunten van de organisatie en voldoet aan de eisen die door de organisatie zijn gesteld ten aanzien van de kwaliteitsaspecten vertrouwelijkheid, integriteit, beschikbaarheid en controleerbaarheid.

Risico’s

De beoogde of vereiste betrouwbaarheid van de webapplicatie wordt ondermijnd door derden, doordat zij in staat zijn het netwerk (of componenten daarin) te manipuleren of verstoren. Oorzaken kunnen gelegen zijn in het niet (correct) of onvolledig toepassen van bekende richtlijnen en (beveiligings)technieken.

Beveiligingsrichtlijn U/NW.01

Operationeel beleid voor netwerken

Richtlijn (wie en wat)
Het operationeel beleid voor netwerken formuleert richtlijnen, instructies en procedures voor inrichting en beheer van netwerken.

Doelstelling (waarom)
Betrouwbare communicatie voor de systemen die binnen het netwerk geïnstalleerd zijn.

Classificatie
Midden

Richtlijn 2012
-

Maatregelen

01 Stel voorschriften (baselines) op voor de veilige inrichting en beheer van netwerken. De baseline dient ook aandacht te geven aan hardening, zie richtlijn U/NW.06.
02 Stel procedures en instructies op voor het inrichten van netwerkcomponenten aan de hand van beveiligingstemplates.
03 Stel aansluitvoorwaarden op die beschrijven wanneer een (nieuwe) component op het netwerk mag worden aangesloten.

Beveiligingsrichtlijn U/NW.02

Beschikbaarheid van netwerken

Richtlijn (wie en wat)
Het netwerk is gebaseerd op betrouwbare netwerkcomponenten, ondersteund door redundantie.

Doelstelling (waarom)
Zekerstellen dat er geen zwakke schakels (single-points-of-failure) in voorkomen en dat het netwerk te allen tijde beschikbaar is.

Classificatie
Hoog

Richtlijn 2012
B1-6

Maatregelen

01 Configureer de netwerkcomponenten op basis van beveiligingstemplates.
02 Voer vooraf gekozen en ontworpen netwerkcomponenten meervoudig uit en configureer deze zodanig dat zij automatisch (zonder menselijke interactie) enkelvoudige storingen opvangen.
03 Signaleer automatisch opgevangen storingen (failover) aan de beheerders.

Beveiligingsrichtlijn U/NW.03

Netwerkzonering

Richtlijn (wie en wat)
Het netwerk is gescheiden in logische en fysieke domeinen (zones), in het bijzonder is er een DMZ die tussen het interne netwerk en het internet gepositioneerd is.

Doelstelling (waarom)
Een beveiligde (of robuuste) netwerkinfrastructuur bieden voor de bedrijfstoepassingen.

Classificatie
Hoog

Richtlijn 2012
B1-1, B1-2, B1-4

Maatregelen

01 Deel het netwerk in domeinen (of zones) op, op grond van gemeenschappelijke kenmerken van de systemen binnen een domein.
02 Sta alleen voor de beoogde diensten noodzakelijke verkeersstromen tussen zones toe.
03 Scheid netwerkzones fysiek of logisch van elkaar, zet een minimale hoeveelheid netwerkcomponenten in op koppelvlakken die deze scheiding handhaven.
04 Gebruik verschillende fysieke interfaces voor aansluiting van verschillende (logische) netwerkzones.
05 Scheid het interne bedrijfsnetwerk en het internet van elkaar door middel van een bufferzone ('demilitarised zone', DMZ) dat bestaat uit frontend-zones en backend-zones.
06 Leg in een DMZ-inrichtingsdocument/ontwerp vast welke uitgangspunten en principes gelden voor de toepassing van de DMZ.
07 Plaats alleen de systemen, (web)applicaties en diensten in de DMZ die in het DMZ-ontwerp voorkomen.
08 Configureer de filters en regels binnen een DMZ conform het DMZ-ontwerp.
09 Laat verkeersstromen tussen interne netwerken en externe netwerken lopen via een DMZ, en controleer en ontkoppel deze op applicatieniveau (sessiescheiding).
10 Sta alleen de voor de beoogde diensten noodzakelijke verkeersstromen tussen internet en de DMZ en tussen de DMZ en het interne netwerk toe.

Beveiligingsrichtlijn U/NW.04

Protectie- en detectiefunctie

Richtlijn (wie en wat)
De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van protectie- en detectiemechanismen.

Doelstelling (waarom)
Het detecteren van aanvallen (onder andere (D)DoS) om te voorkomen dat de vertrouwelijkheid, integriteit en/of beschikbaarheid van geleverde services negatief wordt beïnvloed.

Classificatie
Hoog

Richtlijn 2012
B1-5, B7-1

Maatregelen

01 Zorg voor een actueel DMZ-inrichtingsdocument/ontwerp dat inzicht geeft welke protectiemechanismen zijn betrokken.
02 Pas anti-spoofingmechanismen toe in het netwerk.
03 Reguleer dataverkeer met access control lists (ACL's) op basis van bijvoorbeeld ip-adres of poortnummer.
04 Stel de firewall-regels op en configureer deze via een proces en review dit periodiek.
05 Monitor inkomend en uitgaand verkeer in het netwerk.
06 Monitor de infrastructuur zodat detectie van ((D)DoS-) aanvallen mogelijk is.
07 Implementeer Intrusion Detection Systemen (IDS) of Intrusion Prevention Systemen (IPS).
08 Richt de IDS'en en IPS'en in op basis van een geaccordeerd inrichtingsdocument/ontwerp.
09 Houd rapportage(tool)s beschikbaar voor analyses van de door detectiemechanismen vastgelegde gegevens.

Beveiligingsrichtlijn U/NW.05

Beheer- en productieomgeving

Richtlijn (wie en wat)
Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd.

Doelstelling (waarom)
Het voorkomen van misbruik van de beheervoorzieningen vanaf het internet.

Classificatie
Hoog

Richtlijn 2012
B1-2

Maatregelen

01 Geef in een inrichtingsdocument aan op welke wijze contentbeheer (web- en database-content), applicatiebeheer en technisch beheer worden uitgeoefend.
02 Stel een overzicht op van de ontsluiting van storage en de aansluiting op een back-upinfrastructuur.
03 Stel een overzicht op van ondersteunende communicatieprotocollen voor beheer.
04 Stel een overzicht op van ondersteunende applicaties voor beheer.
05 Leg vast op welke wijze beheerders toegang krijgen tot de beheeromgeving.

Beveiligingsrichtlijn U/NW.06

Hardening van netwerken

Richtlijn (wie en wat)
Voor het configureren van netwerken is een hardeningrichtlijn beschikbaar.

Doelstelling (waarom)
Beperken van het netwerkverkeer tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.

Classificatie
Hoog

Richtlijn 2012
Bo-5

Maatregelen

01 Houd een actueel overzicht bij van de noodzakelijke netwerkprotocollen, -poorten en -services.
02 Schakel op de netwerkcomponenten alle netwerkprotocollen, -poorten en –services uit, behalve de noodzakelijke.
03 Pas de (beveiligings)configuraties van netwerkprotocollen, -poorten en -services op de netwerkcomponenten aan conform richtlijnen.
04 Wijs op switches netwerkpoorten toe aan Virtual LANs (VLANs) op basis van het MAC-adres van de aangesloten systemen (port security).

Beveiligingsrichtlijn U/NW.07

Netwerktoegang tot webapplicatie

Richtlijn (wie en wat)
De opzet van het netwerk garandeert dat alle gebruikers langs dezelfde netwerkpaden toegang krijgen tot webapplicaties, ongeacht hun fysieke locatie.

Doelstelling (waarom)
Voorkom (nieuwe) beveiligingsrisico's omdat de webapplicaties ook bereikbaar moeten zijn vanaf het interne netwerk voor gebruikers binnen de organisatie.

Classificatie
Hoog

Richtlijn 2012
B1-3

Maatregelen

01 Bied gebruikers slechts één netwerkpad om een webapplicatie te bereiken.

Beveiligingsrichtlijn U/NW.08

Netwerkarchitectuur

Richtlijn (wie en wat)
Voor het implementeren, integreren en onderhouden van netwerken zijn architectuurvoorschriften, beveiligingsvoorschriften en de benodigde documentatie beschikbaar.

Doelstelling (waarom)
Een netwerklandschap bieden dat een betrouwbare verwerking garandeert.

Classificatie
Hoog

Richtlijn 2012
-

Maatregelen

01 Onderhoud architectuurvoorschriften actief.
02 Stel hardeningrichtlijnen op voor netwerken, aantoonbaar afgeleid uit de architectuur.
03 Stel inrichtingsrichtlijnen op voor registratie van beveiligingsevents (logging) , aantoonbaar afgeleid uit de architectuur.
04 Stel inrichtingsrichtlijnen op voor de restricties van faciliteiten/utilities en de uitschakeling van features en poorten van netwerkcomponenten.
05 Stel richtlijnen op voor periodieke security-updates, herstelbaarheid van netwerkcomponenten en bescherming (van de stroomvoorziening) van kritieke netwerkcomponenten (zoals UPS/no-breaks voor de stroomvoorziening op de core-switches).
06 Documenteer de plaatsing van servers en aansluitingen van interne netwerkcomponenten en netwerkkoppelingen met externe netwerken.

Beheersingsdomein (control)

Doelstelling

De doelstelling van het beheersingsdomein is er voor te zorgen en/of vast te stellen dat:

» de webapplicatie-omgeving afdoende is ingericht voor het leveren van het gewenste niveau van webapplicatie-diensten,
» het juiste beveiligingsniveau van technische componenten op de lagen toegangsvoorziening, webapplicatie, platformen en webservers en netwerken wordt gegarandeerd.

Risico's

Door het ontbreken van noodzakelijke maatregelen binnen het beheersingsdomein is het niet zeker dat de webapplicatie-omgeving blijvend aan de beoogde beveiligingsvoorwaarden voldoet en dat de governance van die omgeving toereikend is ingericht.

Beveiligingsrichtlijn C.01

Servicemanagementbeleid

Richtlijn (wie en wat)
Het servicemanagementbeleid formuleert richtlijnen voor beheerprocessen, controleactiviteiten en rapportages ten behoeve van het beheer van ICT-diensten.

Doelstelling (waarom)
Effectieve beheersing, door samenhangende inrichting van processen en controle hierover door middel van registratie, statusmeting, monitoring, analyse, rapportage en evaluatie.

Classificatie
Midden

Richtlijn 2012
-

Maatregelen

01 Stel richtlijnen op voor de inrichting van de servicemanagementorganisatie.
02 Stel een beschrijving op van de relevante beheerprocessen.
03 Richt de processen in conform een vastgestelde cyclus.
04 Gebruik geautomatiseerde middelen voor effectieve ondersteuning van beheerprocessen.
05 Stel richtlijnen op voor het uitvoeren van registratie, statusmeting, monitoring, analyse, rapportage en evaluatie.
06 Stel richtlijnen op voor het uitvoeren van controle-activiteiten ten aanzien van identiteit en toegangsbeheer, webapplicatie, platformen en webservers en netwerken.
07 Stel richtlijnen op voor het evalueren van de organisatie, kwaliteit, effectiviteit, borging en informatievoorziening van de beheerprocessen.
08 Leg de taken, verantwoordelijkheden en bevoegdheden (TVB's) van beheerders vast.
09 Leg de relaties met ketenpartijen vast.

Beveiligingsrichtlijn C.02

Compliancemanagement

Richtlijn (wie en wat)
De inrichting en de beveiliging van de webapplicaties (scope) wordt procesmatig en procedureel gecontroleerd (compliance-checks) op basis van vastgestelde beveiligingsrichtlijnen en een vastgestelde webapplicatie-architectuur.

Doelstelling (waarom)
Vaststellen in hoeverre de implementatie van de webapplicatie voldoet aan de vooraf vastgestelde beveiligingsrichtlijnen en geldende wet- en regelgeving.

Classificatie
Midden

Richtlijn 2012
Bo-10

Maatregelen

01 Zorg voor een beschrijving van de webapplicatie-omgeving, waarin de configuratie-elementen genoemd worden.
02 Stel een planning op voor de reguliere policycompliancechecks ten aanzien van de webapplicatie-omgeving.
03 Registreer de uitvoering van en rapporteer over de resultaten van de periodieke policycompliancechecks.
04 Communiceer de rapportages met verbetervoorstellen met verantwoordelijken over de afwijkingen.
05 Beleg implementatieacties en stel uitvoerings- of systeemdocumenten beschikbaar waaruit blijkt dat de verbetervoorstellen zijn geïmplementeerd.

Beveiligingsrichtlijn C.03

Vulnerability-assessments

Richtlijn (wie en wat)
Vulnerability assessments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie (scope).

Doelstelling (waarom)
Identificeren van de kwetsbaarheden en zwakheden in de ICT-componenten van de web applicatie zodat tijdig de juiste beschermende maatregelen kunnen worden getroffen.

Classificatie
Hoog

Richtlijn 2012
Bo-9

Maatregelen

01 Stel een planning op voor het uitvoeren van reguliere vulnerability assessment van de webapplicatie-omgeving.
02 Registreer de uitvoering van de vulnerability assessments.
03 Stel rapportages op met de resultaten van de vulnerability assessments.
04 Communiceer de rapportages met verbetervoorstellen met verantwoordelijken/eigenaren van systemen waarin kwetsbaarheden en zwakheden gevonden zijn.
05 Beleg implementatieacties en stel uitvoerings- of systeemdocumenten beschikbaar waaruit blijkt dat de verbetervoorstellen zijn geïmplementeerd.
06 Zorg voor een actueel overzicht van te onderzoeken componenten, zoals webapplicaties, webservers, netwerk(componenten) en ip-adressen.
07 Stel een overzicht op van kwaliteitseisen en –criteria waarover gerapporteerd moet worden.

Beveiligingsrichtlijn C.04

Penetratietestproces

Richtlijn (wie en wat)
Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope).

Doelstelling (waarom)
Het verkrijgen van inzicht in de weerstand die een webapplicatie kan bieden aan pogingen om het te compromitteren (binnendringen of misbruiken van webapplicatie).

Classificatie
Hoog

Richtlijn 2012
Bo-8

Maatregelen

01 Plan het uitvoeren van reguliere penetratietests van de webapplicatie inclusief de infrastructuur waarop deze draait.
02 Registreer de uitvoering van de penetratietest.
03 Rapporteer over de resultaten van de penetratietest.
04 Communiceer de rapportages met verbetervoorstellen met verantwoordelijken/eigenaren van systemen waarin kwetsbaarheden en zwakheden gevonden zijn.
05 Beleg implementatie-acties en stel uitvoerings- of systeemdocumenten beschikbaar waaruit blijkt dat de verbetervoorstellen zijn geïmplementeerd.
06 Definieer het object van onderzoek in een scopedefinitie.
07 Stem de opdracht af met en accordeer deze door een voldoende gemandateerde vertegenwoordiger.
08 Zorg voor een vrijwaringsverklaring voor penetratietesters, met eventuele beperkingen beschikbaar.

Beveiligingsrichtlijn C.05

Technische controlefunctie

Richtlijn (wie en wat)
De functionaris verantwoordelijk voor de technische controlefunctie van de webapplicaties voert periodiek (technische) evaluaties van de beveiligingsfunctionaliteit van de webapplicaties uit.

Doelstelling (waarom)
Het vaststellen van de juiste werking van de webapplicaties en het tijdig signaleren van afwijkingen/kwetsbaarheden.

Classificatie
Midden

Richtlijn 2012
B3-14, B3-15

Maatregelen

01 Voer periodiek reviews of geautomatiseerde scans op de volledige broncode uit.
02 Voer periodieke (blackbox-)scans uit, waarbij de volledige functionaliteit van de webapplicatie geraakt wordt.

Beveiligingsrichtlijn C.06

Logging

Richtlijn (wie en wat)
In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht.

Doelstelling (waarom)
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.

Classificatie
Hoog

Richtlijn 2012
B7-1, B7-2, B7-4, B7-5, B7-6, B7-7

01 Bepaal welke gebeurtenissen en/of beheeractiviteiten aan de webapplicatie vastgelegd moeten worden.
02 Detecteer aanvallen met detectiesystemen in de webapplicatie-infrastructuur.
03 Leg in de ontwerp- of configuratiedocumentatie vast waar en hoe centralisering van logging is ingericht (inclusief configuratie-instellingen).
04 Configureer de systemen zodanig dat interne systeemklokken automatisch gesynchroniseerd worden.
05 Bepaal vooraf wat te doen bij het uitvallen van loggingmechanismen (alternatieve paden).
06 Stel de (online of offline) bewaartermijn voor logging vast en laat dit tot uitdrukking komen in de configuratie-instellingen van de systemen.
07 Bescherm de loggegevens tegen toegang door onbevoegden beveilig deze tegen achteraf wijzigen/verwijderen.

Beveiligingsrichtlijn C.07

Monitoring

Richtlijn (wie en wat)
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 (waarom)
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.

Classificatie
Hoog

Richtlijn 2012
B7-3, B7-8, B7-9

Maatregelen

01 Breng de door verschillende beheerdisciplines gelogde informatie samen voor analysedoeleinden.
02 Laat de signaleringssystemen (detectie) tijdig melding maken van ongewenste gebeurtenissen.
03 Voer periodiek actief controles uit 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.
04 Voer periodiek reviews uit van toegangslogs.
05 Analyseer de verzamelde loggingsinformatie in samenhang.
06 Analyseer periodiek de geregistreerde menselijke en systeemacties.
07 Analyseer periodiek op ongebruikelijke situaties (incidenten) die de werking van webapplicaties kunnen beïnvloeden.
08 Rapporteer periodiek de geanalyseerde en beoordeelde gelogde gegevens aan de systeemeigenaren en/of aan het management.
09 Analyseer en evalueer de rapportages uit de beheerdisciplines compliancemanagement, vulnerability assessment, penetratietest en logging en monitoring op aanwezigheid van structurele risico's.
10 Geef aantoonbaar opvolging en voer verbeteringen door indien logrecords op misbruik duiden, geïmplementeerde maatregelen niet voldoen aan de gestelde eisen of verwachtingen, of tekortkomingen opleveren.
11 Actualiseer beveiligingsplannen en wijs verantwoordelijken toe voor het realiseren van (delen) van het beveiligingsplan op basis van de geconsolideerde rapportages.

Beveiligingsrichtlijn C.08

Wijzigingenbeheer

Richtlijn (wie en wat)
Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.

Doelstelling (waarom)
Zekerstellen dat wijzigingen op een correcte en gecontroleerde wijze worden doorgevoerd waardoor de veilige werking van ICT-voorziening wordt gegarandeerd.

Classificatie
Hoog

Richtlijn 2012
Bo-6

Maatregelen

01 Laat wijzigingen systematische processtappen doorlopen, zoals intake, acceptatie, impactanalyse, prioritering en planning, uitvoering, bewaking en afsluiting.
02 Laat alle wijzigingsverzoeken verlopen volgens een formele wijzigingsprocedure (voorkomen van ongeautoriseerde

wijzigingen) en OTAP-procedures.
03 Sluit functioneel beheer aan op het generiek proces van wijzigingenbeheer.
04 Lever (beheer)documentatie van wijzigingen op conform vastgestelde eisen.
05 Stel wijzigingsprocedures op voor hardware, software en parameterinstellingen (configuratie).
06 Richt configuratiebeheer in en geef daarmee inzicht in gegevens van de kritieke systemen en applicaties.
07 Registreer en neem wijzigingen binnen een afgesproken tijdslimiet in behandeling op een gestructureerde wijze.
08 Neem alleen geautoriseerde wijzigingsverzoeken (Request for Change (RFC)) in behandeling.
09 Neem autorisatie van doorvoeren van wijzigingen in de verschillende OTAP-omgevingen op in het proces van wijzigingenbeheer.
10 Test alle wijzigingen altijd eerst voordat deze in productie worden genomen en neem ze via vastgestelde wijzigings- en releaseprocedures in productie.
11 Scheid ontwikkel, test en acceptatievoorzieningen van productievoorzieningen (OTAP).
12 Audit de productieomgeving op ongeautoriseerde wijzigingen.

Beveiligingsrichtlijn C.09

Patchmanagement

Richtlijn (wie en wat)
Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings) patches tijdig zijn geïnstalleerd in de ICT-voorzieningen.

Doelstelling (waarom)
Zekerstellen dat technische en software kwetsbaarheden tijdig en effectief worden aangepakt en zo een stabiele omgeving wordt gecreëerd.

Classificatie
Hoog

Richtlijn 2012
Bo-7

Maatregelen

01 Beschrijf het patchmanagementproces en laat het goedkeuren door het management en toekennen aan een verantwoordelijke functionaris.
02 Voorzie alle ICT-componenten van de meest recente, relevante patches.
03 Stel de rollen en verantwoordelijkheden voor patchmanagement vast.
04 Voer registratie over de verworven patches, hun relevantie, besluit tot wel/niet uitvoeren, datum patch-test, resultaat patch-test, datum uitvoeren patch en patch-resultaat.
05 Stel een patchrichtlijn op voor de ondersteuning van patchactiviteiten die op het juiste (organisatorische) niveau is vastgesteld en is geaccordeerd.

Beveiligingsrichtlijn C.10

Beschikbaarheidbeheer

Richtlijn (wie en wat)
Beschikbaarheidbeheer wordt is procesmatig ingericht, zodat bij calamiteiten de webapplicaties binnen de gestelde termijn wordt hersteld en voortgezet.

Doelstelling (waarom)
Waarborgen van beschikbaarheid van informatieverwerkende systemen of webapplicaties.

Classificatie
Hoog

Richtlijn 2012
Bo-11

Maatregelen

01 Beschrijf het beschikbaarheidbeheerproces en laat het goedkeuren door het management en toekennen aan een verantwoordelijke functionaris.
02 Documenteer de back-up- en herstelprocessen en -procedures voor de hele webapplicatie-omgeving.
03 Stel een beschikbaarheidsplan op, met daarin beschikbaarheidseisen per systeem, activiteiten, rollen en verantwoordelijkheden, uit te voeren validaties en escalatiepaden.
04 Test en evalueer het beschikbaarheidplan periodiek.
05 Stel hersteltijden van webapplicaties vast.

Beveiligingsrichtlijn C.11

Configuratiebeheer

Richtlijn (wie en wat)
Het configuratiebeheer is procesmatig ingericht en zorgt ervoor dat slechts operationele websites in gebruik zijn.

Doelstelling (waarom)
Het voorkomen van misbruik van ‘oude’ en niet meer gebruikte websites en/of informatie.

Classificatie
Hoog

Richtlijn 2012
Bo-4, Bo-13

Maatregelen

01 Neem websites conform wijzigingsbeheerprocessen in productie.
02 Voer periodiek controles uit of de operationele websites nog worden gebruikt of informatie bevatten die kan worden verwijderd.
03 Houd een overzichtslijst bij van de websites die operationeel zijn inclusief de daarbij vermelde eigenaren.

Bijlagen

BIJLAGE A
» AFKORTINGEN

A	**ACL**	Access Control List
	AD	Active Directory
	ADH	Anonymous Diffie-Hellman
	Ajax	Asynchronous JavaScript and XML
	API	Application Programming Interface
	APIDS	Application-based Intrusion Detection System
	ASVS	Application Security Verification Standard
B	**BGP**	Border Gateway Protocol
	BREIN	Bescherming Rechten Entertainment Industrie Nederland
	BSN	Burgerservicenummer
C	**CA**	Certification Authority
	CDP	Cisco Discovery Protocol
	CIS	Center for Internet Security
	CMDB	Configuration Management Database
	CMS	Content Management System
	CP	Certificate Policy
	CPS	Certification Practice Statement
	CPU	Central Processing Unit
	CSRF	Cross-Site Request Forgery
	CRL	Certificate Revocation List
	CSS	Cascading Style Sheet
D	**DAC**	Discretionary Access Control
	DBA	Database Administrator
	(D)DoS	(Distributed) Denial-of-Service
	DHCP	Dynamic Host Configuration Protocol
	DMZ	Demilitarised Zone
	DN	Distinguished Name
	DNO	Diensten Niveau Overeenkomst
	DNS	Domain Name Services
	DNSSEC	DNS Security Extensions
	DOM	Document Object Model
	(D)DoS	(distributed) Denial-of-Service
	DRP	Disaster Recovery Plan
E	**EPFW**	End-Point Firewall
	ESAPI	Enterprise Security Application Programming Interface

	EV SSL	Extended Validation SSL (Certificates)
F	**FTP**	File Transfer Protocol
	FTPS	FTP over SSL
G	**GIAC**	Global Information Assurance Certification
	GID	Group Identifier
	GPO	Group Policy Object
	GSLB	Global Server Load Balancing
H	**HIDS**	Host-based Intrusion Detection System
	HTML	Hypertext Markup Language
	HTTP	Hypertext Transfer Protocol
	HTTPS	Hypertext Transfer Protocol Secure
	HSM	hardware security module
I	**IAAS**	Infrastructure-as-a-service
	I&AM	Identity and Access Management
	IANA	Internet Assigned Numbers Authority
	IDMS	Intelligent DDoS Mitigation System
	IDS	Intrusion Detection System
	IIS	Internet Information Services/Server
	IM	Instant Messaging
	IP	Internet Protocol
	IPS	Intrusion Prevention System
	ISAPI	Internet Server Application Program Interface
	ISP	Internet Service Provider
	ISS	Internet Security Systems
	ISSA	Information Systems Security Association
J	**JSON**	JavaScript Object Notation
L	**LAN**	Local Area Network
	LDAP	Lightweight Directory Access Protocol
	LSLB	Local Server Load Balancing
M	**MAC**	Mandatory Access Control
	MAC	Media Access Control
	MTA	Mail Transfer Agent
	MTU	Maximum Transmission Unit
N	**NAT**	Network Address Translation
	NCSC	Nationaal Cyber Security Centrum
	NetBIOS	Network Basic Input Output System
	NetBT	NetBIOS over TCP/IP
	NIDS	Network-based Intrusion Detection System
	NORA	Nederlandse Overheid Referentie Architectuur

	NTP	Network Time Protocol
O	**OASIS**	Organization for the Advancement of Structured Information Stand-ards
	OODA	Observe-Orient-Do-Act
	OS	Operating System
	OSI	Open System Interconnection
	OSPF	Open Shortest Path First
	OTAP	Ontwikkel, Test, Acceptatie en Productie
	OWA	Outlook Web Access
	OWASP	Open Web Application Security Project
P	**PAAS**	Platform-as-a-service
	PDCA	Plan-Do-Check-Act
	PFW	Perimeter Firewall
	PHP	PHP: Hypertext Preprocessor
	PKI	Public-Key Infrastructure
	PL/SQL	Procedural Language/Structured Query Language
	POP	Post Office Protocol
	PVIB	Platform voor Informatiebeveiliging
R	**RA**	Registration Authority
	RBAC	Role-based Access Control
	RBW	Raamwerk Beveiliging Webapplicaties
	RDP	Remote Desktop Protocol
	REST	Representational State Transfer
	RFC	Request For Comments
	RFC	Request for Change
	RFI	Remote File Inclusion
	RP	Reverse Proxy
	RSS	Really Simple Syndication (RSS 2.0)
	RSS	Rich Site Summary (RSS 0.91 en RSS 1.0)
	RSS	RDF Site Summary (RSS 0.9 en 1.0)
	RTBH	Remotely-Triggered Black Hole
S	**SAAS**	Software-as-a-service
	SAML	Security Assertion Markup Language
	SANS	SysAdmin, Audit, Network, Security
	SCP	Secure Copy
	SFTP	SSH File Transfer Protocol
	SIRT	Security Incident Response Team
	SIVA	Structuur, Inhoud, Vorm, Analysevolgorde (audit-methodiek)
	SLA	Service Level Agreement
	SMTP	Simple Mail Transfer Protocol
	SN	Serial Number
	SNMP	Simple Network Management Protocol
	SOAP	Simple Object Access Protocol
	SPoF	Single Point-of-Failure
	SQL	Structured Query Language
	SSD	Secure Software Development
	SSH	Secure Shell
	SSL	Secure Sockets Layer

	SSO	Single Sign-On/Single Sign-Out
	STP	Spanning Tree Protocol
T	**TCP**	Transport Control Protocol
	TFTP	Trivial File Transfer Protocol
	TLS	Transport Layer Security
	TTL	Time-To-Live
U	**UDP**	User Datagram Protocol
	UID	User Identifier
	URL	Uniform Resource Locator
	uRPF	Unicast Reverse-Path-Forwarding
V	**VA**	Vulnerability Assessment
	VLAN	Virtual LAN
	VoIP	Voice over IP
	VPN	Virtual Private Network
W	**WAF**	Web Application Firewall
	WAS	Web Application Scanner
	WASC	Web Application Security Consortium
	Wbp	Wet bescherming persoonsgegevens
	Wcc	Wet computercriminaliteit
	WebDAV	Web-based Distributed Authoring and Versioning
	WEH	Wet Elektronische Handtekeningen
	WSDL	Web Service Description Language
	WS-Trust	Web Services Trust
	WSUS	Windows Server Update Services
X	**XML**	eXtensible Markup Language
	XSRF	Zie CSRF
	XSS	Cross-Site Scripting

BIJLAGE B
» REFERENTIES

Nr.	Omschrijving
[1]	NCSC ‘Raamwerk Beveiliging Webapplicaties’, versie 2.0, de dato 4 november 2010 https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/raamwerk-beveiliging-webapplicaties.html
[2]	OWASP Top 10 Application Security Risks – 2013 https://www.owasp.org/index.php/Top_10_2013
[3]	OWASP Testing Guide v3, de dato 2 november 2008 https://www.owasp.org/index.php/OWASP_Testing_Guide_v3_Table_of_Contents
[4]	OWASP Code Review Guide https://www.owasp.org/index.php/OWASP_Code_Review_Guide_Table_of_Contents
[5]	OWASP Application Security Verification Standard (ASVS) http://code.google.com/p/owasp-asvs/wiki/ASVS
[6]	NEN-ISO/IEC 27001:2013 ‘Managementsystemen voor informatiebeveiliging’ http://www.nen.nl/NEN-Shop/Norm/NENISOIEC-270012013-en.htm
[7]	NEN-ISO/IEC 27002:2013 ‘Praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging’ http://www.nen.nl/NEN-Shop/Norm/NENISOIEC-270022013-en.htm
[8]	NEN-ISO/IEC 27005:2011 ‘Information security risk management’ http://www.nen.nl/NEN-Shop/Norm/NENISOIEC-270052011-en.htm
[9]	Basisnormen Beveiliging en Beheer ICT-infrastructuur Deze norm is uitgegeven door het Platform voor InformatieBeveiliging (PVIB) in 2003, ISBN 90-5931-228-7.
[10]	NORA Dossier Informatiebeveiliging, versie 1.3 http://e-overheid.nl/onderwerpen/architectuur-en-nora/982-dossier-informatiebeveiliging
[11]	NCSC whitepaper ‘Cloudcomputing’, versie 1.0, de dato 19 december 2011 https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/whitepaper-cloudcomputing.html
[12]	NCSC whitepaper ‘Aanbevelingen ter bescherming tegen Denial-of-Service-aanvallen’, versie 1.1, de dato 20 november 2006 https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/bescherming-tegen-ddos-aanvallen.html
[13]	NCSC whitepaper “Patchmanagement”, versie 1.1, de dato 30 juni 2008 https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/patchmanagement.html
[14]	CWE/SANS Top 25 Software Errors http://cwe.mitre.org/top25/

Overige referenties/bronnen/literatuur waar gebruik van is gemaakt zijn:

» Wikipedia – 'Gebruiker' , 'Gebruikersnaam' en 'Gebruikersgroep'
» Logius: Gebruiksvoorwaarden DigiD - https://www.digid.nl/voorwaarden/
» Ehow: Dynamic Separation of Duties - http://www.ehow.com/info_8671842_dynamic-separation-duties.html
» SANS: Role Based Access Control to Achieve Defense in Depth - http://www.sans.edu/research/security-laboratory/article/311
» NGI: Taken, Functies, Rollen en Competenties in de Informatica, Den Haag 2001 - https://www.ngi.nl/TakenEnFuncties/Takenfunctiesrollen_en_competenties.pdf
» Platform Informatiebeveiliging Studie Role Based Access Control, Versie 1.0, November 2005 - http://www.pvib.nl/download/?id=6391714&download=1
» Feisty Duck Limited – 'OpenSSL Cookbook', Version 1.1, de dato October 2013 - https://www.feistyduck.com/library/openssl-cookbook/
» Qualys SSL Labs – 'SSL/TLS Deployment Best Practices', version 1.3, de dato 17 September 2013 - https://www.ssllabs.com/downloads/SSL_TLS_Deployment_Best_Practices_1.3.pdf
» Qualys SSL Test - https://www.ssllabs.com/ssltest/

Deze beveiligingsrichtlijnen zijn tot stand gekomen in een publiek-private samenwerking mede door waardevolle inbreng van de volgende deskundigen:

Eric Nieuwland (Inspearit)
John van Huijgevoort (NCSC)
Michiel Oosterwijk (NCSC)
Koen Sandbrink (NCSC)
Wiekram Tewarie (UWV)

BIJLAGE C
» RELATIE VERSIE 2012 EN 2015

Beveiligingslaag 2012	Richtlijn 2012	Richtlijn 2015	Maatregelen
Algemeen	B0-1	B.01	01 02
	B0-2	B.03	01 02 03 04
	B0-3	B.06	04 05
	B0-4	C.11	01 03
	B0-5[22]	C.08	01 02 05 06 07 08 09 10 11 12
	B0-6[22]	U/PW.07	01 02 03 04 05
		U/NW.06	01 02 03 04
	B0-7	C.09	01 02 03 04
	B0-8	C.04	01 02 03 04 05 06 07
	B0-9	C.03	01 03 05
	B0-10	C.02	01 02 03 04 05
	B0-11	C.10	02 05
	B0-12	B.02	01 02 04 05 06 07 08 09 10
		U/TV.01	01 02 03 04 05 06 08 11
	B0-13	C.11	02 03
	B0-14	B.05	01 02
Netwerk	B1-1	U/NW.03	06 07
	B1-2	U/NW.03	06
		U/NW.05	03 04 05
	B1-3	U/NW.07	01
	B1-4	U/NW.03	03 04 06
	B1-5	U/NW.04	02 03 05 06
	B1-6	U/NW.02	02
Platform	B2-1	U/PW.05	01 02
	B2-2	U/PW.01	01
	B2-3	U/PW.04	01 02
	B2-4	U/PW.06	01 02

22 In de versie 2012 zijn richtlijnen B0-5 en B0-6 in deel 1 per abuis omgekeerd beschreven ten opzichte van deel 2. In deze tabel wordt uitgegaan van de volgorde zoals in deel 1.

Beveiligingslaag 2012	Richtlijn 2012	Richtlijn 2015	Maatregelen
Applicatie	B3-1	U/WA.03	04
	B3-2	U/PW.02	02
	B3-3	U/WA.03	03
	B3-4	U/WA.04	01
	B3-5	U/WA.07	01 02
	B3-6	U/WA.03	01
	B3-7	U/WA.03	02
	B3-8	U/PW.02	04
	B3-9	U/PW.02	05
	B3-10	U/PW.02	06
	B3-11	U/WA.06	01
	B3-12	U/PW.02	03
	B3-13	U/PW.03	02
	B3-14	C.05	01
	B3-15	C.05	02
	B3-16	U/PW.03	03
Identiteit	B4-1	U/TV.01	11
	B4-2	U/WA.08	02 03 04 05
Vertrouwelijkheid	B5-1	B.04	01 02 03 04
	B5-2	U/WA.05	05
	B5-3	U/WA.05	03
	B5-4	U/WA.05	04
	B5-5	U/WA.05	06
	B5-6	-	
	B5-7	B.04	01
Integratie	B6-1	B.06	04 05 09
Monitoring	B7-1	U/NW.04	07 08 09
		C.06	02
	B7-2	C.06	03
	B7-3	C.07	01 05
	B7-4	C.06	04
	B7-5	C.06	05
	B7-6	C.06	06
	B7-7	C.06	07
	B7-8	C.07	02 03 04
	B7-9	C.07	08 09 10 11

Nationaal Cyber Security Centrum
Turfmarkt 147 | 2511 DP Den Haag
Postbus 117 | 2501 CC Den Haag
T 070-751 55 55
www.ncsc.nl | info@ncsc.nl

September 2015