Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

ICT-Beveiligingsrichtlijnen voor webapplicaties

Deel 2

ICT-beveiligingsrichtlijnen voor webapplicaties

Deel 2

Nationaal Cyber Security Centrum
Wilhelmina van Pruisenweg 104 | 2595 AN Den Haag
Postbus 117 | 2501 CC Den Haag

T 070-888 75 55
F 070-888 75 50

E info@ncsc.nl
I www.ncsc.nl

Januari 2012

Nationaal Cyber Security Centrum
Het Nationaal Cyber Security Centrum (NCSC) draagt via samenwerking tussen bedrijfsleven, overheid en wetenschap bij aan het vergroten van de weerbaarheid van de Nederlandse samenleving in het digitale domein.

Het NCSC ondersteunt de Rijksoverheid en organisaties met een vitale functie in de samenleving met het geven van expertise en advies, response op dreigingen en het versterken van de crisisbeheersing. Daarnaast voorziet het in informatie en advies voor burger, overheid en bedrijfsleven ten behoeve van bewustwording en preventie.
Het NCSC is daarmee het centrale meld- en informatiepunt voor ICT-dreigingen en -veiligheidsincidenten.

VOORWOORD

Dit is deel 2 van de ICT beveiligingsrichtlijnen voor webapplicaties. In dit deel worden voor de beveiligingsrichtlijnen uit deel 1 de maatregelen voorgesteld met aanbevelingen en implementatievoorstellen.

Het aanbieden van diensten via internet, door zowel de private als publieke organisaties is vandaag de dag meer standaard dan uitzondering. Deze diensten staan dan ook veelvuldig in de belangstelling van kwaadwillende, die vaak met verschillende intenties een bedreiging kunnen vormen voor de aangeboden dienst.

Naast het wegvallen van de dienstverlening en/of de bijbehorende financiële schade, kan een verstoring een ketenimpact hebben bij klanten, mededienstverleners en/of leveranciers. Goede afspraken rond kenmerken als vertrouwen, continuïteit, het nakomen van wettelijke verplichtingen en adequate reactie bij incidenten zijn daardoor belangrijk.

De *ICT-Beveiligingsrichtlijnen voor webapplicaties* (deel 1 en 2) biedt een organisatie een leidraad, door het toepassen van de bewezen maatregelen, tot het veiliger ontwikkelen, beheren en aanbieden van webapplicaties en diensten.

De Richtlijnen in dit document, zijn door hun opzet, breed toepasbaar voor ICT-oplossingen (die gebruik maken van webapplicaties) en kunnen daardoor zowel door afnemers als door dienstaanbieders worden gebruikt in aan- en uitbestedingen, toezicht en onderlinge afspraken. De maatregelen die in deel 2 worden aangereikt zijn mede tot stand gekomen aan de hand van best-practices van het NCSC[1] in samenwerking met Rijksauditdienst (RAD), Logius, OWASP Nederland, Kwaliteitsinstituut Nederlandse Gemeenten (KING), Belastingdienst, diverse gemeenten en marktpartijen.

Omdat niet elke organisatie gelijk is, denk aan de te verdedigen belangen, regelgeving, inrichting en te verwachten bedreigingen, is het wenselijk om via een eigen risicoanalyse de maatregelen te toetsen en na risicoafweging en voldoende onderbouwing in prioriteit te verhogen of te verlagen.

De Richtlijnen in beide documenten zijn een eerste aanzet voor het veiliger maken van webapplicaties en bijbehorende infrastructuur. De beveiligingsrichtlijnen zullen jaarlijks door het NCSC worden aangepast. Daarnaast is het raadzaam om opvolging te geven aan patch- en security-adviezen van het NCSC en de soft- en hardwareleveranciers.

Het document 'ICT-beveiligingsrichtlijnen Deel 1' bevat een beschrijving van de beveiligingsrichtlijnen op hoofdlijnen. In deel 2 worden de maatregelen verder uitgewerkt en gedetailleerd met voorstellen voor inrichting, beheer en ontwikkeling.

Elly van den Heuvel

Waarnemend Hoofd Nationaal Cyber Security Centrum

1. De 'ICT-beveiligingsrichtlijnen voor webapplicaties' (de beveiligingsrichtlijnen) is mede gebaseerd op het 'Raamwerk Beveiliging webapplicaties (RBW)' van GOVCERT.NL. GOVCERT.NL is per 1 januari opgegaan in het Nationaal Cyber Security Centrum.

INHOUDSOPGAVE

HOOFDSTUK 1

Inleiding

1.1 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 opgaaf blijkt wel uit het veelvoud van incidenten. De beveiligingsrichtlijnen biedt een leidraad naar een veiliger dienstverlening.

De ICT-beveiligingsrichtlijnen (hierna de Richtlijnen genoemd) bestaat uit twee documenten, die na implementatie, bijdragen aan een betere beveiliging van webapplicaties bij organisaties en de (rijks)overheid. Deel 1 beschrijft de beveiligingsrichtlijnen op hoofdniveau voor webapplicaties, bijbehorend beheer en infrastructuur. Dit document vormt een ondersteunend document en beschrijft de maatregelen op detailniveau. Met deze maatregelen kan worden voldaan aan de beveiligingsrichtlijnen uit deel 1.

1.2 Webapplicaties

Wanneer dit document spreekt over een webapplicatie dan gaat het om een applicatie die bereikbaar is via een webbrowser of via een andere client die ondersteuning biedt voor het Hypertext Transfer Protocol (HTTP). Een dergelijke client noemt men een 'HTTP user agent'. Kern van deze definitie is dat een webapplicatie altijd bereikbaar is op basis van HTTP of de versleutelde vorm hiervan: HTTPS (HTTP Secure). De functionaliteit die een webapplicatie kan bieden, is onbeperkt. De techniek is echter altijd gebaseerd op de HTTP-protocolstandaard zoals gedefinieerd in 'Request for Comments' (RFC) 1945[2], 2068[3], 2616[4], 2617[5] en 2965[6].

Ook bijbehorende infrastructuur, de koppeling met internet, de opslag van de gegevens en de netwerkservices worden in het document beschouwd als aandachtsgebied. Voorbeelden van applicaties, die volgens deze definitie onder de noemer webapplicatie vallen, zijn internetsites, extranetten, intranetten, SaaS-applicaties, webservices en webapi's.

1.3 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 maatregelen 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 standaard een objectieve ICT-beveiligingsassessment uitvoeren.

1.4 Doelstelling

De beveiligingsrichtlijnen geven een overzicht van beveiligingsmaatregelen die webapplicaties moeten nemen om een bepaalde mate van veiligheid te bereiken. De maatregelen 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.

1.5 Toepassing van de beveiligingsrichtlijnen

De beveiligingsrichtlijnen kunnen voor een bepaald toepassingsgebied worden verheven tot een normenkader. In tegenstelling tot de beveiligingsrichtlijnen, die adviserend van aard zijn, is een normenkader dwingend voor het toepassingsgebied. Ook kunnen de beveiligingsrichtlijnen worden gebruikt in aanbestedingen, het uitbesteden van dienstverlening en in onderlinge afspraken bij ketenprocessen. Afhankelijk van de aard en de specifieke kenmerken van de dienst kunnen maatregelen worden weggelaten en/of worden opgenomen en kunnen wegingsfactoren van de individuele maatregelen worden aangepast.

1.6 De mate van gewenstheid

De gewenstheid van elke beveiligingsmaatregel wordt in algemene zin gewaardeerd volgens de classificatie *Hoog*, *Midden* of *Laag*. Deze 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 van gewenstheid voor een specifieke webapplicatie voor een specifiek organisatie is afhankelijk van de weging van risico's die uit de risicoanalyse naar voren komen. Daarbij wordt gekeken naar de kans op optreden van een bedreiging, het te verdedigen belang[7] en de mogelijke impact hiervan op de bedrijfsvoering. De beveiligingsrichtlijnen bieden

2 RFC 1945: Hypertext Transfer Protocol -- HTTP/1.0: http://www.ietf.org/rfc/rfc1945.txt
3 RFC 2068: Hypertext Transfer Protocol -- HTTP/1.1: http://www.ietf.org/rfc/rfc2068.txt
4 RFC 2616: Hypertext Transfer Protocol -- HTTP/1.1: http://www.ietf.org/rfc/rfc2616.txt
5 RFC 2617: HTTP Authentication (Basic and Digest): http://www.ietf.org/rfc/rfc2617.txt
6 RFC 2965: HTTP State Management Mechanism: http://www.ietf.org/rfc/rfc2965.txt
7 Of risk appetite

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 aanpassing van de algemene classificaties in specifieke situaties kan worden gekeken naar beschikbaarheidmaatregelen. De gewenstheid van beschikbaarheidmaatregelen kan bijvoorbeeld laag zijn in situaties waar het onbeschikbaar zijn van een webdienst weinig impact heeft op de bedrijfsvoering. De gewenstheid kan juist hoog zijn in situaties waar de impact en de kans op optreden van een bedreiging groot zijn.

1.7 Uitgangspunten

- De beveiligingsrichtlijnen zijn generiek van opzet en voor breed spectrum van dienstverlening toepasbaar.
- De beveiligingsrichtlijnen richten zich op de drie kenmerkenaspecten van informatiebeveiliging: beschikbaarheid, vertrouwelijkheid en integriteit.
- De beveiligingsrichtlijnen hebben betrekking op webapplicaties en de omgeving waarin ze draaien. 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.
- De beveiligingsrichtlijnen kunnen als (toetsbare) norm worden gebruikt bij aan en uitbestedingen van diensten en onderlinge afspraken.
- De beveiligingsrichtlijnen in deel 1 beschrijven vooral maatregelen op hoog niveau die organisaties kunnen nemen om webapplicaties veiliger te maken.
- Deel 2 beschrijft op detailniveau de (deel) maatregelen en hoe deze geïmplementeerd kunnen worden. Dit deel zal door het technische karakter meer aan verandering onderhevig zijn dan deel 1.

1.8 Context/scope

De beveiligingsrichtlijnen richten zich op de beveiliging van webapplicaties vanuit het oogpunt van de aanbiedende partij (de serverzijde). De beveiligingsrichtlijnen richt zich niet op de client inrichting en infrastructuur van de webdienst[8]. Er zijn daarom geen direct maatregelen in de beveiligingsrichtlijnen terug te vinden op de manier waarop afnemende partijen (de werkstations) veilig gebruik kunnen maken van webapplicaties.

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

De beveiligingsrichtlijnen zijn het uitgangspunt voor de beveiliging van webapplicaties en een organisatie kan de beveiliging van hun webapplicaties (laten) toetsen op basis van deze beveiligingsrichtlijnen. De toetsende organisaties kunnen deze beveiligingsrichtlijnen gebruiken om een objectieve beveiligingsassessment uit te voeren. Bij het beoordelen van een specifieke situatie en bij het implementeren van de beveiligingsrichtlijnen (het oplossen van tekortkomingen) wordt verwezen naar deel 2 van de beveiligingsrichtlijnen.

1.9 Opbouw van de documenten

De twee documenten die de beveiligingsrichtlijnen beschrijven zijn op dezelfde manier opgebouwd. Deel 2 bevat alle informatie die deel 1 ook bevat. Deel 2 bevat echter ook informatie *hoe* aan de beveiligingsrichtlijnen kan worden voldaan.

De beschrijving van de beveiligingsrichtlijnen is te vinden in de hoofdstukken 2 tot en met 10 en worden in de volgende lagen[9], elk in een apart hoofdstuk beschreven:

- 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 lagen vormen een middel om de beveiligingsrichtlijnen in clusters te beschrijven. Zoals op een aantal plekken zal blijken, zijn de lagen in de praktijk niet volledig van elkaar te scheiden en kunnen sommige beveiligingsrichtlijnen in meer dan één laag beschreven worden. Omwille van de overzichtelijkheid worden de eisen niettemin zoveel mogelijk in één laag beschreven.

8 Client beveiliging ligt gezien de diversiteit buiten de scope en worden qua risico geclassificeerd als een niet te beïnvloeden en te vertrouwen factor.

9 De beveiligingsrichtlijnen worden beschreven volgens de lagen uit het 'Raamwerk Beveiliging webapplicaties (RBW)' van GOVCERT.NL

De beveiligingsmaatregelen worden allen volgens hetzelfde format beschreven:

- De nummering in de kolom 'Nr.' is de nummering van beveiligingsrichtlijnen zoals die gelden voor webapplicaties.
- De kolom 'Beschrijving van beveiligingsrichtlijn' geeft een beschrijving van de beveiligingsrichtlijn.
- De kolom 'Doelstelling' beschrijft de doelstelling die met de eis beoogd wordt.

In deel 2 van de beveiligingsrichtlijnen wordt dit uitgebreid met:

- De kolom 'Rationale[10]' geeft een toelichting op de beveiligingsrichtlijn.
- De nummering in de kolom 'Referentie RBW' heeft betrekking op de relevante paragraaf uit het Raamwerk beveiliging webapplicaties (RBW) [12] van het NCSC.
- Vereiste succescriteria (conformiteitvereisten)[11]
- De kolom 'Classificatie'[12] beschrijft de initiële mate van gewenstheid van de beveiligingsrichtlijn. Deze kan in een specifieke situatie aangepast worden als gevolg van een risicoanalyse.
- Bewijsvoering.
- Relatie met andere normen en standaarden.

Een overzicht van alle gebruikte afkortingen en termen staat in bijlage A.

We hebben voor de beveiligingsrichtlijnen een aantal literatuurbronnen geraadpleegd. Op plaatsen waar we informatie uit de literatuurbronnen verwerkt hebben, verwijzen we hiernaar in de vorm van '[x]'. '[x]' verwijst naar een document opgenomen in bijlage B. In bijlage C wordt een overzicht gegeven van de in deze beveiligingsrichtlijnen beschreven aanvalsmethoden. Bijlage D bevat een beschrijving van mogelijke webdiensten die onder het toepassingsgebied van de beveiligingsrichtlijnen vallen.

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.

1.10 Onderhoud van de beveiligingsrichtlijnen

Het NCSC is verantwoordelijk voor het opstellen en onderhouden van de beveiligingsrichtlijnen en zal jaarlijks worden geactualiseerd. Indien noodzakelijk zal het NCSC eerder door middel van een advIsory of een update de beveiligingsrichtlijnen aanpassen.
Aanvullingen, opmerkingen of eigen ervaringen ontvangen wij graag via richtlijnen@ncsc.nl.

1.11 Relatie met andere documenten

De beveiligingsrichtlijnen zijn afgeleid van het 'Raamwerk beveiliging webapplicaties (RBW)' [12] van het NCSC.
In deze eerste versie zijn de beveiligingsmaatregelen uit het RBW nagenoeg één-op-één vertaald naar de beveiligingsrichtlijnen.
Daarnaast wordt in beveiligingsrichtlijnen verwezen naar de volgende relevante normen, standaarden, best practices, zoals:

- OWASP[13] Top 10 2010 [1]
- OWASP Testing Guide 3 [2]
- OWASP Code Review Guide [3]
- OWASP Application Security Verification Standard (ASVS) [4]
- NEN-ISO /IEC 27001 'Managementsystemen voor informatiebeveiliging' [5] [14]
- NEN-ISO /IEC 27002 'Code voor informatiebeveiliging' [6] [15]
- NEN-ISO /IEC 27005 'Information security risk management' [7] [16]
- Basisnormen Beveiliging en Beheer ICT-infrastructuur [8]
- NORA[17] Dossier Informatiebeveiliging [9]

10 Definitie Rationale = idee achter een bepaalde handeling, standpuntbepaling, opstelling (Bron: 'Groot woordenboek van de Nederlandse Taal, 14de editie')
11. Definitie Rationale = idee achter een bepaalde handeling, standpuntbepaling, opstelling (Bron: 'Groot woordenboek van de Nederlandse Taal, 14de editie')
12. Voor een geldige verklaring van conformiteit met de Richtlijn, moeten webapplicaties voldoen aan alle succescriteria voor alle beveiligingsrichtlijnen.
13. Met behulp van het classificatiesysteem worden de maatregelen gewaardeerd.
14. De Open Web Application Security Project (OWASP) is een charitatieve wereldwijde not-profit organisatie 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 27001:2005 nl specificeert eisen voor het vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden 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 'Code voor informatiebeveiliging' geeft richtlijnen en principes voor het initiëren, het implementeren, het onderhouden en het verbeteren van informatiebeveiliging binnen een organisatie.
17. NEN-ISO/IEC 27005 'Information security risk management'geeft richtlijnen voor risicobeheer en ondersteunt de uitvoering van informatiebeveiliging op basis van een risico management aanpak.

HOOFDSTUK 2

Algemene maatregelen

In deze paragraaf worden generieke maatregelen beschreven die niet tot een specifieke laag behoren zoals in het RBW beschreven, maar betrekking hebben op het geheel van de ICT-infrastructuur of generiek zijn voor ICT-componenten.

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B0-1	Algemeen	Informatiebeveiliging is als een proces ingericht.	

Doelstelling

- De effectiviteit van informatiebeveiliging (maatregelen en bijbehorende procedures) waarborgen.
- Aantonen dat aan gestelde maatregelen en verwachtingen wordt voldaan.

Rationale

Informatiebeveiliging is een proces, waarbij maatregelen worden afgestemd en bijgesteld op basis van beleid, risicoanalyses en periodieke controles. Voor het effectueren van informatiebeveiliging dient gewerkt te worden via de Plan Do Check Act (PDCA) cyclus. Door het implementeren van (ondersteunende) processen en uitvoeren van vastgestelde activiteiten moet worden aangetoond dat aan de gestelde beveiligingseisen en verwachtingen wordt voldaan. Nadat de betrouwbaarheidseisen (beschikbaarheid, integriteit en vertrouwelijkheid) zijn vastgesteld, moeten maatregelen zijn getroffen en gecontroleerd worden of die maatregelen het gewenste effect sorteren (controle). Deze controle kan direct aanleiding geven tot bijsturing in de maatregelen. Ook kan het totaal van eisen, maatregelen en controle aan revisie toe zijn (evaluatie). Het goed doorlopen van deze kwaliteitscirkel zorgt op elk moment voor het adequate beveiligingsniveau.

De volgende stappen moeten zijn uitgevoerd om de beveiligingsdoelstellingen en -maatregelen vast te stellen en te documenteren:

- Er moet een informatiebeveiligingsbeleid zijn gedefinieerd en vastgesteld.
- Er moet een passende risicoanalyse zijn uitgevoerd en de resultaten moeten zijn vastgelegd. Bij deze risicoanalyse moeten de bedreigingen voor de bedrijfsmiddelen, kwetsbaarheden en de invloeden op de organisatie zijn vastgesteld en het bijbehorende risiconiveau te zijn bepaald.
- Passende maatregelen moeten zijn geselecteerd en geïmplementeerd en deze selectie moet zijn onderbouwd.
- De effectiviteit van de maatregelen, moet door middel van onderzoek worden geverifieerd. Er moet actie worden ondernomen indien log records op kwaadwillend misbruik duiden, geïmplementeerde maatregelen niet voldoen aan de gestelde eisen of verwachtingen of tekortkomingen opleveren.
- Periodiek moet de compliance aan maatregelen geëvalueerd worden.
- Om bovenstaande te bewerkstelligen worden de gegevens op een efficiënte en effectieve manier verzameld, bewerkt en beheerd.

Vereiste succescriteria (conformiteitvereisten)

- Er is een informatiebeveiligingsproces conform PDCA-cyclus ingericht.
- Het informatiebeveiligingsbeleid is gedefinieerd en vastgesteld.
- Er worden periodiek risicoanalyses uitgevoerd en de resultaten worden vastgelegd en op het juiste organisatorische niveau vastgesteld.
- Er worden periodiek evaluaties uitgevoerd met betrekking tot de effectiviteit van de geselecteerde en geïmplementeerde maatregelen en compliance aan maatregelen. De resultaten worden vastgelegd en op het juiste organisatorische niveau vastgesteld.
- Er moet aantoonbaar follow-up worden gegeven in casu verbeteringen worden doorgevoerd indien log records op kwaadwillend misbruik duiden, geïmplementeerde maatregelen niet voldoen aan de gestelde eisen en/of verwachtingen of tekortkomingen opleveren.
- Verantwoordelijkheden, taken en bevoegdheden op het gebied van de informatiebeveiliging (van de webapplicaties) zijn expliciet belegd.

Classificatie
Hoog

Bewijsvoering
- Een beschrijving van het informatiebeveiligingsproces.
- Het informatiebeveiligingsbeleid.
- De resultaten van de risicoanalyses.
- Procedures voor het uitvoeren van de periodieke controles met betrekking tot de effectiviteit van de geselecteerde en geïmplementeerde maatregelen en compliance aan maatregelen.
- Een planning met daarin opgenomen wanneer, door wie en welke controles worden uitgevoerd.
- De resultaten (rapportages) van de uitgevoerde periodieke controles.
- Plan met daarin de activiteiten die worden uitgevoerd (wie, wat en wanneer) indien log records op kwaadwillend misbruik duiden, geïmplementeerde maatregelen niet aan de gestelde eisen en/of verwachtingen hebben voldaan of tekortkomingen hebben opgeleverd.
- Overzicht met de toegewezen verantwoordelijkheden, taken en bevoegdheden op het gebied van de informatiebeveiliging.

Relatie met andere normen en standaarden
- NEN-ISO /IEC 27001 ‘Managementsystemen voor informatiebeveiliging’

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B0-2	Algemeen	Voer actief risicomnagement uit.	

Doelstelling
- Het bewust komen tot betrouwbaarheidseisen en maatregelen aan de hand van een methodische beoordeling van beveiligingsrisico’s.
- Het periodiek evalueren van de beveiligingsrisico’s en geïmplementeerde maatregelen.

Rationale
De impact van een kwetsbaarheid is zeer afhankelijk van de webapplicatie waarin deze kwetsbaarheid zich bevindt. Het is dan ook belangrijk dat de beveiligingsbehoeften aan de hand van een risicoanalyse worden bepaald. Een risicoanalyse is het systematisch beoordelen van:
- de schade die waarschijnlijk zal ontstaan door een beveiligingsincident als de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie en andere bedrijfsmiddelen worden geschonden.
- de waarschijnlijkheid dat een beveiligingsincident optreedt rekening houdend met de aanwezige bedreigingen, kwetsbaarheden en de getroffen maatregelen.

De resultaten van deze risicoanalyse worden gebruikt om te bepalen welke prioriteiten moeten worden gesteld ten aanzien van het beheer van beveiligingsrisico’s en het implementeren van maatregelen ter bescherming tegen deze risico’s. Deze resultaten worden vastgelegd in een informatiebeveiligingsplan. Dit informatiebeveiligingsplan maakt de noodzakelijke stappen voor het implementeren van maatregelen concreet en beschrijft wie, wanneer en waarvoor verantwoordelijk is. Hierin wordt ook beschreven dat de maatregelen regelmatig, door middel van onderzoek, worden gecontroleerd op werking en naleving van deze Richtlijn (zie ook maatregel B0-3).

Het is belangrijk om de beveiligingsrisico's en geïmplementeerde maatregelen periodiek te evalueren, om:

- in te kunnen spelen op wijzigingen in bedrijfsbehoeften en prioriteiten;
- nieuwe bedreigingen en kwetsbaarheden te bepalen;
- te bevestigen dat maatregelen nog steeds effectief en geschikt zijn.

Vereiste succescriteria (conformiteitvereisten)

- Zorg voor een risicoanalyse methodiek.
- Voer risicoanalyses uit voor iedere (nieuwe) webapplicatie en herhaal deze periodiek.
- Evalueer periodiek de beveiligingsrisico's en geïmplementeerde maatregelen.
- Zorg voor een informatiebeveiligingsplan waarin de onderbouwing en verantwoording van gekozen maatregelen is vastgelegd.

Classificatie

Hoog

Bewijsvoering

- Beschrijving van de risicoanalyse methodiek.
- Resultaten van de uitgevoerde risicoanalyses inclusief de onderbouwing en verantwoording van de gekozen maatregelen (informatiebeveiligingsplan).

Relatie met andere normen en standaarden

- NEN-ISO /IEC 27001 'Managementsystemen voor informatiebeveiliging'
- NEN-ISO /IEC 27002 'Code voor informatiebeveiliging'
  - hoofdstuk 4 'Risicobeoordeling en risicobehandeling'
- NEN-ISO /IEC 27005 'Information security risk management'

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B0-3	Algemeen	Voor elke maatregel wordt documentatie vastgelegd en onderhouden.	3.3.1 en 3.3.7

Doelstelling

- Het behouden van een actueel overzicht van de ICT-infrastructuur (inrichting), zodat inzicht wordt verkregen in de interactie en relaties tussen webapplicaties en andere componenten in de ICT infrastructuur.
- Het herleiden van ontwerp en inrichtingskeuzen naar functionele eisen.
- Het aantonen dat classificatie van vereist beveiligingsniveau in relatie is tot risicoanalyse/ risicomanagement.
- Het aantonen dat aan de maatregelen zoals beschreven in de Richtlijn wordt voldaan.

Rationale

De essentie van het documenteren is dat gemaakte ontwerp en inrichtingskeuzen verantwoord en onderbouwd zijn. Dus niet alleen vastleggen wat de huidige situatie (as-is) is, maar ook waarom deze zo is, dus wat de noodzaak van toepassing is. Om dit gefundeerd te onderbouwen zullen er verwijzingen naar functionele eisen, risicoanalyses, best practices en (mogelijke) alternatieven opgenomen moeten worden. Alle gedocumenteerde ontwerp- en inrichtingskeuzen moeten te herleiden zijn naar functionele eisen. Documentatie speelt ook een (belangrijke) rol bij het bepalen van de impact van wijzigingen en het voorkomen van ontwerpbeslissingen (fouten)[18]. Documentatie moet dan ook na elke wijziging

18. Bij het voorkomen van ontwerpfouten spelen natuurlijk ook nog andere zaken een belangrijke rol zoals de eisen/wensen van de klant, het programma van eisen, het functioneel en technisch ontwerp en de inrichting van kwaliteitsmanagement.

worden bijgewerkt en oude documentatie moet worden gearchiveerd. Dit geldt zowel voor systeem- als gebruikersdocumentatie.
Voor elke maatregel wordt documentatie onderhouden, daarnaast wordt afhankelijk van de gevoeligheid van de webapplicatie regelmatig het bestaan van maatregelen gecontroleerd en gedocumenteerd. De mate van compliance wordt aan de verantwoordelijke voor de webapplicatie en de beveiligingsfunctionaris gerapporteerd[19].
Documentatie moet goed leesbaar zijn, voorzien zijn van een datum (alsmede de revisie-data), een eigenaar hebben, op een ordelijke manier worden onderhouden en gedurende een bepaalde periode worden bewaard. Er moeten procedures en verantwoordelijkheden worden vastgesteld en bijgehouden voor het opstellen en aanpassen van documentatie.
Documentatie kan gevoelige informatie bevatten en er moeten dan ook maatregelen zijn getroffen om de documentatie te beveiligen tegen ongeautoriseerde toegang (inzien en wijzigen).
De set aan documentatie beschrijft onder andere:

- Hoe wordt omgegaan met risicomanagement, de benodigde bedrijfsmiddelen, de geïmplementeerde maatregelen en noodzakelijke mate van zekerheid. Kortom de vastgelegde en vastgesteld procedures en processen.
- De plaatsing van servers en aansluiting van interne netwerkcomponenten en netwerk-koppelingen met externe netwerken zijn duidelijk en schematisch gedocumenteerd, zodat de werking van de ICT-infrastructuur begrijpelijk is en de impact van wijzigingen goed kunnen worden bepaald.
- De (beveiligings)instellingen van de ICT-componenten zijn zodanig gedocumenteerd dat duidelijk is waarom voor bepaalde instellingen gekozen is (verantwoording en onderbouwing). Hierbij wordt speciale aandacht besteed aan de defaultwaarden voor systeeminstellingen.

Vereiste succescriteria (conformiteitvereisten)

- De set aan documentatie bevat minimaal de vastgestelde documenten, zoals opgesomd bij bewijsvoering.
- Er moeten procedures zijn opgesteld en onderhouden voor het beheer van alle documentatie.
- De documenten moeten de verantwoordelijkheden en de relevante activiteiten beschrijven.
- De documenten moeten op een zodanige manier worden bewaard, dat deze leesbaar en makkelijk opvraagbaar zijn.
- De plaatsing van servers en aansluiting van netwerkcomponenten en netwerkkoppe-lingen met in- en externe netwerken zijn duidelijk en schematisch gedocumenteerd, zodat de werking van de ICT-infrastructuur begrijpelijk is en de impact van wijzigingen goed kan worden ingeschat.
- Er bestaat altijd een actueel, juist en volledig overzicht van de (beveiligings)instellingen van ICT-componenten.
- De (beveiligings)instellingen van de ICT-componenten zijn zodanig gedocumenteerd dat duidelijk is waarom voor bepaalde instellingen gekozen is.

Classificatie

Hoog

Bewijsvoering

- De set aan documentatie bevat minimaal de volgende vastgestelde documenten:
  - Een informatiebeveiligingsbeleid, dat door het juiste organisatieniveau is vastgesteld.
  - Een technische beschrijving van de webapplicatie. Denk hierbij aan locatie(s), benodigde bedrijfsmiddelen en gebruikte technologieën.
  - De resultaten van de risicoanalyse.

19. Afhankelijk van de organisatie kan dat de beveiligingsmanager, de Chief/Corporate Information Security Officer (CISO), Information Security Officer (ISO), et cetera zijn

- Een overzicht van de geïmplementeerde maatregelen en bijbehorende onderbouwing.
- De resultaten (rapportages) van de controles op de effectiviteit van de maatregelen en de documentatie/procedures die de beveiligingsmaatregelen beschrijven. Denk hierbij aan een architectuurontwerp, infrastructuurontwerp, firewall ruleset, toegangsautorisaties en audit-documenten.

- Procedures met betrekking tot documentbeheer.
- De documentatie maakt onderdeel uit van het standaard wijzigingsbeheerproces.
- De documentatie voldoet aan de volgende criteria:
  - heeft een eigenaar.
  - is voorzien van een datum en versienummer.
  - bevat een documenthistorie (wat is wanneer en door wie aangepast).
  - is actueel, juist en volledig.
  - is door het juiste (organisatorische) niveau vastgesteld/geaccordeerd.

Relatie met andere normen en standaarden

- NEN-ISO /IEC 27001 ‘Managementsystemen voor informatiebeveiliging’

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B0-4	Algemeen	Alle ICT-componenten en -diensten inclusief de onderlinge relaties worden vastgelegd en dit overzicht wordt permanent onderhouden.	

Doelstelling

- Het (betrouwbaar) vastleggen van gegevens over alle ICT-componenten en -diensten, zodat een actueel overzicht van de ICT-componenten en -diensten en relaties tussen deze ICT-componenten en -diensten wordt verkregen en behouden.

Rationale

Configuratiebeheer heeft als doelstelling het (betrouwbaar) vastleggen van gegevens over alle ICT-componenten en -diensten (denk hierbij aan apparatuur, programmatuur, netwerkverbindingen, informatie en documentatie). Tevens worden de onderlinge relaties tussen deze ICT-componenten en -diensten vastgelegd. Dit overzicht moet permanent worden onderhouden zodat ten allen tijde een actueel inzicht bestaat van de ICT-componenten en -diensten.
Elke ICT-component en -dienst dient duidelijk te worden geïdentificeerd en het eigenaarschap hiervan moet zijn vastgelegd en gedocumenteerd.

Een belangrijk aspect bij het vaststellen van de waarde en het belang van alle ICT-componenten en -diensten is een actueel overzicht. Op basis van de waarde en het belang kan een beveiligingsniveau, door middel van een risicoanalyse, worden bepaald dat past bij de ICT-componenten en -diensten. Dit inzicht draagt ertoe bij dat de ICT-componenten en -diensten op de juiste manier worden beveiligd.

Het proces configuratiebeheer is voorwaardenscheppend voor bijna alle andere processen, zoals:

- Risicomanagement, maatregel B0-2.
- Wijzigingsbeheer, maatregel B0-6.
- Patchmanagement, maatregel B0-7.

Vereiste succescriteria (conformiteitvereisten)

- Zorg voor een procesbeschrijving van configuratiebeheer en dat dit proces effectief is geïmplementeerd.
- Wijzigingen met betrekking tot de ICT-componenten en -diensten verloopt via het proces wijzigingsbeheer.

Classificatie

Hoog

Bewijsvoering

- Procesbeschrijving configuratiebeheer.
  - heeft een eigenaar.
  - is voorzien van een datum en versienummer.
  - bevat een documenthistorie (wat is wanneer en door wie aangepast).
  - is actueel, juist en volledig.
  - is door het juiste (organisatorische) niveau vastgesteld/geaccordeerd.
- Overzicht van de ICT-componenten en -diensten, inclusief eigenaarschap.

Relatie met andere normen en standaarden

- Basisnormen Beveiliging en Beheer ICT-infrastructuur:
  - paragraaf 4.7 Configuration Management
- NEN-ISO /IEC 'Code voor informatiebeveiliging':
  - paragraaf 7.1 'Verantwoordelijkheid voor bedrijfsmiddelen'

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B0-5	Algemeen	Maak gebruik van een hardeningsproces[20], zodat alle ICT-componenten zijn gehard tegen aanvallen.	3.3.10, 3.3.11 en 4.3

Doelstelling

- Het tot een minimum beperken van de kans dat onnodige faciliteiten op een systeem worden misbruikt.

Rationale

De meeste systemen voeren een beperkt aantal functies uit. Het is mogelijk om het aantal potentiële aanvallen te verminderen door het systeem te ontdoen van onder andere software, gebruikersaccounts en diensten die niet gerelateerd en vereist (strikt noodzakelijk) zijn voor het functioneren van het systeem. Wanneer dat niet mogelijk is, moeten alle niet strikt noodzakelijke faciliteiten zijn uitgeschakeld. Systeem hardening is een leverancier specifiek proces, aangezien de verschillende leveranciers het systeem op verschillende manieren configureren en voorzien van verschillende diensten tijdens het standaard (default) installatie proces. Voorbeelden zijn:

- Indien (externe) systemen, zoals webservers en mailservers 'reclame' maken voor hun type en versie, wordt het een aanvaller makkelijker gemaakt om bekende zwakke plekken van deze systemen te exploiteren.
- Systemen die onnodige diensten draaien en poorten open hebben die niet open hoeven te staan zijn makkelijker aan te vallen omdat deze diensten en poorten mogelijkheden bieden om het systeem aan te vallen.

20. Hardenen van systemen bestaat uit verschillende stappen om een gelaagde bescherming te bieden. Met van antivirus, -spyware, -spam en -phishing software, regelmatig installeren van de laatste patches van de leverancier, het uitschakelen van onnodige software en diensten leidt tot een beter beveiligd systeem dat moeilijker door kwaadwillende is te misbruiken.

Alle componenten van de ICT-infrastructuur moeten deel uitmaken van het hardeningsproces, zoals:

- Computers
- Servers (denk aan DNS-severs, mail-servers, webservers et cetera)
- Applicatiesoftware
- Routers en switches
- Databases
- Firewalls
- Telefoonsystemen (VOIP)

Hardeningsproces

Grofweg bestaat een ingericht hardeningsproces uit de volgende stappen:

1. Installeer de systemen volgens de instructies van de leverancier.
2. Verwijder onnodige software.
   De meeste systemen worden geleverd met een verscheidenheid aan software pakketten die functionaliteiten bieden aan alle gebruikers. Software die niet zal worden gebruikt in bepaalde installaties moet worden verwijderd van het systeem, of als dat niet mogelijk is worden uitgeschakeld.
3. Uitschakelen of verwijderen van niet noodzakelijke gebruikersnamen.
   De meeste systemen worden geleverd met een set aan vooraf gedefinieerde gebruikers-accounts. Deze zijn noodzakelijk om een diversiteit aan functies mogelijk te maken. Gebruikersaccounts met betrekking tot diensten of functies die niet worden gebruikt, moeten worden verwijderd of uitgeschakeld. Voor alle standaard gebruikersaccounts die wel worden gebruikt, moet het standaard wachtwoord worden gewijzigd. Als het geen nadelige gevolgen heeft voor het systeem, moeten vooraf gedefinieerde gebruikersaccounts worden hernoemd.
4. Uitschakelen of verwijderen van niet noodzakelijke diensten: alle diensten die niet in productie zullen worden gebruikt, moeten worden uitgeschakeld of verwijderd.
5. Patch het systeem.
   Het systeem moet up-to-date worden gebracht. Alle relevante service packs en beveiligingspatches moeten worden geïnstalleerd (zie maatregel B0-7).
6. Voer vulnerability assessments (security scan) uit.
   Het systeem moet worden gescand op kwetsbaarheden en zwakheden. De resultaten van de scan moeten worden gereviewd en vastgestelde potentiële problemen moeten worden opgelost (zie maatregel B0-9).
7. Installeer antivirus, -spyware, -spam en -phishing software.
   Een antivirus, -spyware, -spam en -phishing softwarepakket moet op het systeem worden geïnstalleerd, zodat wordt voorkomen dat zwakke plekken in het systeem worden geintroduceert door kwaadaardige software.
8. Configureer een lokale firewall.
   Als het systeem zijn eigen lokale firewall kan draaien, moeten regels op de firewall worden geconfigureerd zodat alle poorten die, in productie, niet noodzakelijk zijn worden gesloten (zie maatregel B2-4).

- Neem systeem in productie.
  De voorbereidingen kunnen nu worden getroffen om het systeem in productie te nemen. Natuurlijk verloopt dit via het proces wijzigingsbeheer (zie maatregel B0-6)`

Hardeningsmaatregelen op netwerkniveau

Onderstaand enkele voorbeelden van hardeningsmaatregelen op netwerkniveau:

- Sluit beheermogelijkheden zoveel mogelijk af. Biedt webinterfaces voor beheerfuncties alleen aan via beheercompartimenten (zie maatregel B1-2).
- Sta beheer alleen toe vanaf vooraf gedefinieerde IP-adressen.
- Maak gebruik van complexe wachtwoorden en/of sterke authenticatiemechanismen voor het uitvoeren van beheer op de componenten.

- Maak gebruik van logon banners.
  Een logon banner verschijnt op het moment dat een gebruiker een beheersessie opstart met een netwerkcomponent. Deze banner bevat een waarschuwing die de toegangsvoorwaarden tot het systeem beschrijft. De banner kan daarnaast waarschuwen voor juridische acties wanneer de gebruiker misbruik van het systeem maakt.
- Maak gebruik van versleutelde beheermechanismen.
  Verbied verbindingen die de informatie in cleartext (in onversleutelde vorm) over het netwerk versturen. Maak gebruik van Secure Shell (SSH) in plaats van Telnet, Secure Copy (SCP), SSH File Transfer Protocol (SFTP) of FTP over SSL (FTPS) in plaats van File Transfer Protocol (FTP) en HTTPS in plaats van HTTP voor webinterfaces.
- Harden het onderliggende besturingssysteem.
  Veel leveranciers leveren netwerkcomponenten in de vorm van appliances waarop weinig extra hardeningsmaatregelen mogelijk zijn. In de gevallen dat een netwerkcomponent echter niet gebaseerd is op een appliance, is het van belang dat je het onderliggende systeem 'hardent' (zie maatregelen met betrekking tot platformbeveiliging).
- Besteed voldoende aandacht aan de beveiligingsconfiguratie van netwerkservices en -protocollen: Simple Network Management Protocol (SNMP), Network Time Protocol (NTP), SYSLOG, Trivial FTP (TFTP), finger en routeringsprotocollen zoals Border Gateway Protocol (BGP) en Open Shortest Path First (OSPF).
- Schakel alle ongebruikte protocollen, services en netwerkpoorten uit.
  Op deze wijze wordt de kans op misbruik via niet noodzakelijke protocollen, services en netwerkpoorten voorkomen. Voorbeelden van protocollen die veelal standaard zijn ingeschakeld op netwerkcomponenten maar in veel gevallen niet nodig zijn, zijn Cisco Discovery Protocol (CDP) en Spanning Tree Protocol (STP)
- Maak op switches gebruik van Virtual LAN's (VLAN) en beperk de toegang tot netwerkpoorten op basis van MAC-adres (port security).

Harden de (externe) DNS-infrastructuur

Door de vitale rol die DNS speelt in het bereikbaar houden van webapplicaties, verdient de beveiliging van DNS-services extra aandacht. Door de DNS-infrastructuur te hardenen, wordt DNS-misbruik voorkomen. Aandachtspunten bij het beveiligen van DNS-services zijn [21]:

- Beperk de (bron) IP-adressen die zone transfers mogen uitvoeren met de DNS-server. Alleen primaire en secundaire DNS-servers zouden hiertoe gerechtigd mogen zijn.
- Sta via de firewall alleen verkeer toe richting 53/UDP als de grootte van de DNS-antwoorden dit toestaat. Bij DNS-servers die geen gebruik maken van DNSSEC, zal de server alle DNS-verzoeken kunnen afhandelen op basis van UDP. Alleen bij zeer grote antwoorden (mogelijk als gevolg van het gebruik het DNSSEC) en zone transfers zal DNS overschakelen op het gebruik van TCP. Door 53/tcp te blokkeren in de firewall, voorkom je dat willekeurige IP-adressen in staat zijn om zone transfers uit te voeren.
- Maak gebruik van meerdere autoritatieve DNS-servers voor een zone.
- Verwijder onnodige records uit de zone. Onnodige records (bijvoorbeeld HINFO- en TXT-records) zijn niet nodig en leveren een kwaadwillende extra informatie.
- Overweeg het gebruik van DNSSEC ter bescherming tegen bepaalde DNS-aanvallen.

Alleen de hoogst noodzakelijke services zijn geïnstalleerd

- Bij het hardenen van het systeem is een belangrijke strategie om de communicatie-mogelijkheden van het systeem tot een minimum (het strikt noodzakelijke) te beperken. Eén van de manieren om dit te bereiken is door onnodige services onbereikbaar te maken door ze te verwijderen of uit te schakelen. Door benodigde services in kaart te brengen en vervolgens de afhankelijkheden te bepalen, kom je tot een minimale lijst

21. Aanvullende informatie over de manier waarop men DNS kan beveiligen is te vinden in de publicatie 'Secure Domain Name System (DNS) Deployment Guide' van het National Institute of Standards and Technology (NIST) <http://csrc.nist.gov/publications/nistpubs/800-81r1/sp-800-81r1.pdf>.

van services die op het systeem moeten staan. Alle overige services kun je het beste verwijderen of uitschakelen. Bedenk dat niet-actieve maar wel aanwezige services op een systeem uiteindelijk toch tot een kwetsbaar systeem kunnen leiden aangezien 'lekke' programmacode op het systeem aanwezig is. Veiliger is het daarom om onnodige services volledig van het systeem te verwijderen.

Harden de implementatie van essentiële netwerkprotocollen

Door essentiële netwerkprotocollen, zoals TCP, IP en HTTP, op een server te hardenen, voorkom je misbruik van deze netwerkprotocollen en verhoog je de stabiliteit van het systeem. Twee protocollen die zich uitstekend lenen voor hardening zijn TCP en IP. Het hardenen van de TCP/IP-stack zorgt ervoor dat het risico op een succesvolle DoS-aanval vermindert (zie maatregel B1-5). Denk hierbij aan:

- Time-outs gedurende een SYN-attack te verminderen.
- Te voorkomen dat het systeem dynamisch een alternatieve gateway verkiest.
- Te voorkomen dat het systeem een dynamische MTU kiest.
- Keep-alive mechanismen in te schakelen.

In webomgevingen leent ook HTTP zich voor hardening om bijvoorbeeld een Denial-of-Service-aanval op HTTP-niveau te voorkomen. Denk hierbij aan:

- 'Idle time-out' van een HTTP-sessie verkleinen.
- 'Session pooling' tussen een application-level firewall en webservers in te schakelen.

Vereiste succescriteria (conformiteitvereisten)

- Zorg voor een beschrijving van het hardeningsproces en dat dit proces effectief is geïmplementeerd.
- Zorg voor een actueel overzicht van de hoogst noodzakelijke netwerkprotocollen en dat dit overzicht continue wordt onderhouden.
- Zorg voor een actueel overzicht van de hoogst noodzakelijk services.
- Zorg dat dit overzicht onderdeel is van het proces wijzigingsbeheer.
- Zorg dat periodiek wordt getoetst of het systeem voldoet aan het overzicht van hoogst noodzakelijke netwerkprotocollen.
- Afwijkingen moeten worden gedocumenteerd en geaccepteerd door de eigenaar van de webapplicatie en beveiligingsfunctionaris.

Classificatie

Hoog

Bewijsvoering

- Beschrijving van het hardeningsproces.
  - heeft een eigenaar.
  - is voorzien van een datum en versienummer.
  - bevat een documenthistorie (wat is wanneer en door wie aangepast).
  - is actueel, juist en volledig.
  - is door het juiste (organisatorische) niveau vastgesteld/geaccordeerd.
- Een actueel overzicht van de hoogst noodzakelijk netwerkprotocollen is beschikbaar.
- Een actueel overzicht van de hoogst noodzakelijk services is beschikbaar.
- Statusoverzicht van de toets of het systeem voldoet aan het overzicht van de hoogst noodzakelijk netwerkprotocollen.
- Een overzicht van de door de eigenaar van de webapplicatie en beveiligingsfunctionaris geaccepteerde afwijkingen.

Relatie met andere normen en standaarden

- NEN-ISO /IEC 27002 'Code voor informatiebeveiliging':
  - paragraaf '12.6 Beheer van technische kwetsbaarheden'

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B0-6	Algemeen	Alle wijzigingen worden altijd eerst getest voordat deze in productie worden genomen en worden via wijzigingsbeheer doorgevoerd.	3.3.7, 4.3.1 en 4.3.11

Doelstelling

Het garanderen van een correcte en veilige werking van ICT-voorzieningen door het op een gecontroleerde manier doorvoeren van wijzigingen.

Rationale

Wijzigingsbeheer zorgt ervoor dat alle instellingen van de ICT-infrastructuur gecontroleerd en geautoriseerd gewijzigd worden, dit geldt dus ook voor de hardeningsmaatregelen.
Wijzigingen moeten eerst worden getest in een test- of acceptatieomgeving om de impact van de maatregelen vast te stellen. Dit zorgt ervoor dat de ICT-infrastructuur aan de gestelde maatregelen blijft voldoen.
Het aanbrengen van bijvoorbeeld nieuwe verbindingen tussen netwerkcomponenten kan ervoor zorgen dat routepaden en compartimenteringen 'plotseling' ongewenst wijzigen.
Het proces configuratiebeheer (zie maatregel B0-4) is voorwaardenscheppend voor wijzigingsbeheerproces en heeft een beveiligingsbelang in het kader van de integriteits-handhaving, doordat het kan ondersteunen dat updates van ICT-componenten overal worden aangebracht waar ze worden gebruikt.

Webapplicaties worden getest voordat deze in de productie worden genomen

Voordat een webapplicatie in productie wordt genomen, is het van belang dat eerst een uitgebreide test wordt uitgevoerd op de webapplicatie en de omliggende infrastructuur.
Het uitvoeren van tests is niet alleen belangrijk bij de initiële ingebruikname van de webapplicatie, maar ook na het doorvoeren van belangrijke wijzigingen in de webapplicatie of de infrastructuur.
Ook voor alle maatregelen die in deze Richtlijn worden beschreven, geldt dat deze altijd eerst in een representatieve testomgeving moeten worden uitgeprobeerd voordat ze in een productieomgeving toegepast kunnen worden. Systemen moeten opnieuw worden beoordeeld en getest wanneer wijzigingen plaatsvinden.
Wijzigingen kunnen een onvoorziene negatieve impact hebben op de werking van de ICT-infrastructuur en daarom is het belangrijk te verifiëren of een systeem, ook na het effectueren van wijziging, goed blijft functioneren. Dit geldt natuurlijk voor alle maatregelen zoals hardeningsmaatregelen.

Ontwikkel, test en acceptatievoorzieningen moeten zijn gescheiden van productievoorzieningen (OTAP)

Ontwikkel- en testactiviteiten kunnen verstoringen veroorzaken, bijvoorbeeld onbedoelde wijzigingen in bestanden of systeemomgeving, of storingen in het systeem.
Ontwikkel- en testactiviteiten kunnen ook onbedoelde wijzigingen in software en informatie veroorzaken als dezelfde ICT-omgeving wordt gedeeld.
Als ontwikkel- en testmedewerkers toegang hebben tot de productieomgeving en -informatie, zouden zij ongeoorloofde en niet geteste software kunnen invoeren of bedrijfsgegevens kunnen wijzigen.
Voorzieningen voor ontwikkeling, testen en productie moeten zijn gescheiden om het risico van onbedoeld wijzigingen of ongeautoriseerde toegang tot productiesystemen en bedrijfsgegevens te verkleinen.
In bepaalde situaties (omgevingen) kan een OTP-omgeving een afdoende maatregel zijn.

De productieomgeving wordt geaudit op ongeautoriseerde wijzigingen

Op het moment dat een kwaadwillende een (kwetsbaar) systeem compromitteert, kunnen door de kwaadwillende wijzigingen op dit systeem worden aangebracht. Door wijzigingen op de ICT-infrastructuur (bijvoorbeeld besturingsniveau) te auditen worden eventuele problemen of compromittering van de ICT-omgeving gedetecteerd. Het auditen van ongeautoriseerde wijzigingen op systemen, kan daarom helpen bij het waarnemen van misbruik van de ICT-omgeving. Door geautomatiseerde hulpmiddelen in te zetten kunnen deze wijzigingen adequaat worden gemonitord (zie hoofdstuk 9 'Monitoring, auditing en alerting').

Vereiste succescriteria (conformiteitvereisten)

Wijzigingsbeheer:

- Zorg voor een procesbeschrijving van wijzigingsbeheer en dat dit proces effectief is geïmplementeerd.
- Zorg dat configuratiebeheer is ingericht.
- Alle wijzigingen worden op een gestructureerde wijze geregistreerd.
- Er is vastgelegd welke functionarissen wijzigingen mogen aanvragen.
- Er worden alleen geautoriseerde wijzigingsverzoeken (Request for Change (RFC)) in behandeling genomen.
- Er bestaat een actueel en volledig overzicht van wijzigingen met betrekking tot de (beveiligings)instellingen van de ICT-infrastructuur.
- Van alle wijzigingen wordt de impact met betrekking tot informatiebeveiliging vastgesteld.
- Er is vastgelegd wie de prioriteit van wijzigingen bepaalt en wie toestemming verleent. Bijvoorbeeld een beslissingsforum (Change Advisory Board (CAB))
- De voortgang van de afhandeling van wijzigingen wordt bewaakt.
- Realisatie en implementatie van wijzigingen worden gepland en deze planningsgegevens worden gepubliceerd (changekalender).
- Gerealiseerde wijzigingen worden voor implementatie getest.
- Wijzigingen worden geëvalueerd, waarbij in elk geval vastgesteld wordt of de wijziging niet tot incidenten heeft geleid.
- Voor elke wijziging is een terugvalscenario (fallback) opgesteld, denk hierbij aan beheersprocedures en verantwoordelijkheden bij uitvoering van het terugvalscenario.

De productieomgeving wordt geaudit op ongeautoriseerde wijzigingen:

- Zorg voor een actueel snapshot van de verschillende systemen.
- Zorg dat systemen continue worden geaudit tegen de actuele snapshot (detecteren van wijzigingen).
- Zorg dat het overzicht met auditregels (policy) en de snapshots onderdeel zijn van het proces wijzigingsbeheer.

Webapplicaties worden getest voordat deze in de productie worden genomen:

- Voor nieuwe systemen, upgrades en nieuwe versies moeten acceptatiecriteria zijn vastgesteld.
- Wijzigingen worden getest voordat deze in productie worden genomen.
- Er zijn procedures opgesteld voor de omvang en diepgang van de tests. Als de wijziging impact heeft op de informatiebeveiliging, is bepaald of er specifieke beveiligingstests uitgevoerd moeten worden (bijvoorbeeld penetratietests (zie maatregel B0-8), code reviews (zie maatregel B3-14) et cetera).
- Penetratietesten maken onderdeel uit van de testen (zie maatregel B0-8).

- Als het gaat om standaardsoftware, Software-as-a-Service (SaaS) kan worden gedacht aan de volgende aandachtspunten:
  - Externe certificering van de extern ontwikkelde software.
  - Afspraken in het contract vastleggen om de software te mogen auditen.
  - Uitvoeren van andere tests, bijvoorbeeld penetratietest (zie maatregel B0-8) of blackbox scan (zie maatregel B3-15), om mogelijke kwetsbaarheden op te sporen.

Ontwikkel, test, acceptatie en productieomgeving (OTAP):

- Zorg voor een gescheiden ontwikkel-, test- (, acceptatie-) en productie- omgeving (OTAP).
- Zorg dat procedures zijn gedocumenteerd en vastgesteld voor het overdragen van de ene naar de andere omgeving (van ontwikkel naar test, van test naar acceptatie en van acceptatie naar productie).

Classificatie

Hoog

Bewijsvoering

Wijzigingsbeheer:

- Beschrijving van het configuratie- en wijzigingsbeheerproces.
  - heeft een eigenaar.
  - is voorzien van een datum en versienummer.
  - bevat een documenthistorie (wat is wanneer en door wie aangepast).
  - is actueel, juist en volledig.
  - is door het juiste (organisatorische) niveau vastgesteld/geaccordeerd.
- Een overzicht met alle wijzigingsverzoeken inclusief autorisatie en impactanalyse met betrekking tot informatiebeveiliging.
- De changekalender.

(geautomatiseerde) Audit op wijzigingen:

- Actueel overzicht met de auditregels (policy).
- Procedurebeschrijving met betrekking tot het creëren en onderhouden van snapshots.
- Resultaten van de uitgevoerde audits.

Webapplicaties worden getest voordat deze in de productie worden genomen:

- Acceptatiecriteria voor nieuwe systemen.
- De datasets en testscripts die worden gebruikt om de tests uit te voeren.
- De resultaten van de uitgevoerde tests.
- De autorisatie dat de tests met goed gevolg zijn doorlopen en dat de wijziging in productie mag worden genomen.

Ontwikkel, test, acceptatie en productieomgeving (OTAP):

- Regels voor het overdragen van systemen van de ene naar de andere omgeving (van ontwikkel naar test, van test naar acceptatie en van acceptatie naar productie).

Relatie met andere normen en standaarden

- Basisnormen Beveiliging en Beheer ICT-infrastructuur:
  - paragraaf 4.11 Change Management
- NEN-ISO /IEC 27002 ‘Code voor informatiebeveiliging’:
  - paragraaf 10.1.2 ‘Wijzigingsbeheer’.
  - paragraaf 10.1.4 ‘Scheiding van faciliteiten voor ontwikkeling, testen en productie’.
  - paragraaf 10.3.2 ‘Systeemacceptatie’.
  - paragraaf 12.5.1 ‘Procedures voor wijzigingsbeheer’.
  - paragraaf 12.5.2 ‘Technische beoordeling van toepassingen na wijzigingen in het besturingssysteem’.

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B0-7	Algemeen	De laatste (beveiligings)patches zijn geïnstalleerd en deze worden volgens een patchmanagement proces doorgevoerd.	4.3.2 en 6.4.1

Doelstelling

- Alle aanwezige software is tijdig voorzien van de laatste versies/patches om mogelijke uitbuiting van kwetsbaarheden voor te zijn.
- Op een zo efficiënt mogelijk wijze met zo min mogelijk verstoringen een stabiel (veilig) systeem te creëren.

Rationale

Een solide updatemechanisme is essentieel om voldoende beschermd te zijn tegen bekende beveiligingsproblemen in software. Een updatemechanisme voor alle applicatieplatformen, applicaties, databases, et cetera die bovenop dit platform draaien, is minstens zo belangrijk.
De noodzaak van patchen staat vaak niet ter discussie. Er ontstaat echter wel vaak discussie over de urgentie waarmee deze patches uitgevoerd moeten worden. De tijdsduur tussen het uitkomen van een patch en de implementatie van een patch is hierbij afhankelijk van de gevoeligheid van de webapplicatie en de ernst van de patch. Daarom is het van belang vast te stellen welke doelstelling (en prioriteit) nagestreefd wordt (worden) met patchmanagement[22]. Het kan voorkomen dat systemen die niet meer gesupport worden, (tijdelijk) operationeel gehouden moeten worden. Het is van belang om te weten welke systemen dat zijn en welke aanvullende maatregelen getroffen zijn om deze systemen voor het uitbuiten van kwetsbaarheden te behoeden.

Grofweg bestaat een ingericht patchmanagementproces uit de volgende stappen:

1. stel vast dat een patch beschikbaar is.
2. beoordeel de impact van de uitgebrachte patch en de bijbehorende kwetsbaarheid.
3. verkrijg de patch via de leverancier.
4. test de patch in een test- en/of acceptatieomgeving.
5. rol de patch uit in de productieomgeving.
6. volg berichtgeving rondom de patch.
7. evalueer het gehele proces.

Het proces configuratiebeheer (zie maatregel B0-4) is voorwaardenscheppend voor het patchmanagement proces en heeft een beveiligingsbelang in het kader van de integriteitshandhaving, doordat het kan ondersteunen dat updates van ICT-componenten overal worden aangebracht waar ze worden gebruikt.

Vereiste succescriteria (conformiteitvereisten)

- Zorg voor een beschrijving van het patchmanagementproces en dat dit proces effectief is geïmplementeerd.
- Zorg dat configuratiebeheer is ingericht.
- Zorg voor een technische implementatie van een updatemechanisme.
- Er moet een procedure zijn ingericht waarin staat beschreven hoe de organisatie omgaat met updates: hoe snel implementeert de organisatie een kritieke patch, welke stadia moet de patch doorlopen, wie draagt de verantwoordelijkheid, et cetera?

Classificatie

Hoog

22. Meer informatie en tips over de inrichting van het patchmanagement proces is na te lezen in het GOVCERT.NL whitepaper “Patchmanagement” [11]

Bewijsvoering

- Beschrijving van het configuratie en patchmanagementproces. Deze procesbeschrijving:
  - heeft een eigenaar.
  - is voorzien van een datum en versienummer.
  - bevat een documenthistorie (wat is wanneer en door wie aangepast).
  - is actueel, juist en volledig.
  - is door het juiste (organisatorische) niveau vastgesteld/geaccordeerd.
- Een actueel overzicht van systemen die in productie draaien maar niet meer worden ondersteund.

Relatie met andere normen en standaarden

- Basisnormen Beveiliging en Beheer ICT-infrastructuur:
  - paragraaf 4.11 Change Management

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B0-8	Algemeen	Penetratietests[23] worden periodiek uitgevoerd.	2.8

Doelstelling

- Inzicht krijgen en houden in de mate waarin een webapplicatie weerstand kan bieden aan pogingen om het te compromitteren (binnendringen of misbruiken van webapplicatie).[24]

Rationale

Dit is een impliciet onderdeel van wijzigingsbeheer (zie maatregel B0-6), maar wordt in verband met de belangrijkheid afzonderlijk geadresseerd. Vanuit beveiligingsoptiek is het van belang dat via een penetratietest[25] (ook pentest genoemd) wordt gecontroleerd of de webapplicatie en/of de infrastructuur op enigerlei wijze is binnen te dringen of te misbruiken. Penetratietests zijn daarom een waardevolle aanvulling op de beveiliging van webapplicaties. Een penetratietest uitvoeren kan echter een uitdaging zijn. Risico's moeten minimaal zijn, de kwaliteit van de test optimaal en resultaten moeten bruikbaar zijn om kwetsbaarheden efficiënt te verhelpen.

Verschillende varianten penetratietests

Penetratietests kent verschillende varianten zoals black box tests, grey box, white box en crystal box. Het verschil zit onder meer in de hoeveelheid kennis en achtergrondinformatie die de tester krijgt. Als een tester minimale voorkennis heeft, is er sprake van black box; krijgt een tester van tevoren inzicht in alle aspecten van de systeemarchitectuur, dan heet die white box. Beschikt een tester over gedeeltelijke informatie, dan heet dit grey box. Met crystal box wordt meestal bedoeld dat de testers ook de broncode van de applicatie hebben en toegang hebben tot alle mogelijke configuratie-informatie.
Wordt er getest vanuit het perspectief van een interne medewerker (privileged test) of vanuit het perspectief van een aanvaller vanaf internet (non-privileged).

23. Andere termen die voor penetratietests gebruikt worden zijn ethical hacking test, legal hacking test, hacktest en diverse samenstellingen van deze termen. De termen komen min of meer op hetzelfde neer.
24. Een pentest is een momentopname beperkt naar de laatste stand der techniek. Door ontwikkelingen in deze techniek kunnen er zich nieuwe risico's voordoen of bestaande risico's zwaarde gaan wegen.
25. Meer informatie en tips over het uitvoeren van penetratietests is na te lezen in de GOVCERT.NL whitepaper 'pentesten doe je zo' <http://www.govcert.nl/dienstverlening/Kennis+en+publicaties/whitepapers/pentesten-doe-je-zo.html>.

Wanneer pentesten?

Er kunnen meerdere momenten zijn waarop een penetratietest zinvol is:

- De frequentie dient vastgesteld te worden op basis van het risicoprofiel.
- In de acceptatiefase van een nieuw systeem of een nieuwe applicatie.
- Bij significante wijzigingen van een belangrijk systeem of een belangrijke applicatie.
- Periodiek (jaarlijks/tweejaarlijks), om bestaande systemen te testen op nieuwe inbraaktechnieken en/of als onderdeel van de PDCA-cyclus (zie maatregel B0-1).
- Als er een andere reden is om te denken dat de beveiliging van een systeem minder goed is dan gedacht.

Opdrachtomschrijving

Essentieel in de (offerte)aanvraag is de opdrachtomschrijving met daarin een heldere onderzoeksvraag. Welke informatie moet de pentest opleveren; welke vraag moet beantwoord worden? Het moet voor aanbieders duidelijk zijn wat er van hen wordt verwacht. Denk hierbij aan de volgende vragen:

- Is het mogelijk om toegang tot het systeem te krijgen?
- Is het mogelijk om, eenmaal binnengedrongen, toegang te verkrijgen tot vertrouwelijk materiaal?
- Kan een geautoriseerd gebruiker met beperkte toegangsrechten misbruik maken van een andere geautoriseerde gebruiker meer toegangsrechten?

Scopedefinitie

Een ander belangrijke aspect is de inkadering van de test. Wat is het object van onderzoek?

- Geef goed aan om welke componenten het gaat.
  Denk hierbij aan firewalls, databses, applicaties, et cetera.
- Geef goed aan om welke omgeving het gaat.
  Hoeveel systemen en apparaten moeten worden getest en zijn ze vergelijkbaar?
- Als u van het te testen object een ontwikkel-, test- en/of acceptatieomgevingen heeft, dan kan het verstandig zijn om één van die omgevingen voor de duur van de pentest precies zo in te richten als de productieomgeving en de test daarop laten plaatsvinden.
- Wordt de penetratietest van buiten via het internet (non- privileged) of vanaf het interne netwerk uitgevoerd (privileged)?
- Geef vooraf de diepgang van de penetratietest aan. Valt bijvoorbeeld het gebruiken van exploits binnen scope of niet? Wordt de scope beperkt tot de OWASP Top 10 [1], CWE/SANS Top 25[26] of worden hier geen beperking aan gesteld?
- Voer voorafgaand een risicoanalyse uit waaruit blijkt dat kwetsbaarheden in een systeem een groot risico zijn en vervolgens wordt dan de penetratietest uitgevoerd om in kaart te brengen welke kwetsbaarheden er zijn en hoe ze opgelost kunnen worden.

Planning

Een pentest moet ruim van tevoren gepland worden. Houd rekening met bijvoorbeeld de volgende aspecten:

- Zijn er momenten waarop er niet getest mag worden?
- Vermijd kritieke periodes, zoals een pentest van een salarisverwerkend systeem aan het eind van de maand
- Doe geen pentest als een systeem tijdens de test veranderingen ondergaat.

Rapportage

De resultaten van de pentest worden vastgelegd in een vorm van een rapportage.
Geef duidelijk aan welke informatie de rapportage moet bevatten, bijvoorbeeld:

- Type penetratietest (white, grey, back of crystal box).
- Het tijdstip waarop de test is uitgevoerd.
- De gebruikte applicaties (inclusief versienummer).

26. http://cwe.mitre.org/top25/ of http://www.sans.org/top25-software-errors/

- De parameters die zijn gebruikt bij de tests.
- Het IP-adres waarvandaan de test is uitgevoerd.
- Op welke omgeving de penetratietest heeft plaatsgevonden (ontwikkel, test, acceptatie of productie)
- Een toelichting per gevonden verbeterpunt.
- Een inschatting van de prioriteit per verbeterpunt.

Opvolging

Er moet actie worden ondernomen indien geïmplementeerde maatregelen niet voldoen aan de gestelde eisen en/of verwachtingen of tekortkomingen opleveren.

De methodiek en testplan

De kwaliteit van de penetratietest wordt mede bepaald door de methodiek.
Denk hierbij aan:

- stappenplan waarin de activiteiten in volgorde worden beschreven en op welke methodiek de aanpak is gebaseerd.
- testplan waarbij per test staat vermeld wat de risico's zijn.

Vereiste succescriteria (conformiteitvereisten)

- Pentests worden niet alleen bij nieuwbouw en wijzigingen uitgevoerd, maar moeten periodiek worden herhaald.
- Zorg voor een opdrachtomschrijving, scopedefinitie, planning en kwaliteitseisen.
- De resultaten van de pentest worden vastgelegd in een rapportage. Waarbij duidelijk is aangegeven welke informatie de rapportage moet bevatten.
- Er moet aantoonbaar follow-up worden gegeven in casu verbeteringen worden doorgevoerd indien geïmplementeerde maatregelen niet voldoen aan de gestelde eisen en/of verwachtingen of tekortkomingen opleveren.

Classificatie

Hoog

Bewijsvoering

- Planning.
- Opdrachtomschrijving(en) met daarin een heldere onderzoeksvraag.
- Scopedefinitie(s) met daarin het object van onderzoek.
- Rapportageformat met daarin duidelijk vastgelegd welke informatie de rapportage moet bevatten.
- Rapportages met de resultaten van de pentest(s).
- Plan met daarin de activiteiten die worden uitgevoerd (wie, wat en wanneer) indien geïmplementeerde maatregelen niet aan de gestelde eisen en/of verwachtingen hebben voldaan of tekortkomingen hebben opgeleverd.

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B0-9	Algemeen	Vulnerability assessments (security scans) worden periodiek uitgevoerd.	

Doelstelling

- Inzicht hebben in de mate waarin de ICT-omgeving bekende kwetsbaarheden en zwakheden bevat, zodat deze waar mogelijk weggenomen kunnen worden.

Rationale

Kwaadwillenden maken gebruik van kwetsbaarheden en zwakheden in ICT-componenten (zowel ICT-systemen als netwerken). Zonder inzicht in de huidige stand van zaken, tast de beheerder in het duister en kan deze niet goed anticiperen op nieuwe ontwikkelingen. Vragen die hierbij een rol spelen:

- Hoe is de ICT-omgeving opgebouwd en geconfigureerd (zie maatregel B0-4)?
- Wat zijn bekende kwetsbaarheden en zwakheden?

Frequentie

De frequentie voor het uitvoeren van vulnerability assessments dient vastgesteld te worden op basis van het risicoprofiel.

Opvolging

Er moet actie worden ondernomen indien geïmplementeerde maatregelen niet voldoen aan de gestelde eisen en/of verwachtingen of tekortkomingen opleveren.

(Geautomatiseerde) Vulnerability assessment

Bij een vulnerability assessment (VA) wordt er met behulp van een scanner een (geautomatiseerde) scan uitgevoerd op een van te voren bepaald aantal IP adressen. Hierbij worden de servers en services onderzocht op alle bekende kwetsbaarheden en zwakheden en worden de gevonden kwetsbaarheden en zwakheden gerangschikt naar risico (hoog, midden en laag). Het te analyseren aantal IP-adressen kan door de beheerder worden ingevoerd of automatisch worden bepaald door een netwerkscan uit te voeren. Door een VA uit te voeren over de ICT-componenten (zowel ICT-systemen als netwerken), komen aanwezige kwetsbaarheden en zwakheden naar boven en worden deze weergegeven in een rapportage. Op basis van de rapportage kan de organisatie een afweging maken welke kwetsbaarheden relevant zijn en verholpen moeten worden en welke geaccepteerd worden. Het kan voorkomen dat bepaalde kwetsbaarheden niet verholpen kunnen worden omdat dan de webapplicatie niet meer functioneert.

Netwerk- of Hostgebaseerde VAs

Voor het uitvoeren van een VAs zijn twee varianten: host- of netwerk gebaseerd. Netwerkgebaseerde VAs worden uitgevoerd door gebruik te maken van netwerkscanners. Netwerkscanners zijn in staat om open poorten te detecteren, services te identificeren die op deze poorten draaien, mogelijke kwetsbaarheden te detecteren van deze services en aanvallen te simuleren. Aan de andere kant, worden hostgebaseerde VAs uitgevoerd door hostscanners. Hostscanners zijn in staat om kwetsbaarheden op systeemniveau te herkenen, waaronder onjuist toegekende rechten en configuratiefouten. In tegenstelling tot de netwerkscanners, is voor hostscanners een administrator account nodig met voldoende toegangsrechten.

Vereiste succescriteria (conformiteitvereisten)

- Zorg dat vulnerability assessment periodiek worden herhaald.
- Zorg voor een scopedefinitie (denk hierbij aan host- of netwerkgebaseerde VA, te onderzoeken IP-adressen en/of type besturingssysteem), planning en kwaliteitseisen.

- Zorg dat de resultaten van de vulnerability assessment worden vastgelegd in een rapportage, waarbij duidelijk is aangegeven welke informatie de rapportage moet bevatten.
- Er moet aantoonbaar follow-up worden gegeven in casu verbeteringen worden doorgevoerd indien geïmplementeerde maatregelen niet voldoen aan de gestelde eisen en/of verwachtingen of tekortkomingen opleveren.

Classificatie

Hoog

Bewijsvoering

- Een planning wanneer reguliere vulnerability assessment worden uitgevoerd met daarin duidelijk het object van onderzoek omschreven.
- Het rapportageformat met daarin duidelijk vastgelegd welke informatie de rapportage moet bevatten.
- Rapportages met de resultaten van de vulnerability assessments.
- Een plan met daarin opgenomen welke activiteiten worden uitgevoerd en wie verantwoordelijk is om de gedetecteerde kwetsbaarheden en zwakheden te verhelpen.

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B0-10	Algemeen	Policy compliance checks worden periodiek uitgevoerd.	

Doelstelling

- Inzicht krijgen en houden in de mate waarin de ICT-omgeving en ICT-componenten die van belang zijn voor de webapplicatie voldoen aan de vooraf vastgestelde security policies.

Rationale

Vanuit beveiligingsoptiek is het van belang dat via policy compliance checks wordt gecontroleerd of de ICT-omgeving na verloop van tijd nog steeds voldoet (naleving) aan de vastgestelde en geïmplementeerde security policies.

Wanneer policy compliance checks uitvoeren?

Er kunnen meerdere momenten zijn waarop een policy compliance check zinvol is:

- De frequentie voor het uitvoeren van policy compliance checks dient vastgesteld te worden op basis van het risicoprofiel.
- Bij wijzigingen van een security policy.
- Periodiek (maandelijks/per kwartaal/halfjaarlijks/jaarlijks), om bestaande systemen te testen op naleving van de secuity policy en/of als onderdeel van de PDCA-cyclus (zie maatregel B0-1).
- Als er een andere reden is om te denken dat de secuity policy niet wordt nageleefd.

Rapportage

De resultaten van de policy compliance check worden vastgelegd in de vorm van een rapportage. Geef duidelijk aan welke informatie de rapportage moet bevatten, bijvoorbeeld:

- Het tijdstip waarop de policy compliance check is uitgevoerd.
- De gebruikte applicaties (inclusief versienummer).
- De parameters die zijn gebruikt bij de policy compliance check.
- Op welke omgeving de policy compliance check heeft plaatsgevonden (ontwikkel, test, acceptatie of productie).
- Een toelichting per gevonden afwijking.
- Een inschatting van de prioriteit per afwijking.

Opvolging

Er moet actie worden ondernomen indien geïmplementeerde maatregelen niet voldoen aan de gestelde eisen en/of verwachtingen of tekortkomingen opleveren.

Vereiste succescriteria (conformiteitvereisten)

- Zorg dat policy compliance checks periodiek worden herhaald.
- Zorg voor een scopedefinitie (denk hierbij aan het te onderzoeken type besturingssysteem), planning en kwaliteitseisen.
- Zorg dat de resultaten van de policy compliance check worden vastgelegd in een rapportage, waarbij duidelijk is aangegeven welke informatie de rapportage moet bevatten.
- Er moet aantoonbaar follow-up worden gegeven in casu verbeteringen worden doorgevoerd indien geïmplementeerde maatregelen niet voldoen aan de gestelde eisen en/of verwachtingen of tekortkomingen opleveren.

Classificatie

Midden

Bewijsvoering

- Een planning wanneer reguliere policy compliance checks worden uitgevoerd met daarin duidelijk het object van onderzoek omschreven.
- Het rapportageformat met daarin duidelijk vastgelegd welke informatie de rapportage moet bevatten.
- Rapportages met de resultaten van de policy compliance checks.
- Plan met daarin de activiteiten die worden uitgevoerd (wie, wat en wanneer) indien afwijkingen zijn gedetecteerd..

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B0-11	Algemeen	Er moet een toereikend recovery proces zijn ingericht waar back-up en restore onderdeel vanuit maken.	4.3.9

Doelstelling

- Het waarborgen van de integriteit en beschikbaarheid van informatieverwerkende systemen of webapplicaties.

Rationale

Er moeten hersteltijden worden vastgesteld op basis van de gevoeligheid van de web-applicaties. Herstelmaatregelen moeten zijn geborgd, bijvoorbeeld back-up en restore en een calamiteitenplan.
Er moeten regelmatig back-ups (reservekopieën) worden gemaakt van essentiële informatie en systemen of webapplicaties om de integriteit en beschikbaarheid van systemen of webapplicaties te waarborgen. Hiervoor moeten goede voorzieningen beschikbaar zijn, zodat alle essentiële gegevens en systemen tijdig hersteld kunnen worden na een incident. Dagelijkse back-ups zijn vaak voldoende maar voor sommige dynamische componenten (zoals databases) is deze dagelijkse snapshot wellicht niet afdoende. Bij dergelijke componenten kun je overwegen om de transactielog van de database beschikbaar te stellen op een uitwijklocatie (‘remote journaling’). In het geval dat een component crasht, kan een up-to-date versie van het component worden gecreëerd door de laatste back-up hiervan terug te zetten en hierop de transactielog toe te passen.
Het is aan te raden om back-ups te versleutelen. Valt een back-up onverhoopt in handen van een kwaadwillende, dan kan deze in dit geval geen toegang krijgen tot de informatie in de back-up.

Tot slot is het van belang om regelmatig te testen of de gemaakte back-ups de mogelijkheid bieden om een verloren gegaan systeem opnieuw op te bouwen. Maak back-ups onderdeel van een Disaster Recovery Plan (DRP). De frequentie voor het testen dient vastgesteld te worden op basis van het risicoprofiel. Er moet actie worden ondernomen indien geïmplementeerde maatregelen niet voldoen aan de gestelde eisen en/of verwachtingen of tekortkomingen opleveren.

Het kan voorkomen dat voor een gecompromitteerde server, gecompromitteerde bestanden worden gerestored. Om de integriteit van systemen of webapplicaties te garanderen moet in sommige gevallen een 'clean install' van het systeem of webapplicatie worden uitgevoerd en alleen de data vanuit een back-up wordt teruggehaald.
Als de informatieverwerking, en de bijbehorende verantwoordelijkheid, is uitbesteed aan een andere organisatie moeten hierover afspraken worden vastgelegd in een overeenkomst (contract en/of SLA) tussen beide partijen. Dit geldt ook op het moment dat Software-as-a-Service diensten worden ingekocht, denk dan bijvoorbeeld aan cloud escrow[27].

Vereiste succescriteria (conformiteitvereisten)

- Zorg dat een recovery procedure is vastgesteld en geïmplementeerd, back-up en restore maken hier onderdeel vanuit.
- Zorg voor vastgestelde hersteltijden van webapplicaties.
- Zorg dat restore periodiek wordt getest.
- Er moet aantoonbaar follow-up worden gegeven in casu verbeteringen worden doorgevoerd indien geïmplementeerde maatregelen niet voldoen aan de gestelde eisen en/of verwachtingen of tekortkomingen opleveren.

Classificatie

Hoog

Bewijsvoering

- Recovery procedure inclusief back-up en restore.
- Overzicht van vastgestelde hersteltijden.
- Testresultaten van de geteste restores.
- Plan met daarin de activiteiten die worden uitgevoerd (wie, wat en wanneer) indien geïmplementeerde maatregelen niet aan de gestelde eisen en/of verwachtingen hebben voldaan of tekortkomingen hebben opgeleverd.

Relatie met andere normen en standaarden

- Maatregel B1-2 (in verband met het ontsluiten van de storage en back-up infrastructuur)
- NEN-ISO /IEC 27002 'Code voor informatiebeveiliging'
  - paragraaf 10.5 'Back-up'

27. http://www.computable.nl/artikel/producten/cloud_computing/4279284/2333364/escrow-alliance-introduceert-cloud-escrow.html

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B0-12	Algemeen	Ontwerp en richt maatregelen in met betrekking tot toegangsbeveiliging/toegangsbeheer.	4.3.4, 4.3.7, 6.3.1, 8.3.1, 8.3.3, 8.3.5 en 11.2.5

Doelstelling

- Voorkom ongeautoriseerde toegang tot netwerken, besturingssystemen, informatie en informatiesystemen en -diensten, zodat schade bij misbruik zo beperkt mogelijk is.

Rationale

Ontwerp identiteit- en toegangsbeheer

Eén van de belangrijkste stappen op het gebied van identiteit- en toegangsbeheer, is bepalen welke componenten identiteit- en toegangsbeheer uitvoeren. Wordt voor dit doel een centrale voorziening gekozen of wordt dit steeds opnieuw los in de applicatie verwerkt?

De vijf ontwerpmogelijkheden met betrekking tot identiteit- en toegangsbeheer zijn:

1. Alles is in de webapplicatie zelf ingebouwd. De webapplicatie kan geheel zelfstandig functioneren maar maakt geen gebruik van bestaande mechanismen.
2. Alleen identiteitbeheer wordt centraal afgenomen, maar de webapplicatie geeft een eigen invulling aan authenticator-, profiel- en toegangsbeheer.
3. Zowel identiteit als authenticatorbeheer wordt centraal afgenomen, maar de webapplicatie geeft een eigen invulling aan profiel- en toegangsbeheer.
4. Zowel identiteit-, authenticator als profielbeheer wordt in zijn geheel centraal afgenomen, maar de webapplicatie geeft een eigen invulling aan toegangsbeheer. Het vaststellen van de identiteit vertrouwt de webapplicatie toe aan een centraal mechanisme, maar het uitdelen van rechten aan deze identiteit is voorbehouden aan de webapplicatie.
5. Er is geen logica voor identiteit- en toegangsbeheer in de webapplicatie ingebouwd. De webapplicatie vertrouwt volledig op centraal belegde functionaliteiten op dit gebied.

Richt toegangsbeheer in.

Toegangsbeheer betreft alle activiteiten die systemen moeten uitvoeren om de autorisaties voor webapplicaties in te regelen en af te dwingen.

Risico's van systeemmisbruik kunnen aanzienlijk worden verminderd door rechten op een systeem te beperken. De manier waarop rechten op het systeem beperkt kunnen worden, is afhankelijk van het besturingssysteem en het beleid met betrekking tot toegangsbeheer. Principes die in het beleid gehanteerd kunnen worden, zijn bijvoorbeeld gebaseerd op 'standaard geen toegang', 'least privilege', 'need-to-know' of functiescheiding (Separation of Duties).

Hieronder volgen enkele aanwijzingen voor het inperken van rechten op twee populaire typen besturingssystemen: Microsoft Windows en Linux.

Microsoft Windows biedt de mogelijkheid om rechten toe te passen op o.a. bestanden, directories en het register. Via zogenaamde Group Policy Objects (GPO) kunnen beheerders de rechten van gebruikers centraal via de Active Directory (AD) beheren. Een GPO maakt het mogelijk om centraal beperkingen af te dwingen voor verschillende Windows-onderdelen en -systemen.

Linux/UNIX biedt commando's zoals chmod (change mode), chown (change owner), umask, setuid (Set UserID) en setgid (Set GroupID) om toegangsbeheer in te richten.

Wie de autorisaties verleent (aanvraag goedkeuren), vormt een ander aandachtspunt, bijvoorbeeld de eigenaar van de gegevens of een manager. Het toekennen van toegang moet gebaseerd zijn op dataclassificatie[28] en risicoafweging. Bij het bepalen van

28. Informatie dient te worden geclassificeerd, om de behoefte aan, de prioriteit en de mate van beveiliging aan te geven.

dataclassificaties moet rekening worden gehouden met de zakelijke behoefte om informatie te verspreiden of verspreiding te beperken en met mogelijke schade bij bijvoorbeeld ongeautoriseerde toegang tot de informatie.

Gebruikersidentificatie en -authenticatie moeten voldoen aan de zakelijke behoeften en beveiligingseisen.

Welk authenticatiemechanisme moet worden toegepast om een webapplicatie te beschermen moet zijn gebaseerd op een risicoanalyse (classificatie van informatie), zakelijke behoeften en beveiligingseisen.
Authenticatie is gebaseerd op verschillende 'factoren'. Een factor beschrijft op welke manier een gebruiker zich moet authenticeren. Dit kan op basis van:

- Iets dat de gebruiker weet (bijvoorbeeld een wachtwoord of pincode).
- Iets dat de gebruiker heeft (bijvoorbeeld een token of smartcard).
- Iets dat de gebruiker is (bijvoorbeeld een vingerafdruk).
- Bij webapplicaties worden de eerste twee factoren (iets dat de gebruiker weet of heeft) het meest toegepast. Gebruik van biometrische kenmerken voor authenticatie tot webapplicaties is nog geen gemeengoed.
- Om de kans op het omzeilen van het authenticatiemechanisme te voorkomen, is het gangbaar om minimaal 2 verschillende factoren te combineren ('2-factor authentication'). Hierbij kun je denken aan het combineren van smartcards (iets dat de gebruiker heeft) met een passphrase (iets dat de gebruiker weet).

Maak gebruik van strikte OS-authenticatie(mechanismen)

Het is cruciaal dat de authenticatie tot systemen zeer strikt wordt ingeregeld. Afhankelijk van het type besturingssysteem kunnen hier verschillende maatregelen voor worden getroffen. De volgende aanbevelingen zijn van toepassing op vrijwel alle besturingssystemen:

- Zorg dat het systeem niet toegankelijk is op basis van 'anonieme' accounts zoals een gastaccount.
- Beperk de toegang op afstand tot accounts met gelimiteerde rechten. Zorg dat de toegang op basis van root- of beheerderaccounts niet mogelijk is. Beheerders moeten op afstand inloggen met een gelimiteerd beheeraccount en vervolgens lokaal, daar waar nodig, gebruik maken van verhoogde rechten via mechanismen als sudo (Linux) en RunAs (Windows).
- Overweeg de invoering van sterke authenticatiemechanismen voor de toegang tot systemen. Deze mechanismen kenmerken zich door het gebruik van twee factoren voor authenticatie.
- Beperk het aantal groepen waartoe een gebruiker behoort (groepslidmaatschappen). Machtigingen en rechten die aan een groep worden toegekend, gelden ook voor de leden van die groep.
- Implementeer een strikt wachtwoordbeleid. In een wachtwoordbeleid worden de minimale wachtwoordlengte, lengte van de wachtwoordhistorie, complexiteit van het wachtwoord en account lock-outs vastgelegd.
- Voorkom dat wachtwoorden in leesbare vorm worden opgeslagen door middel van het gebruik van hashing (in combinatie met salts).
- Verwijder of blokkeer ongebruikte accounts en standaard aanwezige accounts.
- Hernoem 'bekende' accounts die niet verwijderd kunnen worden (zoals 'administrator') of maak gebruik van sterke wachtwoorden.

De webapplicatie maakt gebruik van platformaccounts met beperkte rechten

Een webapplicatie maakt vaak direct of indirect gebruik van een groot aantal verschillende platformaccounts op een systeem. Door aan de webapplicatie platformaccounts toe te wijzen met beperkte rechten, verlaag je de schade die een aanval kan toebrengen.
Bij het inperken van rechten van platformaccounts moet je bij webapplicaties denken aan de volgende typen platformaccounts:

- Accounts voor het opzetten van verbindingen tussen de webapplicatie en webapplicaties op de datalaag zoals databases en LDAP-stores. Hiermee beperk je de mogelijke schade van injectieaanvallen (SQL-injectie, LDAP-injectie).
- Platformaccounts waaronder de webserver, de databaseserver en de applicatieserver draaien. Hiermee beperk je de schade van buffer overflows en injectieaanvallen.
- Platformaccounts voor toegang tot het bestandssysteem. Vaak gebruikt een webapplicatie voor toegang tot het bestandssysteem het account waaronder de webapplicatie draait. Het is daarom verstandig om op bestandsniveau de rechten van dit account te beperken waardoor dit account bijvoorbeeld niet de mogelijkheid heeft om nieuwe bestanden aan te maken. Dit is niet altijd mogelijk als de applicatie deze rechten nodig heeft om te functioneren.

Maak gebruik van uniforme en flexibele authenticatiemechanismen

Het is van belang dat webapplicaties gebruik maken van bestaande authenticatiemechanismen en dat deze authenticatiemechanisme ingebouwd kunnen worden in verschillende technologieën en protocollen (zoals HTML en XML).
Houdt hierbij rekening met de volgende overwegingen:

- Zorg dat gebruikersgegevens zoveel mogelijk in dezelfde dataverzameling terecht komen (zie maatregel B4-1). Creëer geen aparte databases met gebruikers voor verschillende webapplicaties, maar consolideer deze zoveel mogelijk in één database. Hierdoor wordt het proces efficiënter en vermindert de beheerlast, voorkom je dat authenticatiemechanismen gerepliceerd en gesynchroniseerd moeten worden en verhoog je de mogelijkheid tot de invoering van Single Sign-On (SSO) en Single Sign-Out.
- Zorg dat ontwikkelde authenticatiemechismen eenvoudig ingebouwd kunnen worden in verschillende technologieën en protocollen. Hierbij is een rol weg gelegd voor (I&AM) tooling. Deze tooling moet ondersteuning bieden aan zowel HTML- als XML-applicaties zonder dat grote inspanningen nodig zijn. Denk hierbij bijvoorbeeld aan de implementatie van authenticatie op basis van digitale (X.509-) certificaten: wanneer je dit hele proces hebt ingericht voor een webapplicatie op basis van HTML, moet het hele authenticatiemechanisme eenvoudig te gebruiken zijn door een webservice op basis van XML.

Zorg dat diverse technologieën eenvoudig kunnen worden ingepast. Denk hierbij aan zaken als Federated Identity, SAML, WS-Trust, et cetera.

Audit de uitgedeelde autorisaties regelmatig

Autorisaties op webapplicaties zijn aan continue veranderingen. Niet alleen moeten nieuwe autorisaties worden uitgedeeld, ook moeten bestaande autorisaties worden verwijderd of ingeperkt. De toegewezen autorisaties moeten regelmatig onder de loep worden genomen. Dit kan op basis van een overzicht van alle autorisaties voor de webapplicatie. De webapplicatieverantwoordelijke moet bekijken of er autorisaties bestaan die niet meer nodig zijn of die gewijzigd moeten worden. Belangrijk is wel dat het overzicht te behappen is voor een webapplicatieverantwoordelijke.

Opvolging

Er moet actie worden ondernomen indien geïmplementeerde maatregelen niet voldoen aan de gestelde eisen en/of verwachtingen of tekortkomingen opleveren.

Vereiste succescriteria (conformiteitvereisten)

- Zorg voor beleid ten aanzien van toegangsbeveiliging (identiteit- en toegangsbeheer).
- Zorg voor een wachtwoordbeleid en technische maatregelen om sterke wachtwoorden af te dwingen.
- De zakelijke behoeften en beveiligingseisen moeten zijn gedocumenteerd.

- De inrichting van het identiteit- en toegangsbeheer is gebaseerd op een vastgesteld inrichtingsdocument/ontwerp waarin is vastgelegd welke functies (identiteit-, authenticator, profiel- en toegangsbeheer) waar (centraal/decentraal) worden uitgevoerd.
- Zorg dat het inrichtingsdocument/ontwerp onderdeel is van het proces wijzigingsbeheer.
- Zorg voor een procedurebeschrijving met betrekking tot toegangsbeveiliging voor identiteit- en toegangsbeheer (autorisaties) voor netwerken, besturingssystemen, informatiesystemen, informatie en -diensten.
- Zorg voor een actueel overzicht van service accounts[29].
- Zorg voor een actueel overzicht van personen die beheeraccounts hebben en dat dit overzicht continue wordt onderhouden.
- Zorg voor een actueel overzicht van personen die een gebruikersaccount hebben en dat dit overzicht continue wordt onderhouden.
- Zorg dat periodiek wordt getoetst of het systeem voldoet aan het overzicht van personen die beheeraccounts hebben.
- Accounts die de webapplicatie gebruiken, hebben niet meer rechten dan vereist voor het functioneren van de webapplicatie.
- De data die door webapplicatie(s) wordt aangeboden, moet zijn geclassificeerd.
- De inrichting van het identiteit- en toegangsbeheer is gebaseerd op een vastgesteld inrichtingsdocument/ontwerp waarin is vastgelegd welke functies (identiteit-, authenticator, profiel- en toegangsbeheer) waar (centraal/decentraal) worden uitgevoerd.
- Zorg dat het inrichtingsdocument/ontwerp onderdeel is van het proces wijzigingsbeheer.
- Iedere webapplicatie heeft een eigenaar (verantwoordelijke)
- Er moeten (actuele) overzichten zijn met alle autorisaties voor de webapplicatie.
- Er moet een procesbeschrijving zijn voor het controleren van de gebruikersaccounts en de bijbehorende autorisaties.
- Er moet aantoonbaar follow-up worden gegeven in casu verbeteringen worden doorgevoerd indien geïmplementeerde maatregelen niet voldoen aan de gestelde eisen en/of verwachtingen of tekortkomingen opleveren.
- Het inrichtingsdocument/ontwerp:
  - heeft een eigenaar.
  - is voorzien van een datum en versienummer.
  - is actueel.
  - is op het juiste niveau geaccordeerd.

Classificatie

Hoog

Bewijsvoering

- Beleidsdocument ten aanzien van toegangsbeveiliging (identiteit- en toegangsbeheer).
- Beleidsdocument ten aanzien van wachtwoorden.
- Het dataclassificatieschema.
- De zakelijke behoeften en beveiligingseisen. Rapportage van de risicoanalyse waarop de beslissing is gebaseerd.
- Procedurebeschrijving met betrekking tot toegangsbeveiliging (identiteit- en toegangs-beheer).
- Een actueel overzicht van service accounts is beschikbaar.
- Een actueel overzicht van personen die beheeraccounts hebben is beschikbaar.
- Een actueel overzicht van personen die een gebruikersaccount hebben is beschikbaar.
- Statusoverzicht van de toets of het systeem voldoet aan het overzicht van de hoogst noodzakelijk services.
- Er is gedocumenteerd van welke accounts de webapplicatie gebruik maakt.

29. Een service account is een account dat gebruikt wordt in een geautomatiseerd proces.

- Er is vastgesteld/gedocumenteerd welke minimale rechten deze accounts nodig hebben voor het normaal functioneren van de webapplicatie. De geïmplementeerde rechten zijn beperkt tot deze minimale rechten.
- Plan met daarin de activiteiten die worden uitgevoerd (wie, wat en wanneer) indien geïmplementeerde maatregelen niet aan de gestelde eisen en/of verwachtingen hebben voldaan of tekortkomingen hebben opgeleverd.
- Ontwerp/architectuur van identiteit- en toegangsbeheer, inclusief de besluitvorming.

Relatie met andere normen en standaarden

- NEN-ISO /IEC 27002 'Code voor informatiebeveiliging'.
  - paragraaf 7.2 'Classificatie van informatie'.
- NEN-ISO /IEC 27002 'Code voor informatiebeveiliging'.
  - hoofdstuk 11 'Toegangsbeveiliging'.

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B0-13	Algemeen	Niet (meer) gebruikte websites en/of informatie moet worden verwijderd.	

Doelstelling

- Voorkom misbruik van 'oude' en niet meer gebruikte websites en/of informatie.

Rationale

Websites die niet meer worden gebruikt[30], dienen niet meer live te staan en te worden verwijderd. Ook de informatie die op de 'oude' website(s) is gepubliceerd en koppelingen met backoffice systemen moeten worden verwijderd.

Vereiste succescriteria (conformiteitvereisten)

- Er moet een actueel overzicht zijn van de websites die operationeel zijn. Zorg dat dit overzicht onderdeel is van het proces wijzigingsbeheer.
- Iedere website heeft een eigenaar.
- Voer periodiek controles uit of de operationele websites nog worden gebruikt en/of informatie bevat die kan worden verwijderd.

Classificatie

Hoog

Bewijsvoering

- Overzicht van websites die operationeel zijn inclusief de eigenaar van de websites.

30. Denk hierbij aan oude marketingacties, verlopen promotiecampagnes of testdoeleinden.

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B0-14	Algemeen	Leg afspraken met leveranciers vast in een overeenkomst.	

Doelstelling

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

Rationale

Wanneer de ontwikkeling en/of het beheer over de gehele of een deel van de ICT-dienstverlening met betrekking tot webapplicaties wordt uitbesteedt, moeten de beveiligingseisen in een overeenkomst (bijvoorbeeld contract en/of Service Level Agreement (SLA)) tussen beide partijen worden vastgelegd. Dit geldt ook als standaard software wordt ingekocht, zoals bij Software-as-a-Service (SaaS). Deze overeenkomst moet garanderen dat er geen misverstanden bestaan tussen beide partij.

Aandachtspunten die in de overeenkomst geadresseerd moeten worden, zijn onder andere:

- Beschrijving van de dienst.
  Verwijzing per geleverde dienst naar de betreffende service level specificaties. Denk hierbij aan concrete beschrijving van diensten, servicetijden (normale servicetijden, weekends, feestdagen en vakantiedagen), service beschikbaarheid, responsetijden, oplostijden et cetera.
- Overlegstructuren, contactpersonen en correspondentie.
  Vastleggen wanneer gestructureerd overleg plaatsvindt, wie aan dit overleg deelnemen. Ook zal een overzicht opgenomen moeten worden van alle contactpersonen en verantwoordelijken bij escalatie of calamiteiten (escalatiematrix).
- Geschillen.
  Beschrijving wat de procedure is bij het optreden van onderlinge conflicten of geschillen tussen gebruikersorganisatie en dienstverlener (-aanbieder).
- Prestatie indicatoren, meten en rapportages.
  Beschrijving van de prestatie indicatoren (Key Performance Indicators (KPI's)), hoe deze worden gemeten en hoe hierover wordt gerapporteerd.
- Rapportages.
  Om zicht te hebben, te krijgen en te houden op alles wat te maken heeft met de dienstverlening. Denk hierbij aan afspraken over de inhoud, de frequentie en de verspreiding (distributie) van de rapportage.
- Beveiliging.
  Denk hierbij aan afspraken over procedures voor de beveiliging van systemen, services en data, maatregelen bij het schenden van beveiligingsprocedures en hoe met beveiligingsincidenten wordt omgegaan.
- De noodzakelijke beveiligingseisen, zodat aan de beveiligingseisen en -wensen wordt voldaan.
  - Afspraken over het uitvoeren van audits bij de externe partij.
  - Afspraken over de toegang tot de ICT-omgeving door derden.
  - Afspraken over externe certificering van de (extern) ontwikkelde software. Denk hierbij aan standaardsoftware, Software-as-a-Service (SaaS) of de ontwikkeling van (maatwerk) software is uitbesteed.
  - Afspraken om de (extern) ontwikkelde software te mogen auditen, bijvoorbeeld het uitvoeren van code reviews.
  - Afspraken over het uitvoeren van andere tests, bijvoorbeeld penetratietest (zie maatregel B0-8) of blackbox scan (zie maatregel B3-15), om mogelijke kwetsbaarheden op te sporen.

Vereiste succescriteria (conformiteitvereisten)

- Zorg voor een overeenkomst (bijvoorbeeld contract, Service Level Agreement (SLA) of Diensten Niveau Overeenkomst (DNO)) waarin de beveiligingseisen en -wensen zijn vastgelegd en op het juiste (organisatorische) niveau is vastgesteld/geaccordeerd.

Classificatie

Hoog

Bewijsvoering

- De overeenkomst.
- Rapportages van de dienstleverancier over de geleverde dienstverlening
- Mits van toepassing: Rapportages over uitgevoerde audits, tests, certificeringen.

Relatie met andere normen en standaarden

- NEN-ISO /IEC 27002 ‘Code voor informatiebeveiliging’.
  - paragraaf 6.2 ‘Externe partijen’.

HOOFDSTUK 3

Netwerkbeveiliging

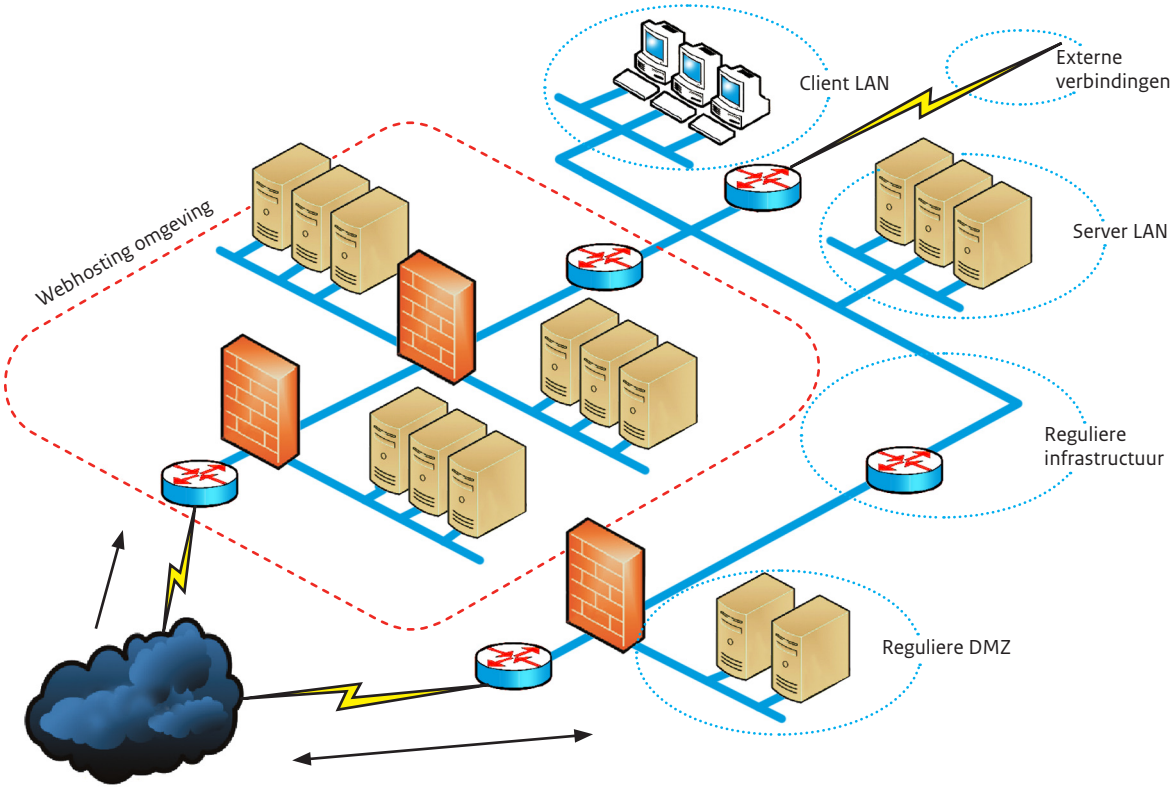
Het netwerk omvat zowel de infrastructuur om de webapplicatie bereikbaar te maken (de koppeling van de webserver met het internet), als de infrastructuur om de webserver resources op te kunnen laten vragen (koppeling met interne systemen en andere systemen in de DMZ). Figuur 3-1 illustreert deze netwerkinfrastructuur, met daarin de afbakening van de Richtlijn (vlak binnen rode stippellijn). Het uitvallen van het netwerk, of een succesvolle aanval daarop, kan ernstige gevolgen hebben voor de beschikbaarheid van de webapplicatie en in sommige gevallen voor de integriteit en vertrouwelijkheid van het netwerkverkeer en de data.

In het kader van deze Richtlijn richt netwerkbeveiliging zich voornamelijk op het beveiligen van informatiestromen op het transport- en netwerkniveau en omvat:

- netwerkcomponenten zoals routers en firewalls.
- netwerkdiensten zoals DNS.
- ontwerp, implementatie en beheer van de (netwerk)infrastructuur.

Als eerste wordt een overzicht gegeven van de mogelijke kwetsbaarheden en bedreigingen op netwerkniveau die van belang zijn voor webapplicaties. Achtereenvolgens komen aan de orde: (Distributed) Denial-of-Service, Pivoting of server hopping, kwetsbare DNS en kwetsbare firewall.

Figuur 3-1 Reikwijdte RBW



3.1 Kwetsbaarheden en bedreigingen

Deze paragraaf beschrijft kwetsbaarheden en bedreigingen die op het gebied van het netwerk bestaan. Mogelijke kwetsbaarheden en bedreigingen zijn:

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
K1-1	Netwerkbeveiliging	(distributed) Denial of Service ((d)DoS).	3.2.1

Toelichting

Over het algemeen gelden de volgende eigenschappen voor een (d)DoS aanval.
Het is bedoeld om:

- een netwerk te overspoelen met dataverkeer, waardoor legitiem dataverkeer niet meer kan doorkomen.
- connecties tussen twee systemen te verbreken.
- een gebruiker geen toegang te geven tot een systeem.
- een service op een systeem te onderbreken.

Voorbeelden van (d)DoS aanvallen om een webapplicatie onbereikbaar te maken zijn via flooding (bijvoorbeeld via een SYN-aanval), Smurf-aanval, et cetera.

Testmethodiek (OWASP Testing Guide/OWASP Code Review Guide)

In paragraaf 4.9 'Denial of Service Testing' worden de volgende tests beschreven:

- OWASP-DS-001 Testing for SQL Wildcard Attacks - SQL Wildcard vulnerability.
- OWASP-DS-002 Locking Customer Accounts - Locking Customer Accounts.
- OWASP-DS-003 Testing for DoS Buffer Overflows - Buffer Overflows.
- OWASP-DS-004 User Specified Object Allocation - User Specified Object Allocation.
- OWASP-DS-005 User Input as a Loop Counter - User Input as a Loop Counter.
- OWASP-DS-006 Writing User Provided Data to Disk - Writing User Provided Data to Disk.
- OWASP-DS-007 Failure to Release Resources - Failure to Release Resources.
- OWASP-DS-008 Storing too Much Data in Session - Storing too Much Data in Session.

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
K1-2	Netwerkbeveiliging	Pivoting (server hopping)	3.2.2

Toelichting

Toegang tot servers in het netwerk door via een gecompromitteerde machine andere machines in het netwerk te benaderen.

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
K1-3	Netwerkbeveiliging	Domain Name System (DNS)	3.2.3

Toelichting

Misbruik van DNS-services voor DoS-aanvallen en cache poISOning (ten behoeve van bijvoorbeeld phishing).
De belangrijkste bedreigingen zijn:

- Toestaan van 'zone transfers'.
- Denial-of-Service.
- DNS cache poISOning.
- Kwetsbaarheden in DNS-software.

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
K1-4	Netwerkbeveiliging	Firewall	3.2.4

Toelichting

Firewall als kwetsbaar element vanwege de essentiële rol die de firewall in een netwerk vervult.

De belangrijkste bedreigingen zijn:

- De organisatie redeneert: 'we hebben een firewall, dus we zijn veilig'.
- De firewall is geconfigureerd als router.
- Misconfiguratie van firewalls door wildgroei in de firewall regels (bijvoorbeeld te ruime toegang of aanwezigheid van oude regels)
- Kwetsbaarheden in firewall software.
- Onduidelijke wensen.

3.2 Doelstelling

Het handhaven van de beveiliging van informatie in netwerken en de bescherming van de ondersteunende infrastructuur zodat de beschikbaarheid van de webapplicatie en de vertrouwelijkheid van het netwerkverkeer en opgeslagen data wordt gewaarborgd.

Aangezien het netwerk een generiek 'onderstel' is voor alle mogelijke toepassingen, zijn veel maatregelen niet specifiek gericht op de beveiliging van webapplicaties, maar op de algemene beveiliging van de infrastructuur rondom de webapplicatie. De Richtlijn richt zich op het beveiligen van de informatiestromen op het transport- en netwerkniveau.

3.3 Beveiligingsrichtlijnen

Deze paragraaf besteedt aandacht aan de maatregelen om netwerkbeveiliging voor webapplicaties in te richten.

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B1-1	Netwerkbeveiliging	Er moet gebruik worden gemaakt van een Demilitarised Zone (DMZ), waarbij compartimentering wordt toegepast en de verkeersstromen tussen deze compartimenten wordt beperkt tot alleen de hoogst noodzakelijke.	3.3.1, 3.3.2, 3.3.3, 3.3.6 en 3.3.7

Doelstelling

- Voorkom of beperk de risico's van een aanval door het scheiden van componenten waaraan verschillende beveiligingsniveaus (betrouwbaarheidseisen) worden gesteld.
- Voorkom rechtstreekse toegang tot het interne netwerk vanaf het internet door het toepassen van compartimentering en het controleren van de verkeersstromen tussen deze compartimenten.

Rationale

Een Demilitarised Zone (DMZ) is een apart stuk netwerk dat specifiek bedoeld is om webapplicaties - en andere vanaf het internet bereikbare applicaties - in onder te brengen. De DMZ vormt de scheiding tussen het internet enerzijds en het interne netwerk anderzijds. Op alle snijvlakken (internet-DMZ en DMZ-intern netwerk) staat een organisatie beperkte verkeersstromen toe, waardoor het risico op het binnendringen van het interne netwerk via het internet zo laag mogelijk wordt gehouden.

Een DMZ kan bestaan uit meerdere compartimenten. Uitgangspunt bij compartimenteren is dat servers, webapplicaties en toepassingen van een gelijk beveiligingsniveau in één gezamenlijk compartiment worden geplaatst. Zo komen bijvoorbeeld webproxies in één compartiment, webservers voor internetsites in één compartiment, webservers voor extranetten in één compartiment, databases in één compartiment, et cetera.

Door compartimentering toe te passen, wordt voorkomen dat het compromitteren van een server, applicatie of toepassing in één compartiment, directe gevolgen heeft voor servers, webapplicaties en toepassingen in een ander compartiment. Slaagt een kwaadwillende erin een server binnen een compartiment aan te vallen, dan heeft de kwaadwillende vanaf deze server alleen toegang tot andere systemen in datzelfde compartiment. De impact van een succesvolle aanval op een systeem wordt hierdoor verkleind. De impact is uiteraard afhankelijk van de verkeersstromen die zijn toegestaan tussen de verschillende compartimenten. Zo bestaat de kans dat een kwaadwillende via een succesvol aangevallen webserver alsnog een databaseserver in een ander compartiment kan benaderen omdat de firewall bepaalde databaseverbindingen vanaf de webserver richting de databaseserver toestaat.Een veilige inrichting van de DMZ is daarom van groot belang om te voorkomen dat kwaadwillenden via internet toegang krijgen tot verschillende compartimenten en uiteindelijk het interne netwerk van de organisatie.

Hieronder een indicatie van systemen die niet in een DMZ mogen worden geplaatst:
- Databaseserver;
- Mailserver;
- Directory services zoals LDAP en Active Directory.

Hieronder een indicatie van systemen die wel in een DMZ kunnen worden geplaatst:
- Webservers;
- Mailgateway (MTA);
- (reverse)Proxy.

Onderstaande aandachtspunten/overwegingen dienen als input voor het ontwerp van de DMZ. De gemaakte beslissingen moeten worden onderbouwd, op het juiste (organisatie) niveau worden vastgesteld, zijn gedocumenteerd en worden onderhouden. Hierdoor is altijd over een actueel ontwerp/inrichting van de DMZ beschikbaar. Het uitgangspunt moet steeds zijn: plaats alleen in de DMZ wat absoluut noodzakelijk is om de gewenste functionaliteit te kunnen bieden.
- Stel vast welke webapplicaties ontsloten worden.
- Stel vast welke informatie in de DMZ opgenomen mag worden.
- Stel vast welke ondersteunende applicaties nodig zijn (functioneel).
- Stel de indeling van de compartimenten vast.
- Stel de koppelvlakken tussen de compartimenten vast.
- Stel de (gecontroleerde) verkeersstromen tussen de compartimenten vast.
- Stel vaste routepaden vast om het verkeer door de DMZ te routeren.
- Stel vastwelk uitgaand verkeer vanaf de webserver mogelijk is.
- Stel de regels van de firewall (rulebase) vast.
- Maak gebruik van het dual-vendor concept.
- Zorg voor een actueel en geaccordeerd DMZ-ontwerp.

Bovenstaande aandachtspunten/overwegingen zullen hierna kort worden toegelicht.

Stel vast welke webapplicaties ontsloten worden

Welke webapplicaties worden ontsloten via de DMZ, bepaalt mede het ontwerp van de DMZ.
Ondersteunt de DMZ alleen webapplicaties, dan bestaat er bijvoorbeeld de mogelijkheid om al het binnenkomende verkeer af te laten handelen door een reverse proxy. Als de DMZ echter ook andere diensten naar het internet ontsluit (bijvoorbeeld e-mail), dan is deze

mogelijkheid er wellicht niet of moet deze op een andere manier binnen de DMZ worden ingebouwd.

Stel vast welke informatie in de DMZ opgenomen mag worden.
In een DMZ worden hooguit openbare gegevens van een organisatie opgeslagen.

Stel vast welke ondersteunende applicaties nodig zijn (functioneel).
Welke ondersteunende applicaties[31] nodig zijn in verband met de functionele werking van de webapplicatie, bepaalt mede het ontwerp van de DMZ.
De verschillende typen applicaties bepalen onder andere hoeveel compartimenten er gecreëerd moeten worden. Als de wens bestaat om al het verkeer te filteren, moet voor elk type applicatie intelligentie binnen de DMZ worden ingebouwd.

Stel de indeling van de compartimenten vast.
Compartimentering maakt het mogelijk om met verschillende beveiligingsniveaus binnen een netwerkinfrastructuur te werken en verkeersstromen te monitoren en controleren. Elk compartiment heeft andere risico's, die afhankelijk zijn van de diensten of ICT-voorzieningen die erin zijn ondergebracht. Er wordt dan ook een ander compartiment ingericht als het risicoprofiel dat vereist. Dit kan bijvoorbeeld noodzakelijk zijn om verschillende productieomgevingen uit elkaar te houden, die niet hetzelfde beveiligingsniveau hebben.
Door deze compartimentering wordt een directe verbinding naar de backoffice vanaf het internet voorkomen. De backoffice is het interne netwerk (LAN) waarin systemen staan waarvan de webapplicatie gebruik maakt.

Stel nummerplan vast.
Bepaal welke private en publieke IP-adressen[32] worden toegepast en of er gebruik van Dynamic Host Configuration Protocol (DHCP) en/of Network Address Translation (NAT) wordt gemaakt. Leg dit vast in een IP-nummerplan.

Stel de koppelvlakken tussen de compartimenten vast.
Aandachtspunten bij het vaststellen van de koppelvlakken zijn onder andere de beschikbaarheid van de verbinding en de mogelijkheid om alle verkeer tussen de compartimenten te monitoren.

Stel de verkeersstromen tussen de compartimenten vast.
Welke verkeersstromen (dit bevat zowel bron- en bestemmings-IP-adressen als netwerk-protocollen) zijn noodzakelijk voor het ontsluiten van webapplicaties via de DMZ en de ondersteunende applicaties. Deze verkeerstromen bepalen mede het ontwerp van de DMZ.
Volstaat HTTP-verkeer vanaf het internet richting de webapplicatie of zijn ook koppelingen nodig vanuit de DMZ naar het interne netwerk?
Op het koppelvlak tussen compartimenten zijn filterfuncties gepositioneerd voor het gecontroleerd doorlaten van gegevens; niet-toegestane gegevens worden tegengehouden.

Stel aansluitvoorwaarden op.
Leg in aansluitvoorwaarden (eisen, criteria) vast wat binnen de compartimenten (DMZ) geplaatst mag worden. In deze aansluitvoorwaarden staat beschreven waaraan de ICT-omgeving moet voldoen om gebruik te mogen maken van de geboden ICT-faciliteiten.

31. Bijvoorbeeld databases, directory services (Active Directory, LDAP), authenticatie en autorisatie services, document management systemen (DMS), Content Management Systemen (CMS), Groupware.o
32. RFC1918 'Address Allocation for Private Internets' < http://tools.ietf.org/html/rfc1918> en RFC3330 'Special-Use IPv4 Addresses' < http://tools.ietf.org/html/rfc3330>

Stel vaste routepaden vast om het verkeer door de DMZ te routeren.
De vastgestelde compartimentering van de DMZ vormt de basis voor het opstellen van routepaden. Een routepad beschrijft een toegestane verkeersstroom door de DMZ. Door routepaden vast te stellen wordt het omzeilen van verplichte beveiligingsmechanismen voorkomen. Hierdoor worden maatregelen voor elke webapplicatie afgedwongen.

Stel uitgaand verkeer vanaf de webserver vast.
Het is bij compartimentering niet alleen belangrijk om aandacht te besteden aan inkomend verkeer, maar ook aan uitgaand verkeer. Veel aanvallen maken misbruik van het feit dat een webserver de mogelijkheid heeft om een verbinding met een ander systeem op te zetten via internet. Het beste is om geen enkel verkeer vanuit de webomgeving naar andere omgevingen toe te staan. Als het absoluut noodzakelijk is, zorg dan dat dit op een gecontroleerde wijze wordt uitgevoerd. Denk hierbij aan het gebruik van een proxy voor het toestaan van HTTP-verkeer vanaf een webserver richting een beperkte set systemen op internet. Door verkeer vanaf een webserver richting het internet te blokkeren, wordt misbruik van een kwetsbaarheid bemoeilijkt of de schade door misbruik van deze kwetsbaarheid beperkt.

Stel vast de regels van de firewall (rulebase) vast
Het is belangrijk om overzicht te houden over de verkeersstromen die de firewall toestaat. Bij nieuwe verkeersstromen moeten de bijbehorende toegangsregels efficiënt worden ingepast in de bestaande rulebase. Bij nieuwe webapplicaties moet een helder en gefundeerd overzicht worden aangeleverd van de verkeersstromen die de te implementeren webapplicatie nodig heeft. Maak hierbij gebruik van 'verkeersoverzichten'.
Het verkeersoverzicht bevat alle firewalls en servers die betrokken zijn bij het aanbieden van de webapplicatie. Dit betekent dat naast de webserver ook alle andere servers waarvan de webapplicatie gebruik maakt (zoals databaseservers), onderdeel uit moeten maken van het verkeersoverzicht. In dit overzicht zijn alle verkeersstromen tussen de componenten ingetekend. Hierdoor ontstaat een overzicht van de regels die op de firewalls nodig zijn om de webapplicatie te kunnen laten functioneren.

Maak gebruik van het dual-vendor concept.
Voorkom dat kwaadwillenden gebruik kunnen maken van dezelfde kwetsbaarheid bij functioneel vergelijkbare producten. Hierdoor wordt de impact van een kwetsbaarheid beperkt. Het concept dual-verdor zal worden toegelicht aan de hand firewalls, maar geldt voor alle functioneel vergelijkbare producten. Door de centrale plaatsing van de firewall(s) kan een kwetsbaarheid op deze firewall(s) grote gevolgen hebben. Door een dual-vendor concept te implementeren wordt de schade bij een dergelijke kwetsbaarheid beperkt. Het dual-vendor concept houdt in dat twee firewalls de netwerkbeveiliging in de DMZ uitvoeren en dat deze firewalls van verschillende makelij (merken) zijn.
Zonder het dual-vendor concept, firewalls van dezelfde makelij (merk), kan een kwaadwillende, na het compromitteren van de eerste firewall, op eenzelfde manier de tweede firewall compromitteren. Dit vanwege het feit dat een potentiële kwetsbaarheid dan op beide systemen aanwezig zal zijn.
Opmerking: Het toepassen van een dual-vendor concept hoeft niet automatisch te betekenen dat je twee typen centrale firewalls in de omgeving plaatst. Dit concept kan ook ingevuld worden door, naast de centraal geplaatste firewalls, firewalls lokaal op de machines te installeren (zie maatregel B2-4).

Zorg voor een actueel en geaccordeerd DMZ-ontwerp
Het is van cruciaal belang om een actueel en geaccordeerd overzicht te hebben van het DMZ-ontwerp, waarin de antwoorden op bovenstaande overwegingen zijn beschreven. Dit is noodzakelijk zodat impactanalyses van voorgestelde wijzigingen altijd zijn gebaseerd op de huidige netwerkinfrastructuur.

Vereiste succescriteria (conformiteitvereisten)

- De inrichting van de DMZ is gebaseerd op een vastgesteld inrichtingsdocument/ontwerp waarin is vastgelegd welke uitgangspunten/principes gelden voor de toepassing van de DMZ. Deze ontwerp- en inrichtingskeuzes moeten zijn onderbouwd en op het juiste (organisatie)niveau zijn verantwoord.
- De (beveiligings)instellingen van de ICT-componenten zijn zodanig gedocumenteerd dat duidelijk is waarom voor bepaalde instellingen gekozen is (verantwoording en onderbouwing). Besteed hierbij speciale aandacht aan de defaultwaarden voor systeeminstellingen.
- De plaatsing van servers en aansluiting van interne netwerkcomponenten en netwerkkoppelingen met externe netwerken zijn duidelijk en schematisch gedocumenteerd, zodat de werking van de ICT-infrastructuur begrijpelijk is en de impact van wijzigingen goed kunnen worden bepaald.
- De volgende aandachtspunten moeten worden geadresseerd in het DMZ-inrichtingsdocument/ontwerp:
  - Welke webapplicaties worden ontsloten?
  - Welke informatie mag in de DMZ worden opgenomen?
  - Welke ondersteunende applicaties zijn noodzakelijk?
  - Welke compartimenten, koppelvlakken en verkeersstromen tussen de compartimenten zijn noodzakelijk?
  - Welke IP-adressen worden gebruiken (NAT, DHCP)?.
  - Welke vaste routepaden om het verkeer door de DMZ te routeren kunnen worden toegepast?
  - Welk uitgaand verkeer vanaf de webserver is noodzakelijk?
  - Zijn aansluitvoorwaarden opgesteld?
- Het DMZ-inrichtingsdocument/ontwerp is actueel en op het juiste (organisatie)niveau vastgesteld.

Classificatie

Hoog

Bewijsvoering

- Het DMZ-inrichtingsdocument/ontwerp waarin minimaal de aandachtspunten zijn geadresseerd zoals benoemd bij de vereiste succescriteria.

Relatie met andere normen en standaarden

- Informatiebeveiligingsproces, zie maatregel B0-1.
- Risicomanagement, zie maatregel B0-2.
- Wijzigingsbeheer, zie maatregel B0-6.
- Penetratietesten, zie maatregel B0-8.
- Beveiligingstemplates, zie maatregel B2-2.
- Basisnormen Beveiliging en Beheer ICT-infrastructuur.
  - hoofdstuk 3 ‘Basisnormen ICT-infrastructuur’.
- NEN-ISO/IEC 27002 'Code voor informatiebeveiliging'.
  - paragraaf 10.6 ‘Beheer van netwerkbeveiliging’.
  - paragraaf 11.4.5 ‘Scheiding van netwerken’.
  - paragraaf 11.4.6 ‘Beheersmaatregelen voor netwerkverbindingen’.
  - paragraaf 11.4.7 ‘Beheersmaatregelen voor netwerkroutering’.
- NORA Dossier Informatiebeveiliging.
  - hoofdstuk 5 ‘Zonering’.
  - hoofdstuk 6 ‘Filtering’.

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B1-2	Netwerkbeveiliging	Beheer- en productieverkeer zijn van elkaar gescheiden.	3.3.5

Doelstelling

Voorkom dat misbruik kan worden gemaakt van de beheervoorzieningen vanaf het internet.

Rationale

Maak onderscheid tussen een productie- en een beheergedeelte. Het productiegedeelte is in feite het gedeelte van de DMZ waarop verkeer vanaf internet terecht komt.
Het onderscheid is aangebracht om te voorkomen dat beheer- en productieverkeer door elkaar gaan lopen. Beheer werkt vaak via webinterfaces en door beheer toe te staan via het productiegedeelte, wordt het risico gelopen dat de bijbehorende webinterfaces en andere beheervoorzieningen te benaderen zijn vanaf het internet.

Met betrekking tot beheer kan onderscheid worden gemaakt tussen drie vormen met ieder hun eigen maatregelen:

- Contentbeheer (bijvoorbeeld web en database content).
  Contentbeheer wordt over het algemeen door de organisatie zelf, vanaf hun eigen werkplek, uitgevoerd en hiervoor gelden dan de aandachtspunten zoals die zijn benoemd in maatregel B1-1. De contentbeheerders moeten op een veilige en gecontroleerde wijze toegang krijgen tot de systemen waar de content is opgeslagen. Denk hierbij aan webservers, databases en Content Management Systemen (CMS). Afhankelijk van de mogelijkheden die de contentbeheerders hebben, bijvoorbeeld het ontwikkelen van formulieren en dynamische content, moet rekening worden gehouden met andere relevante maatregelen zoals die in deze Richtlijn zijn beschreven.
- Applicatiebeheer (bijvoorbeeld het ontwikkelen en onderhouden van webapplicaties).
  Voor applicatiebeheer gelden in hoofdlijnen de maatregelen zoals die zijn beschreven in hoofdstuk 5 ‘Applicatiebeveiliging’.
- Technisch beheer (bijvoorbeeld besturingssystemen en netwerk)

Onderstaande aandachtspunten/overwegingen dienen als input voor het ontwerp van de DMZ. De gemaakte beslissingen moeten worden onderbouwd, op het juiste (organisatie) niveau worden vastgesteld, zijn gedocumenteerd en worden onderhouden zodat altijd over een actueel ontwerp/inrichting van de DMZ wordt beschikt. Het uitgangspunt moet steeds zijn, wat minimaal noodzakelijk (hoogst nodig) is om de gewenste functionaliteit te kunnen bieden.

- Stel vast hoe het beheer van de DMZ wordt ingeregeld.
- Stel vast welke ondersteunende applicaties nodig zijn (beheer).
- Stel vast hoe de storage en back-up infrastructuur wordt ontsloten.
- Stel vast welke beheermechanismen toegepast worden.
- Stel vast hoe beheerders toegang krijgen tot het beheergedeelte.

Bovenstaande overwegingen zullen hierna kort worden toegelicht.

Stel vast hoe het beheer van de DMZ wordt ingeregeld

Denk hierbij aan welke verkeerstromen, netwerkkoppelingen, compartimenten (zie maatregel B1-1), et cetera zijn benodigd om het beheer adequaat uit te kunnen voeren. Het beheer van compartimenten vindt plaats vanuit een eigen compartiment. Het is belangrijk dat de compartimentering die is aangebracht in het productiegedeelte, ook terugkomt in het beheergedeelte. Is dit niet het geval, dan kan een kwaadwillende via het beheergedeelte de compartimentering alsnog omzeilen.
De scheiding van het productie- en beheergedeelte betekent dat servers minimaal twee netwerkaansluitingen krijgen: één voor aansluiting op het productiegedeelte en één voor aansluiting op het beheergedeelte.

Bij de inrichting van de ICT-infrastructuur wordt vastgesteld welke maatregelen moeten en kunnen worden getroffen om netwerkverkeer tussen compartimenten te beperken en te beheersen. Technieken die toegepast kunnen worden, zijn:

- Bridging
- Switching
- Virtual LAN (VLAN)

Stel vast welke ondersteunende applicaties nodig zijn (beheer).

Welke ondersteunende applicaties[33] nodig zijn in verband met het technisch beheer, bepaalt mede het ontwerp van de DMZ.
De verschillende typen applicaties bepalen onder andere hoeveel compartimenten er gecreëerd moeten worden. Als de wens bestaat om al het verkeer te filteren, moet voor elk type applicatie intelligentie binnen de DMZ worden ingebouwd.

Stel vast hoe de storage en back-up infrastructuur wordt ontsloten.

De typen aanvallen met betrekking tot storage en back-up zijn snooping, spoofing en denial of service (DoS). Bij het ontwerp van de storage- en back-up-infrastructuur moet hier uiteraard rekening worden gehouden. Hoe is autorisatie geïmplementeerd met betrekking tot SANs (Storage Area Network), denk hierbij aan 'LUN (Logical Unit Number) masking' en 'zoning'[34]. Als LUN masking wordt geïmplementeerd op HBA-niveau (Host Bus Adapater) is het kwetsbaar voor aanvallen die de HBA compromitteren.

Stel vast welke beheermechanismen toegepast worden.

Maak gebruik van bewezen standaardprotocollen die geen beveiligingsrisico's bevatten of waarvan de beveiligingsrisico's bekend en beheersbaar zijn. Het is dan ook noodzakelijk om vooraf vast te stellen welke beheermechanismen juist wel en welke juist niet toegepast mogen worden. Maak gebruik van versleutelde beheermechanismen en verbied verbindingen die de informatie in cleartext (in onversleutelde vorm) over het netwerk versturen. Voorbeelden van veilige verbindingen zijn:

- Secure Shell (SSH) in plaats van Telnet.
- Secure Copy (SCP), SSH File Transfer Protocol (SFTP) of FTP over SSL (FTPS) in plaats van File Transfer Protocol (FTP).
- HTTPS in plaats van HTTP voor webinterfaces.

Stel vast hoe beheerders toegang krijgen tot het beheergedeelte.

Er moet vastgesteld worden hoe beheerders toegang krijgen tot het beheergedeelte.
Hier zijn verschillende mogelijkheden voor:

- Implementeer beheerclients in het beheergedeelte, die alleen te gebruiken zijn in een afgeschermde ruimte. Beheer over de omgeving kan alleen plaatsvinden via deze fysiek afgeschermde beheerclients.
- Implementeer beheerclients in het beheergedeelte die op basis van een remote interface (bijvoorbeeld Citrix of Microsoft RDP) te benaderen zijn voor een beperkte groep werkstations in het interne netwerk. Beheerders maken vanaf hun werkstation in het LAN een verbinding met de beheerclients en kunnen vervolgens via deze beheerclients het beheer over de omgeving uitvoeren.
- Implementeer een apart beheer-LAN binnen het interne netwerk en sta verbindingen richting het beheergedeelte alleen toe vanuit dit beheer-LAN.
- Implementeer een VPN tunnel op het moment dat het beheer remote via het internet wordt uitgevoerd. Een VPN tunnel kan natuurlijk ook toegepast worden als het beheer vanaf het bedrijfsnetwerk wordt uitgevoerd.

33. Bijvoorbeeld logging, monitoring, analyse- en beheerhulpmiddelen.
34. Verschillende vormen van zoning zijn: hard en soft; port, WWN (World Wide Name).

Vereiste succescriteria (conformiteitvereisten)

- De inrichting van de DMZ is gebaseerd op een vastgesteld inrichtingsdocument/ontwerp waarin is vastgelegd welke uitgangspunten/principes gelden voor de toepassing van de DMZ. Deze ontwerp- en inrichtingskeuzes moeten zijn onderbouwd en op het juiste (organisatie)niveau zijn verantwoord.
- De plaatsing van servers en aansluiting van interne netwerkcomponenten en netwerkkoppelingen met externe netwerken zijn duidelijk en schematisch gedocumenteerd, zodat de werking van de ICT-infrastructuur begrijpelijk is en de impact van wijzigingen goed kunnen worden bepaald.
- De (beveiligings)instellingen van de ICT-componenten zijn zodanig gedocumenteerd dat duidelijk is waarom voor bepaalde instellingen gekozen is (verantwoording en onderbouwing). Besteed hierbij speciale aandacht aan de defaultwaarden voor systeeminstellingen.
- De volgende aandachtspunten moeten worden geadresseerd in het DMZ-inrichtings-document/ontwerp:
  - Welke ondersteunende beheerapplicaties zijn noodzakelijk?
  - Welke compartimenten, koppelvlakken en verkeersstromen tussen de compartimenten zijn noodzakelijk in verband met het beheer?
  - Hoe wordt de storage en back-up infrastructuur ontsloten?
  - Welke vaste routepaden om het verkeer door de DMZ te routeren kunnen worden toegepast?
  - Welke beheermechanismen worden toegepast?
  - Hoe krijgen beheerders toegang tot het beheergedeelte?
- Het DMZ-inrichtingsdocument/ontwerp is actueel en op het juiste (organisatie)niveau vastgesteld.

Classificatie

Hoog

Bewijsvoering

- Het DMZ-inrichtingsdocument/ontwerp met daarin minimaal de aandachtspunten geadresseerd zoals benoemd bij de vereiste succescriteria.

Relatie met andere normen en standaarden

- Informatiebeveiligingsproces, zie maatregel B0-1.
- Risicomanagement, zie maatregel B0-2.
- wijzigingsbeheer, zie maatregel B0-6.
- penetratietesten, zie maatregel B0-8.
- beveiligingstemplates, zie maatregel B2-2.
- Basisnormen Beveiliging en Beheer ICT-infrastructuur
  - hoofdstuk 3 ‘Basisnormen ICT-infrastructuur’
- NEN-ISO/IEC 27002 'Code voor informatiebeveiliging'
  - paragraaf 10.6 ‘Beheer van netwerkbeveiliging’
  - paragraaf 11.4.5 ‘Scheiding van netwerken’
  - paragraaf 11.4.6 ‘Beheersmaatregelen voor netwerkverbindingen’
  - paragraaf 11.4.7 ‘Beheersmaatregelen voor netwerkrouting’
- NORA Dossier Informatiebeveiliging
  - hoofdstuk 5 ‘Zonering’
  - hoofdstuk 6 ‘Filtering’

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B1-3	Netwerkbeveiliging	Netwerktoegang tot de webapplicaties is voor alle gebruikersgroepen op een zelfde wijze ingeregeld.	3.3.4

Doelstelling

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

Rationale

Als webapplicaties ook bereikbaar moeten zijn vanaf het interne netwerk moet hiervoor een koppeling tot stand gebracht worden wat een extra verkeersstroom introduceert (zie maatregel B1-1). Deze extra verkeersstroom mag natuurlijk geen (nieuwe) beveiligingsrisico's introduceren.
Er moet worden voorkomen dat beveiligingsbeperkingen die zijn opgelegd door componenten in de DMZ (onbedoeld) door interne medewerkers worden omzeild. Gebruikers binnen de organisaties moeten dezelfde netwerkmaatregelen voorgeschoteld krijgen als gebruikers van buiten de organisatie[35][36]. Het is dan ook van belang om vastgestelde routepaden (zie maatregel B1-1) ook voor intern netwerkverkeer te bekrachtigen. Hierdoor zal intern netwerkverkeer in grote lijnen dezelfde weg moeten volgen als internetverkeer, met als gevolg dat intern netwerkverkeer op dezelfde plek de DMZ moet binnenkomen als regulier internetverkeer. Dit geldt voor productieverkeer en niet voor netwerkverkeer in verband met beheerdoeleinden, zoals in maatregel B1-2 beschreven.

Vereiste succescriteria (conformiteitvereisten)

- De inrichting van de DMZ is gebaseerd op een vastgesteld inrichtingsdocument/ontwerp waarin is vastgelegd welke uitgangspunten/principes gelden voor de toepassing van de DMZ. Deze ontwerp en inrichtingskeuzes moeten zijn onderbouwd en op het juiste (organisatie)niveau zijn verantwoord.
- De plaatsing van servers en aansluiting van interne netwerkcomponenten en netwerkkoppelingen met externe netwerken zijn duidelijk en schematisch gedocumenteerd, zodat de werking van de ICT-infrastructuur begrijpelijk is en de impact van wijzigingen goed kunnen worden bepaald.
- De (beveiligings)instellingen van de ICT-componenten zijn zodanig gedocumenteerd dat duidelijk is waarom voor bepaalde instellingen gekozen is (verantwoording en onderbouwing). Besteed hierbij speciale aandacht aan de defaultwaarden voor systeeminstellingen.
- De volgende aandachtspunten moeten worden geadresseerd in het DMZ-inrichtingsdocument/ontwerp:
  - Hoe verloopt de interne/externe routering van webverkeer?
  - Welke vaste routepaden om het verkeer door de DMZ te routeren kunnen worden toegepast.
  - Welke beheermechanismen worden toegepast.
- Het DMZ-inrichtingsdocument/ontwerp is actueel en op het juiste (organisatie)niveau vastgesteld.

Classificatie

Hoog

35. Het gaat hierbij om beveiligingsmaatregelen (bijvoorbeeld interne routering) met betrekking tot het webverkeer en niet over andere beveiligingsmaatregelen zoals toegangsmechanismen.
36. Een interne medewerker moet net zo min worden vertrouwd als een willekeurige gebruiker op het internet. Om aanvallen van binnenuit effectief te kunnen beperken is het daarom van belang dat je dezelfde beperkingen oplegt aan een externe gebruiker als aan een interne gebruiker.

Bewijsvoering

- Het DMZ-inrichtingsdocument/ontwerp met daarin minimaal de aandachtspunten geadresseerd zoals benoemd bij de vereiste succescriteria.

Relatie met andere normen en standaarden

- Informatiebeveiligingsproces, zie maatregel B0-1.
- Risicomanagement, zie maatregel B0-2.
- Basisnormen Beveiliging en Beheer ICT-infrastructuur.
  - hoofdstuk 3 ‘Basisnormen ICT-infrastructuur’.
- NEN-ISO/IEC 27002 'Code voor informatiebeveiliging'.
  - paragraaf 10.6 ‘Beheer van netwerkbeveiliging’.
  - paragraaf 11.4.5 ‘Scheiding van netwerken’.
  - paragraaf 11.4.6 ‘Beheersmaatregelen voor netwerkverbindingen’.
  - paragraaf 11.4.7 ‘Beheersmaatregelen voor netwerkrouting’
- NORA Dossier Informatiebeveiliging.
  - hoofdstuk 5 ‘Zonering’.
  - hoofdstuk 6 ‘Filtering’.

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B1-4	Netwerkbeveiliging	Netwerkcompartimenten bevatten geen fysieke koppelingen door middel van gedeelde componenten.	3.3.8

Doelstelling

Voorkom het omzeilen van logische scheidingen door fysieke scheiding van netwerkcomponenten.

Rationale

Bij het ontwerpen/inrichten van de DMZ (zie maatregel B1-1) wordt tenminste een logische scheiding van netwerkcompartimenten rondom de firewall(s) gecreëerd. Deze logische scheiding betekent niet per definitie ook een fysieke scheiding van netwerkcompartimenten. Verschillende netwerkcomponenten, servers en andere apparatuur kunnen immers wel aangesloten zijn op dezelfde switch of hub. In dat geval vormt de hub of switch een fysieke koppeling (bypass). Hierdoor is het mogelijk om de logische compartimentering van het netwerk via deze netwerkcomponenten te omzeilen.

Maak voor de fysieke scheiding van netwerkcompartimenten gebruik van één van de twee onderstaande mogelijkheden:

1. Netwerksegmenten zijn gescheiden door een firewall en interfaces naar verschillende netwerksegmenten (bijvoorbeeld naar de DMZ en naar de backoffice) gebruiken verschillende (fysieke) netwerkcomponenten.

2. Er worden (reverse) proxies inline geplaatst. Inline plaatsing houdt in dat de proxies twee interfaces krijgen: één interface voor de het externe netwerk (buitenkant) en één interface voor het interne netwerk (binnenkant). Al het verkeer van en naar de webapplicatie is in dit geval verplicht om via de proxy te lopen. Het nadeel van een dergelijke plaatsing van een proxy is dat alle webapplicaties via deze proxy moeten verlopen waardoor men afhankelijk is van ondersteuning van de proxy voor het specifieke type verkeer (bijvoorbeeld een HTTP-proxy voor webverkeer, een SMTP-proxy voor e-mailverkeer, et cetera). De mogelijkheid tot het inline plaatsen van een proxy is dan ook zeer afhankelijk van de andere webapplicaties die de organisatie via de DMZ ontsluit.

OPMERKING 1: Bij het gebruik van inline proxies is het van belang dat de twee interfaces gebruik maken van verschillende switches. Plaatst men de componenten uit de compartimenten die de proxy van elkaar scheidt in dezelfde switches, dan kan de logische compartimentering van het netwerk alsnog worden omzeild.
OPMERKING 2: Bij de toepassing van twee interfaces binnen één server is in strikte zin nog niet echt sprake van een fysieke scheiding.

De mate van gewenstheid van deze beveiligingsrichtlijn hangt af van de risicoanalyse (zie maatregel B0-2) en zakelijke behoeften. Daarbij wordt gekeken naar de kans op optreden van bedreigingen en de mogelijke impact hiervan op de bedrijfsvoering.

Vereiste succescriteria (conformiteitvereisten)

- De inrichting van de DMZ is gebaseerd op een vastgesteld inrichtingsdocument/ontwerp waarin is vastgelegd welke uitgangspunten/principes gelden voor de toepassing van de DMZ. Deze ontwerp- en inrichtingskeuzes moeten zijn onderbouwd en op het juiste (organisatie)niveau zijn verantwoord.
- De plaatsing van servers en aansluiting van interne netwerkcomponenten en netwerkkoppelingen met externe netwerken zijn duidelijk en schematisch gedocumenteerd, zodat de werking van de ICT-infrastructuur begrijpelijk is en de impact van wijzigingen goed kunnen worden bepaald.
- De volgende aandachtspunten moeten worden geadresseerd in het DMZ-inrichtingsdocument/ontwerp:
  - Hoe verloopt de interne/externe routering van webverkeer?
  - Welke vaste routepaden om het verkeer door de DMZ te routeren kunnen worden toegepast?
- Het DMZ-inrichtingsdocument/ontwerp is actueel en op het juiste (organisatie)niveau vastgesteld.

Classificatie

Hoog

Bewijsvoering

- Het DMZ-inrichtingsdocument/ontwerp met daarin minimaal de aandachtspunten geadresseerd zoals benoemd bij de vereiste succescriteria.

Relatie met andere normen en standaarden

- Informatiebeveiligingsproces, zie maatregel B0-1.
- Risicomanagement, zie maatregel B0-2.

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B1-5	Netwerkbeveiliging	Implementeer maatregelen tegen (d)DoS.	3.3.9

Doelstelling

Beperken impact van (d)DoS aanvallen.

Rationale

Het GOVCERT.NL whitepaper 'Aanbevelingen ter bescherming tegen Denial-of-Service-aanvallen'[10] beschrijft een aantal maatregelen om zichzelf tegen (d)DoS-aanvallen te beschermen. De maatregelen die dit whitepaper voorstelt, zijn hieronder kort samengevat:

- Maak gebruik van anti-spoofingmechanismen:
  - Unicast Reverse-Path Forwarding (uRPF).
    URPF controleert op een interface of een IP-pakket afkomstig is van een bron IP-adres dat volgens de routeringstabel bereikbaar is via de betreffende interface.

  - Bogon lijst.
    Een bogon lijst[37] bevat een overzicht van alle IP-blokken die nog niet door IANA zijn uitgegeven en waarvandaan dus ook nooit verkeer afkomstig kan zijn. Een dergelijke bogon lijst kan als basis voor de rulebase van elke firewall gebruikt worden.
  - Access Control Lists (ACL).
    Reguleer dataverkeer op basis van bijvoorbeeld IP-adres of poortnummer.
- Zet firewalls in.
  Voorkom dat Stateful firewalls en Intrusion Prevention apparatuur gebruikt worden als beschermingsmaatregel direct voor de website. Deze apparatuur kan namelijk de DoS versterken. Het is beter om netwerk policies te implementeren op routers en switches. Als toch gebruik wordt gemaakt van firewalls die kunnen meekijken en ingrijpen op applicatieniveau, maak dan gebruik van software op de webserver zelf (zie maatregel B2-4).
- Harden systemen. Vooral het 'tunen' van de TCP/IP-stack kan helpen in het beveiligen tegen (d)DoS-aanvallen (zie maatregel B0-5).
- Besteed aandacht aan de netwerkomgeving (zie maatregel B1-1), bijvoorbeeld:
  - Implementeer IDMS[38] (Intelligent dDoS Mitigation System) en RTBH[39] (Remotely-Triggered Black Hole). Deze maatregelen voorkomen overbelasting van web-, DNS- en mailservers. Ze zijn ook een goede oplossing als stateful apparatuur om wat voor reden dan ook, niet uit het netwerk verwijderd mag of kan worden. Daarnaast zijn ze in staat om loadbalancers te beschermen.
  - Zorg ervoor dat authoratieve DNS-servers en recursive/caching DNS-servers logisch gescheiden zijn, door ze in aparte netwerken te plaatsen.
- Maak afspraken met (hosting) providers.
  De rol van de provider wordt soms over het hoofd gezien of onderschat. De meeste (hosting) providers kunnen op de volgende gebieden helpen en maak hierover afspraken:
  - Een goed anti-spoofing mechanisme blokkeert verkeer dat afkomstig is van RFC19185 IP-adressen of van adressen die de Internet Assigned Numbers Authority[40] (IANA) nog niet heeft gealloceerd[41].
  - Een detectiemechanisme, zoals Netflow, kan een DoS-aanval signaleren.
  - Krachtige systemen, zoals routers, kunnen effectief een DoS-aanval stoppen of beperken.
  - Upstream-providers en andere netwerkrelaties van uw provider kunnen aanvallen uit andere netwerken blokkeren.
- Monitor actief het inkomende en uitgaande verkeer in het netwerk zodat in een vroeg stadium gereageerd kan worden op (d)DoS-aanvallen. Maak hiervoor gebruik van bijvoorbeeld een tool als Netflow. Voorbeelden van open source software voor de analyse van Netflow-data zijn NFSen[42] en NFDump[43].

De afweging in welke mate aan deze maatregel wordt voldaan, hangt af van de risicoanalyse (zie maatregel B0-2) en zakelijke behoeften. Daarbij wordt gekeken naar de kans op optreden en de mogelijke impact.

37. Team Cymru, een non-profit beveiligingsorganisatie, biedt via haar website een bogon lijst aan. De actuele lijst wordt dor Team Cymru aangeboden via de volgende URL: http://www.cymru.com/Documents/bogon-list.html
38. http://www.arbornetworks.com/en/docman/the-growing-need-for-intelligent-ddos-mitigation-systems/download.html
39. http://tools.ietf.org/pdf/rfc5635.pdf
40. http://www.iana.org/
41. Voor een overzicht van IP-blokken die door IANA nog niet zijn uitgedeeld aan een Local Routing Registry (LIR) vindt op http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml
42. http://nfsen.sourceforge.net
43. http://nfdump.sourceforge.net

Het GOVCERT.NL factsheet 'FS 2010-03: Bescherm uw online dienst(en) tegen (d)DoS-aanvallen' [44] zet in deze factsheet doelwitten en gevolgen van DoS-aanvallen uiteen en legt uit hoe u zich kunt beschermen.

Vereiste succescriteria (conformiteitvereisten)

- De inrichting van de DMZ is gebaseerd op een vastgesteld inrichtingsdocument/ontwerp waarin is vastgelegd welke uitgangspunten/principes gelden voor de toepassing van de DMZ. Deze ontwerp- en inrichtingskeuzes moeten zijn onderbouwd en op het juiste (organisatie)niveau zijn verantwoord.
- Het volgende aandachtspunt moet worden geadresseerd in het DMZ-inrichtingsdocument/ontwerp:
  - Welke maatregelen zijn geïmplementeerd om de impact van (d)DoS aanvallen te beperken (minimaliseren van de gevolgen)?
- Het DMZ-inrichtingsdocument/ontwerp is actueel en op het juiste (organisatie)niveau vastgesteld.
- De zakelijke behoeften moeten zijn vastgesteld en er moet een risicoanalyse zijn uitgevoerd.

Classificatie

Midden

Bewijsvoering

- Het DMZ-inrichtingsdocument/ontwerp met daarin minimaal de aandachtspunten geadresseerd zoals benoemd bij de vereiste succescriteria.
- Resultaten van de risicoanalyse waaruit blijkt waarom wel of niet wordt voldaan aan deze maatregel.

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B1-6	Netwerkbeveiliging	Implementeer maatregelen zodat het netwerk geen Single Points-of-Failure (SPOF) bevat.	3.3.12

Doelstelling

Voorkom uitval (beschikbaarheid) van de (netwerk)omgeving.

Rationale

Het netwerk vormt de basis(infrastructuur) voor webapplicaties, daarom is het van belang dat het netwerk te maken krijgt met een minimum aan storingen. Het ontwerp van het netwerk dient daarom zodanig te zijn dat deze zo min mogelijk (liefst geen) Single Points-of-Failure (SPOF) bevat. Load balancing en redundantie zijn twee technieken die ingezet kunnen worden om de beschikbaarheid van de infrastructuur te vergroten.
Naast het feit dat het ontwerp van het netwerk zo moet zijn dat er zo min mogelijk (liefst geen) uitval zal plaatsvinden, is ook een adequate monitoring, alerting, bewaking en auditing van belang (zie hoofdstuk 9 'Monitoring, auditing en alerting').

Load balancers

Load balancers kunnen verkeer voor een webapplicatie over verschillende gelijkwaardige componenten verdelen. Voor webapplicaties bestaan twee belangrijke load balancing technieken:

- Local Server Load Balancing (LSLB).
  Een 'LSLB load balancer' verdeelt verkeer lokaal (dat wil zeggen binnen hetzelfde

44. http://www.govcert.nl/dienstverlening/Kennis+en+publicaties/factsheets/factsheet-over-bescherming-tegen-dos-aanvallen.html

datacenter) over verschillende webservers. Uitval van een webserver zal in dit geval niet per definitie leiden tot het niet meer beschikbaar zijn van de website doordat een andere webserver nog wel beschikbaar is.
- Global Server Load Balancing (GSLB).
  Een 'GSLB load balancer' is een stuk complexer dan een 'LSLB load balancer' en heeft als doel om load balancing uit te voeren over geografisch gescheiden locaties. DNS-functionaliteit is een mechanisme om GSLB voor webapplicaties te bewerkstelligen. De 'GSLB load balancer' is hierbij autoritatief voor de zone waarin de webapplicatie zich bevindt en fungeert voor deze zone als DNS-server. Door verzoeken voor de zone te beantwoorden met steeds wisselende IP-adressen, komen gebruikers uit op de verschillende geografisch gescheiden locaties

Welke load balancing oplossing het meest geschikt is voor een bepaalde webapplicatie, is afhankelijk van verschillende variabelen zoals het beschikbare budget, het ontwerp van het netwerk en de architectuur van de webapplicatie (zie maatregel B1-1).

Redundantie

Veel netwerkcomponenten bieden standaard ondersteuning voor redundantie en bijbehorende statussynchronisatie. Netwerkcomponenten die in aanmerking komen voor redundante uitvoering zijn:
- Communicatieverbindingen
- Firewalls
- Load balancers
- Proxies
- Routers
- Switches
- et cetera

Maar denk ook aan redundant uitvoeren van componenten zoals:
- Energievoorziening;
- Koeling/klimaatbeheersing
- Voeding
- Controllers
- et cetera

Vereiste succescriteria (conformiteitvereisten)
- De inrichting van de DMZ is gebaseerd op een vastgesteld inrichtingsdocument/ontwerp waarin is vastgelegd welke uitgangspunten/principes gelden voor de toepassing van de DMZ. Deze ontwerp en inrichtingskeuzes moeten zijn onderbouwd en op het juiste (organisatie)niveau zijn verantwoord.
- De volgende aandachtspunten moeten worden geadresseerd in het DMZ-inrichtingsdocument/ontwerp:
  - Welke maatregelen zijn geïmplementeerd zodat SPOFs worden voorkomen of de gevolgen worden geminimaliseerd?
- Het DMZ-inrichtingsdocument/ontwerp is actueel en op het juiste (organisatie)niveau vastgesteld.
- De zakelijke behoeften moeten zijn vastgesteld en er moet een risicoanalyse zijn uitgevoerd.

Classificatie

Midden

Bewijsvoering

- Het DMZ-inrichtingsdocument/ontwerp met daarin minimaal de aandachtspunten geadresseerd zoals benoemd bij de vereiste succescriteria.
- Resultaten van de risicoanalyse waaruit blijkt waarom wel of niet wordt voldaan aan deze maatregel.

Relatie met andere normen en standaarden

- Maatregelen uit hoofdstuk 9 ‘Monitoring, auditing en alerting’.

HOOFDSTUK 4

Platvormbeveiliging

Het platform waarop een webapplicatie draait, is in de regel een besturingssysteem als Windows of Linux-/UNIX-varianten. Ditzelfde geldt voor applicaties waarvan een webapplicatie gebruik maakt zoals applicatieservers en databaseservers.

Als eerste wordt een overzicht gegeven van de mogelijke kwetsbaarheden en bedreigingen die er bestaan op het gebied van platformen en geeft tevens aanbevelingen om het risico bij deze kwetsbaarheden en bedreigingen te verlagen.

Platformbeveiliging richt zich op het beveiligen van de verschillende platformen (zoals besturingssystemen en firmware van bijvoorbeeld routers) waarvan webapplicaties - en aanverwante componenten zoals databases - gebruik maken.

4.1 Kwetsbaarheden en bedreigingen

Het platform bevindt zich tussen het netwerk en de webapplicatie. In sommige gevallen zijn de services die het platform aanbiedt rechtstreeks via internet te benaderen, waardoor kwetsbaarheden in het platform direct de beveiliging van de webapplicatie in gevaar brengen.

Mogelijke kwetsbaarheden en bedreigingen zijn:

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
K2-1	Platformbeveiliging	Kwetsbaarheden in het besturingssysteem	4.2.1

Toelichting

Niet alle kwetsbaarheden met betrekking tot besturingssystemen hebben direct gevolgen voor servers die in gebruik zijn door webapplicaties. Dit komt voornamelijk doordat webservers in de regel slechts bereikbaar zijn op een beperkt aantal poorten. Wanneer een kwetsbaarheid in het besturingssysteem aanwezig is die kwaadwillenden via de webserver kunnen misbruiken (bijvoorbeeld met de mogelijkheid om willekeurige code uit te voeren), dan kan dit ernstige gevolgen hebben voor alle webapplicaties die van deze server gebruik maken.

TREND: Kwaadwillenden zijn steeds sneller in staat om exploits voor deze kwetsbaarheden te schrijven en als een kwetsbaarheid op veel servers aanwezig is zullen kwaadwillenden veel moeite doen om deze uit te kunnen buiten. Dit heeft tot gevolg dat leveranciers steeds minder tijd hebben om bekende kwetsbaarheden te patchen.

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
K2-2	Platformbeveiliging	Onveilige beheermechanismen	4.2.2

Toelichting

Het beheer van servers kan op verschillende manieren plaatsvinden.
Enkele van de meest gebruikte beheermechanismen zijn:

- Consoleverbindingen.
  Een consoleverbinding kan normaal gesproken alleen worden gemaakt via fysieke toegang tot de server. Tegenwoordig bestaan er echter ook apparaten waarmee deze consoleverbinding via het netwerk (op basis van bijvoorbeeld Telnet of SSH) kan worden benaderd.
- Telnet.
  Via telnet kan een command-line sessie worden geopend met een server. Telnet is een verouderd mechanisme dat vanwege het ontbreken van goede beveiligingsmechanismen steeds minder vaak wordt toegepast.
- Secure Shell (SSH).
  Via een SSH-verbinding kan een veilige (versleutelde) verbinding opgezet worden tussen een client en een server. Optioneel kan SSH gebruik maken van certificaten om wederzijdse authenticatie te laten plaatsvinden. Via SSH kan een command-line sessie worden geopend met een server. Het is echter ook mogelijk om andere functionaliteiten (zoals het kopiëren van bestanden via Secure Copy) via een SSH-verbinding te tunnelen.
- File Transfer Protocol (FTP).
  Via FTP kunnen bestanden worden uitgewisseld tussen een client en een server. FTP maakt gebruik van authenticatie op basis van een gebruikersnaam en wachtwoord. Deze gegevens verstuurt de FTP-client in cleartext (in onversleutelde vorm) over het netwerk. Dit laatste is één van de belangrijkste redenen dat het gebruik van FTP onveilig is.

- Webinterface.
  Veel systemen bieden tegenwoordig een webinterface waarmee beheerders de belangrijkste beheeractiviteiten kunnen uitvoeren. Een dergelijke webinterface kan gebruik maken van bestaande beveiligingsmechanismen zoals versleuteling via SSL, authenticatie op basis van X.509-certificaten, et cetera.

Beheermechanismen op basis van een onversleutelde verbinding brengen altijd een beveiligingsrisico met zich mee. Wanneer een organisatie dergelijke beheermechanismen ook toestaat over het internet, vergroot dit de kans dat kwaadwillenden deze authenticatiegegevens onderscheppen (zie maatregel B1-12).

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
K2-3	Platformbeveiliging	Onjuiste autorisaties	4.2.3

Toelichting
Het is van belang om de rechten die worden toekent aan processen, het bestandssysteem, het register, et cetera zoveel mogelijk in te perken. Het principe dat iets of iemand voor een taak niet meer rechten krijgt toegekend dan strikt noodzakelijk, wordt in het Engels ook wel het 'least privilege'-principe genoemd. Het is één van de basisuitgangspunten voor goede informatiebeveiliging, dat niet alleen wordt toegepast op mensen, maar ook op programma's en processen. De argumenten voor dit uitgangspunt zijn kortweg dat (1) iemand zijn werk moet kunnen doen en dat (2) in het geval van een incident, de schade zoveel mogelijk beperkt moet blijven. Op het moment dat dit 'least privilege'-principe niet wordt gevolgd, kunnen onveilige situaties ontstaan. Het foutief inrichten van rechten kan in de praktijk tot een grote verscheidenheid aan beveiligingsproblemen leiden.
Koppel altijd rechten aan processen, bestanden, directories, et cetera.
Als een webserver niet op een juiste manier is ingericht, kunnen kwaadwillenden dit uitbuiten.

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
K2-4	Platformbeveiliging	Onnodige service	4.2.4

Toelichting
Niet alle geactiveerde services na de installatie van een besturingssysteem zullen nodig zijn. Elke service op een platform kan kwetsbaarheden bevatten en vormt daarmee een potentieel lek.

4.2 Doelstelling

Het ontwerpen, inrichten en handhaven van de beveiliging voor platformen/ besturingssystemen zodat deze systemen beter bestand zijn tegen aanvallen van kwaadwillenden.

4.3 Beveiligingsrichtlijnen

De paragraaf besteedt aandacht aan de maatregelen om platformbeveiliging voor webapplicaties in te richten, deze maatregelen hebben allemaal als doel het besturingssysteem te hardenen (zie maatregel B0-5). Hardening houdt in dat je het besturingssysteem zo inricht, dat dit systeem beter bestand is tegen aanvallen van kwaadwillenden. De technische stappen die nodig zijn om een besturingssysteem te hardenen verschillen per type besturingssysteem. De logische stappen verschillen echter veel minder. De maatregelen uit deze paragraaf zijn dan ook generiek van aard.

Per maatregel wordt ook beschreven hoe deze stap er op een specifiek type besturingssysteem uitziet. Specifieke maatregelen voor de verschillende besturingssystemen zoals Microsoft Windows, verschillende UNIX en Linux distributies worden aangeboden door de 'Security Benchmarks division'[45].

CIS Security Benchmarks Division

De 'Security Benchmarks division' (voorheen het Center for Internet Security) helpt organisaties hun informatiebeveiliging te verbeteren door het verminderen van het risico als gevolg van ontoereikende technische beveiligingsmaatregelen. Om dit te bereiken faciliteert de Security Benchmarks division de op consensus gebaseerde ontwikkeling van (1) best practices (maatregelen) voor beveiligingsconfiguratie, (2) tools voor het meten van de status van informatiebeveiliging, en (3) hulpmiddelen om weloverwogen investeringsbeslissingen op het gebied van informatiebeveiliging te kunnen nemen. De Security Benchmarks division heeft een reputatie als een betrouwbare, onafhankelijke instantie die de samenwerking tussen publieke en private industrie experts faciliteert om op deze manier consensus te bereiken over praktische en uitvoerbare oplossingen. De hulpmiddelen (benchmarks) die worden aangeboden door de Security Benchmarks division worden (vaak) gezien als de de facto beveiligingsconfiguratie maatregelen en worden gebruikt bij het uitvoeren van audits. De CIS benchmarks ontwikkelt en toegepast door zowel de overheid, het bedrijfsleven, de industrie als de academische wereld zijn hier te downloaden https://benchmarks.cisecurity.org/en-us/?route=downloads.multiform.

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B2-1	Platformbeveiliging	Maak gebruik van veilige beheermechanismen.	4.3.8

Doelstelling

Voorkom misbruik van beheervoorzieningen.

Rationale

Maak gebruik van bijvoorbeeld SSH in plaats van Telnet. Zorg er daarnaast voor dat beheerinterfaces alleen bereikbaar zijn vanaf een gescheiden beheernetwerk (zie maatregel B1-2).

Het gebruik van 'backdoors' moet absoluut uitgesloten zijn. Een backdoor voor beheer is bijvoorbeeld een beheerinterface waarvoor geen authenticatie nodig is maar die draait op poort 8888 en daardoor moeilijk te ontdekken zou moeten zijn ('security through obscurity'). De kans is echter groot dat kwaadwillenden backdoors vroeg of laat ontdekken, en erin slagen om deze te misbruiken.

Vereiste succescriteria (conformiteitvereisten)

- Zorg dat procedures met betrekking tot beheermechanismen zijn vastgesteld.

Classificatie

Hoog

Bewijsvoering

- Procedurebeschrijving met betrekking tot beheermechanismen.

Relatie met andere normen en standaarden

Nauwe relatie met maatregel B1-2

45. Https://benchmarks.cisecurity.org/en-us/?route=default

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B2-2	Platformbeveiliging	Maak gebruik van beveiligingstemplates bij de beveiliging van systemen.	4.3.12

Doelstelling

Alle systemen worden conform een vastgestelde wijze ingericht/gehardend (en niet conform de kennis van een willekeurige beheerder).

Rationale

De hardeningsmaatregelen moeten worden opgenomen in beveiligingstemplates die als basis fungeren om systemen veilig in te richten. Bij het opstellen van beveiligingstemplates is het gebruikte besturingssysteem en de rol van het systeem (bijvoorbeeld webserver, databaseserver, et cetera) relevant.
Beveiligingstemplates bestaan uit documenten die de hardening beschrijven en worden technisch ondersteund door scripts, images, configuratiebestanden, et cetera.
De noodzaak van de beveiligingsrichtlijn neemt toe naar mate de schaalgrootte van een serverpark toeneemt. Ook wanneer er slechts van één of enkele servers gebruik wordt gemaakt is het gebruik van beveiligingstemplates echter aan te bevelen. Deze bieden in alle gevallen een middel om de inrichting gestructureerd en doordacht op te zetten.
Voorbeelden van handleidingen die kunnen worden gehanteerd bij het opstellen van beveiligingstemplates zijn:

- Microsoft:
  - Windows Server 2003 Security Guide:
    http://www.microsoft.com/downloads/details.aspx?familyid=8a2643c1-0685-4d89-b655-521ea6c7b4db
  - The Threats and Countermeasures Guide:
    http://www.microsoft.com/downloads/details.aspx?FamilyID=1b6acf93-147a-4481-9346-f93a4081eea8&DisplayLang=en
- Red Hat
  - Security Guide - A Guide to Securing Red Hat Enterprise Linux 6:
    http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/6/html/Security_Guide/
- SANS Institute
  - Firewall Checklist
    http://www.sans.org/score/checklists/FirewallChecklist.pdf
  - Oracle Database Security Checklist
    http://www.sans.org/score/checklists/Oracle_Database_Checklist.pdf
  - Linux Security Checklist
    http://www.sans.org/score/checklists/linuxchecklist.pdf

Vereiste succescriteria (conformiteitvereisten)

- Zorg voor een actueel overzicht van beveiligingstemplates en zorg dat deze continue worden onderhouden.
- Zorg dat de beveiligingstemplates onderdeel zijn van het proces wijzigingsbeheer (zie maatregel B0-6).

Classificatie

Midden

Bewijsvoering

- Actueel overzicht van de beveiligingstemplates.
- Procedurebeschrijving met betrekking tot het creëren en onderhouden van beveiligingstemplates.

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B2-3	Platformbeveiliging	Maak gebruik van jailing (sandboxing)	4.3.6

Doelstelling
Beperk de schade bij misbruik van processen.

Rationale
Het is een manier om een proces te ISOleren van de rest van een besturingssysteem.
Een bekende implementatie hiervan is chroot. Het commando chroot wijzigt de root-directory voor een proces (change root). Door een proces via chroot te laten werken, heeft het proces geen toegang meer tot bestanden die zich buiten deze root-directory bevinden. Dit mechanisme kan bijvoorbeeld worden ingezet om een Apache-server geïsoleerd te laten draaien.
Naast het afschermen van directories via chroot bestaan er ook mechanismen om andere delen van het besturingssysteem af te schermen; voorbeelden zijn het beperken van I/O rates, het beperken van het toegestane hoeveelheid geheugen en het beperken van de toegestane hoeveelheid CPU-cycles.
Virtualisatie is een vorm van afscherming van processen door volledig autonome besturingssystemen naast elkaar te laten functioneren.
Jailing (sandboxing) is een mechanisme dat voornamelijk op het Linux- en UNIX-platform bestaat, maar kan ook in andere omgevingen gerealiseerd worden.

Vereiste succescriteria (conformiteitvereisten)
- De inrichting van de decentrale systemen is gebaseerd op een vastgesteld inrichtings-document/ontwerp waarin is vastgelegd welke functie deze decentrale systemen vervullen. Denk hierbij aan welke software (applicaties) is hierop geïnstalleerd, welke (netwerk)protocollen zijn noodzakelijk, et cetera.
- Zorg dat het inrichtingsdocument/ontwerp onderdeel is van het proces wijzigingsbeheer.
- Het inrichtingsdocument/ontwerp:
  - heeft een eigenaar.
  - is voorzien van een datum en versienummer.
  - bevat een documenthistorie (wat is wanneer en door wie aangepast).
  - is actueel, juist en volledig.
  - is door het juiste (organisatorische) niveau vastgesteld/geaccordeerd

Classificatie
Midden

Bewijsvoering
- Het inrichtingsdocument/ontwerp

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B2-4	Platformbeveiliging	Maak gebruik van lokale firewalls	4.3.10

Doelstelling
Het controleren van het netwerkverkeer, zowel op poort- als procesniveau, dat lokaal binnenkomt en uitgaat.

Rationale
In hoofdstuk 3 is beschreven hoe centraal geplaatste firewalls de omgeving beschermen tegen kwaadwillenden (zie maatregel B1-1). Naast deze centrale firewalls is het gewenst om decentraal, op de verschillende machines, een aparte firewall te laten werken. Deze lokale

(decentrale) firewalls, dit kan een aparte (host) firewall zijn of de firewall functionaliteit wordt aangeboden door het besturingssysteem zelf, vormen daarmee een extra laag in de beveiliging. Enkele voorbeelden van deze firewalls zijn: Ipfw, Pf, Iptables, Ipfilter (ipf) en Microsoft Windows Firewall.
Lokale firewalls hebben als voordeel dat deze zowel op poort- als procesniveau controles uitvoeren. Verder hebben lokale firewalls vaak meer inzicht in het binnenkomende verkeer omdat op de machine zelf ontsleuteling van versleutelde tunnels plaatsvindt. Daarnaast bevatten lokale firewalls vaak veel minder regels in de rulebase waardoor fouten in de configuratie minder aannemelijk zijn.
Tot slot bieden deze firewalls veelal ook uitgebreide mogelijkheden op het gebied van logging en Network Address Translation (NAT).

Vereiste succescriteria (conformiteitvereisten)

- De inrichting van de decentrale systemen is gebaseerd op een vastgesteld inrichtingsdocument/ontwerp waarin is vastgelegd welke functie deze decentrale systemen vervullen. Denk hierbij aan welke software (applicaties) is hierop geïnstalleerd, welke (netwerk)protocollen zijn noodzakelijk, et cetera.
- Zorg dat het inrichtingsdocument/ontwerp onderdeel is van het proces wijzigingsbeheer.
- Het inrichtingsdocument/ontwerp:
  - heeft een eigenaar.
  - is voorzien van een datum en versienummer.
  - bevat een documenthistorie (wat is wanneer en door wie aangepast).
  - is actueel, juist en volledig.
  - is door het juiste (organisatorische) niveau vastgesteld/geaccordeerd

Classificatie

Midden

Bewijsvoering

- Het inrichtingsdocument/ontwerp

HOOFDSTUK 5

Applicatiebeveiliging

Daar waar netwerkbeveiliging zich richt op het afschermen van het netwerk op basis van te onderscheiden protocollen, zal applicatiebeveiliging een niveau dieper gaan en de inhoud van de protocollen willen bekijken. De nadruk bij het beveiligen van webapplicaties ligt op dit niveau.

Applicatiebeveiliging richt zich op het beveiligen van de webapplicatie en het applicatieplatform. Applicatiebeveiliging hoeft geen geïntegreerd onderdeel van de webapplicatie zelf te zijn, maar kan ook als losstaand component functioneren in de infrastructuur van de webapplicatie. Een firewall op applicatieniveau (Web Application Firewall) is een typisch losstaande component dat geen geïntegreerd onderdeel van de applicatie is, maar wel beveiligingservices biedt aan deze applicatie.

Deze paragraaf beschrijft de meest voorkomende kwetsbaarheden in webapplicaties.

De meest bekende kwetsbaarheden in webapplicaties zijn ongetwijfeld XSS en SQL-injectie. Ondanks deze bekendheid komen beide kwetsbaarheden nog steeds veelvuldig voor in webapplicaties.
Deze twee kwetsbaarheden staan dan ook op nummer 1 en 2 in OWASP Top-10 2010.

Mogelijke kwetsbaarheden en bedreigingen zijn:

Nr.	Beveiligingslaag	Kwetsbaarheid	Referentie RBW
K3-1	Applicatiebeveiliging	SQL-injectie	5.2.1

Toelichting
Webapplicaties maken vaak gebruik van databases voor het opslaan en oproepen van allerhande informatie. Structured Query Language (SQL) is de taal die elke database ondersteunt om toegang tot deze informatie mogelijk te maken.
Databases lijken tegenwoordig kleine besturingssystemen, aangezien de acties die men via queries (of stored procedures) kan uitvoeren steeds krachtiger en uitgebreider worden.
Hieronder volgt een kleine opsomming de mogelijkheden die SQL biedt:

- Elke database biedt de mogelijkheid om informatie uit de database op te vragen (SELECT), te verwijderen (DELETE) en te wijzigen (UPDATE). Daarnaast is het uiteraard mogelijk om nieuwe informatie aan de database toe te voegen (INSERT). Deze functionaliteiten vormen de basis van elke database.
- Databases bieden vaak de mogelijkheid om DNS-verzoeken uit te voeren (bijvoorbeeld utl_inaddr.get_host_address in Oracle) waardoor men vanuit de database hostnamen kan omzetten naar IP-adressen.
- Vaak is het mogelijk om via de aanroep van een stored procedure (bijvoorbeeld xp_sendmail in Microsoft SQL Server), mail te versturen. Daarbij biedt de database vaak de mogelijkheid om de inhoud van de mail te baseren op de uitvoer van een query.
- Het inlezen van een webpagina behoort ook vaak tot de mogelijkheden van een database (bijvoorbeeld utl_http.request in Oracle).
- Sommige databases bieden zelfs de mogelijkheid om commando's op OS-niveau aan te roepen (bijvoorbeeld xp_cmdshell in Microsoft SQL Server).

Deze functionaliteiten kunnen zeer nuttig zijn voor ontwikkelaars en de mogelijkheid bieden om in korte tijd een complexe webapplicatie te implementeren. Nadeel is dat de schade door kwetsbaarheden in de webapplicatie erg groot kan worden. Daarom is SQL-injectie een belangrijke bedreiging.

Een SQL-injectiekwetsbaarheid ontstaat door onvoldoende controles op de invoer van gebruikersdata en door onveilige programmeergewoonten. De aanwezigheid van een SQL-injectiekwetsbaarheid betekent dat iedereen vanaf internet in staat is om de SQL-verzoeken die de webapplicatie verstuurt naar de database, te manipuleren. Daarbij heeft de aanvaller vaak toegang tot alle functionaliteiten die de database biedt. De gevolgen van deze kwetsbaarheid zijn in grote mate afhankelijk van de programmalogica.

Een kwaadwillende kan:

- het authenticatiemechanisme van de webapplicatie omzeilen en op deze manier ongeautoriseerd 'inloggen' op de webapplicatie.
- gegevens in de database wijzigen.
- de volledige database verwijderen ('droppen') waardoor alle informatie uit de database verloren gaat.

- een eigen gebruikersaccount aanmaken en dit account gebruiken om toegang tot de webapplicatie te verkrijgen en te behouden.
- informatie aan de database of het onderliggende besturingssysteem onttrekken.
- malafide links in de database injecteren waardoor bezoekers van de website geïnfecteerd raken met malware.

Referentie OWASP Top-10

- A1-Injection
  https://www.owasp.org/index.php/Top_10_2010-A1

Testmethodiek (OWASP Testing Guide/OWASP Code Review Guide)

OWASP Testing Guide:

- Data Validation Testing
  - Testing for SQL Injection (OWASP-DV-005)
    https://www.owasp.org/index.php/Testing_for_SQL_Injection_(OWASP-DV-005)
    Oracle Testing
    MySQL Testing
    SQL Server Testing
    MS Access Testing
    Testing PostgreSQL (from OWASP BSP)

OWASP Code Review Guide:

- Reviewing Code for SQL Injection
  https://www.owasp.org/index.php/Reviewing_Code_for_SQL_Injection

Nr.	Beveiligingslaag	Kwetsbaarheid	Referentie RBW
K3-2	Applicatiebeveiliging	Cross-Site Scripting (XSS)	5.2.2

Toelichting

Een kwaadwillende kan via een kwaadaardige website veelal willekeurige JavaScript (en andere scripts) uitvoeren op het systeem van een gebruiker. De kwaadwillende heeft via deze scripts echter geen toegang tot mogelijk gevoelige informatie op het systeem van deze gebruiker, vanwege beperkingen die browsers opleggen aan de scripts die het uitvoert. Zo kan een kwaadwillende bijvoorbeeld nooit toegang krijgen tot de inhoud van cookies die gekoppeld zijn aan een ander domein dan het domein van de kwaadwillende (same origin policy), omdat de browser toegang tot deze gegevens niet toestaat.

Via Cross-Site Scripting (XSS) is het echter mogelijk om deze beperkingen te omzeilen. Bij XSS slaagt een kwaadwillende erin om kwaadaardige JavaScript terug te laten komen in het antwoord van een vertrouwde website. Het antwoord van de website wordt hierbij met andere woorden deels bepaald door de invoer van de kwaadwillende. De kwaadwillende slaagt hierin als bij een website alle onderstaande zaken van toepassing zijn:

- De website maakt gebruik van de invoer vanaf de client: om de uitvoer van de website te kunnen manipuleren moet een kwaadwillende malafide JavaScript kunnen injecteren via invoer naar de website.
- De website voert geen of onvoldoende controles uit op deze invoer.
- De website voert geen of onvoldoende controles uit op het antwoord dat deze terugstuurt aan de client.

De kwaadwillende kan XSS-kwetsbaarheden misbruiken om gevoelige informatie, zoals een sessie-ID, van een gebruiker te achterhalen.
Grofweg bestaan er drie soorten XSS: reflected XSS, stored XSS en DOM-based XSS.

Referentie OWASP Top-10

- A2-Cross Site Scripting (XSS)
  https://www.owasp.org/index.php/Top_10_2010-A2

Testmethodiek (OWASP Testing Guide/OWASP Code Review Guide)

OWASP Testing Guide:

- Data Validation Testing
  - Testing for Reflected Cross Site Scripting (OWASP-DV-001)
    https://www.owasp.org/index.php/Testing_for_Reflected_Cross_site_scripting_(OWASP-DV-001)
  - Testing for Stored Cross Site Scripting (OWASP-DV-002)
    https://www.owasp.org/index.php/Testing_for_Stored_Cross_site_scripting_(OWASP-DV-002)
  - Testing for DOM based Cross Site Scripting (OWASP-DV-003)
    https://www.owasp.org/index.php/Testing_for_DOM-based_Cross_site_scripting_(OWASP-DV-003)

OWASP Code Review Guide:

- Reviewing Code for Cross-Site Scripting
  https://www.owasp.org/index.php/Reviewing_Code_for_Cross-site_scripting

Nr.	Beveiligingslaag	Kwetsbaarheid	Referentie RBW
K3-3	Applicatiebeveiliging	Cross-Site Request Forgery (CSRF)	5.2.3

Toelichting

Cross-Site Request Forgery (CSRFof XSRF-) kwetsbaarheden ontstaan wanneer een website onvoldoende autorisatiecontroles uitvoert op een bepaalde transactie. Hierdoor kan het gebeuren dat een gebruiker onbedoeld een transactie uitvoert op een website waarmee deze gebruiker een sessie heeft. Misbruik vindt als volgt plaats: de gebruiker bezoekt een malafide of geïnfecteerde website en krijgt via deze website een link aangeboden naar een andere website waarmee de gebruiker een sessie heeft en die de kwaadwillende wil aanvallen. De gebruiker merkt hier vaak niets van, maar onder water vindt een transactie plaats vanuit de browser van de gebruiker naar een website waar de gebruiker zich mogelijk eerder heeft geauthenticeerd.

Referentie OWASP Top-10

- A5-Cross Site Request Forgery (CSRF)
  https://www.owasp.org/index.php/Top_10_2010-A5

Testmethodiek (OWASP Testing Guide/OWASP Code Review Guide)

OWASP Testing Guide:

- Session Management
  - Testing for Cross Site Request Forgery (CSRF) (OWASP-SM-005)
    https://www.owasp.org/index.php/Testing_for_CSRF_(OWASP-SM-005)

OWASP Code Review Guide:

- Reviewing Code for Cross-Site Request Forgery
  https://www.owasp.org/index.php/Reviewing_Code_for_Cross-Site_Request_Forgery

Nr.	Beveiligingslaag	Kwetsbaarheid	Referentie RBW
K3-4	Applicatiebeveiliging	Lekken van informatie (Onbedoeld vrijgeven van 'teveel' informatie)	5.2.4

Toelichting

Webservers en webapplicaties kunnen op allerlei manieren technische informatie over zichzelf 'lekken'[46]. Deze informatie kan een kwaadwillende helpen om een beeld te krijgen van de omgeving waarin de webapplicatie zich bevindt. De kwaadwillende kan bijvoorbeeld bepalen of de webapplicatie gebruik maakt van kwetsbare software.

Uitgebreide foutmeldingen

Sommige webapplicaties leveren bij het optreden van een foutsituatie allerlei informatie aan over de achtergrond(en) van de fout. Een uitgebreide foutmelding kan een kwaadwillende helpen om meer inzicht te krijgen in de programmalogica van een webapplicatie. Een foutmelding vertelt vaak iets over de gebruikte database, het uitgevoerde SQL-verzoek of het aangeroepen bestand. Al deze informatie draagt bij aan kennisvorming van de kwaadwillende over de infrastructuur.

Header-informatie

HTTP-headers kunnen veel informatie bevatten over de webapplicatie en de software waarvan de webapplicatie gebruik maakt. Eén van de bekendste HTTP-headers die informatie vrijgeeft, is de 'Server'-header. In veel gevallen zal de webserver via deze header informatie geven over het type webserver waar de pagina van afkomstig is. In sommige gevallen bevat deze header echter nog veel meer informatie.

Commentaarregels in scripts

Commentaarregels in code kunnen ongewild informatie vrijgeven. Vooral HTML-code en 'client-side scripts' (zoals JavaScript) bevatten vaak commentaar. Commentaarregels zijn niet altijd problematisch. In sommige gevallen bevat commentaar echter 'een geheugensteuntje' voor programmeurs en vergeten zij deze informatie te verwijderen zodra een webapplicatie in productie gaat.

Referentie OWASP Top-10

- A6 - Security Misconfiguration
  https://www.owasp.org/index.php/Top_10_2010-A6
- A6 - Information Leakage and Improper Error Handling
  (Top 10 - 2007, dropped in Top 10 - 2010)
  https://www.owasp.org/index.php/Top_10_2007-A6

Testmethodiek (OWASP Testing Guide/OWASP Code Review Guide)

OWASP Testing Guide:

- Configuration Management
  https://www.owasp.org/index.php/Testing_for_configuration_management
- Information Gathering
  - Spiders, Robots and Crawlers (OWASP-IG-001)
    https://www.owasp.org/index.php/Testing:_Spiders,_Robots,_and_Crawlers_(OWASP-IG-001)
  - Search Engine Discovery/Reconnaissance (OWASP-IG-002)
    https://www.owasp.org/index.php/Testing:_Search_engine_discovery/reconnaissance_(OWASP-IG-002)

46. Het gaat hier dus niet om mogelijk vertrouwelijke informatie uit een database maar over informatie over de gebruikte technieken/technologieën op de server. Het lekken van vertrouwelijke informatie uit de database is een kwetsbaarheid op de laag 'Vertrouwelijkheid en onweerlegbaarheid' van het RBW.

- Identify application entry points (OWASP-IG-003)
  https://www.owasp.org/index.php/Testing:_Identify_application_entry_points_(OWASP-IG-003)
- Testing for Web Application Fingerprint (OWASP-IG-004)
  https://www.owasp.org/index.php/Testing_for_Web_Application_Fingerprint_(OWASP-IG-004)
- Application Discovery (OWASP-IG-005)
  https://www.owasp.org/index.php/Testing_for_Application_Discovery_(OWASP-IG-005)
- Analysis of Error Codes (OWASP-IG-006)
  https://www.owasp.org/index.php/Testing_for_Error_Code_%28OWASP-IG-006%29

OWASP Code Review Guide:

- Chapter on Error Handling
  https://www.owasp.org/index.php/Error_Handling

OWASP Application Security Verification Standard (ASVS)

- V8 - Error Handling and Logging Verification Requirements
  http://code.google.com/p/owasp-asvs/wiki/Verification_V8

Nr.	Beveiligingslaag	Kwetsbaarheid	Referentie RBW
K3-5	Applicatiebeveiliging	HTTP response splitting	5.2.5

Toelichting

HTTP werkt met vraag- en antwoordberichten. Bij het bezoeken van een website stuurt een browser diverse vragen (HTTP-requests) aan een webserver die de webserver vervolgens beantwoordt. Eén vraag leidt daarbij normaal gesproken tot maximaal één antwoord. Bij HTTP-response splitting aanvallen is dit niet het geval. Doordat de webapplicatie onvoldoende validatie van gebruikersinvoer uitvoert, geeft deze webapplicatie niet alleen het eigen antwoord terug, maar ook het antwoord dat in de gebruikersinvoer werd meegegeven. Zo is het mogelijk dat één HTTP-request leidt tot meerdere logische HTTP-responses. Dit is mogelijk op het moment dat de webapplicatie ongevalideerde gebruikersinvoer rechtstreeks gebruikt in een HTTP response header.

Testmethodiek (OWASP Testing Guide v3.0)

OWASP Testing Guide:

- Data Validation Testing
  - Testing for HTTP Splitting/Smuggling - HTTP Splitting, Smuggling (OWASP-DV-016)
    https://www.owasp.org/index.php/Testing_for_HTTP_Splitting/Smuggling_(OWASP-DV-016)

Nr.	Beveiligingslaag	Kwetsbaarheid	Referentie RBW
K3-6	Applicatiebeveiliging	Remote File Inclusion (RFI)	5.2.6

Toelichting

Remote File Inclusion (RFI) is een kwetsbaarheid die zich voordoet op webservers die gebruik maken van dynamische file includes in script- en programmeertalen. Wanneer een dergelijke website kwetsbaar is voor RFI, kan een kwaadwillende zijn eigen code door de server laten uitvoeren. RFI is mogelijk op het moment dat een pagina op een webserver de volgende kenmerken heeft:

- De pagina is geschreven in PHP.
- De pagina maakt gebruik van andere PHP-scripts via een include (of een andere vergelijkbare functie).
- Gebruikersinvoer bepaalt de naam van de scripts waarvan de pagina gebruik maakt.
- PHP staat URL includes toe (allow_url_include = 'On').

Of een aanval succesvol is, hangt ook af van de configuratie van de webserver. Als de PHP-optie allow_url_include bijvoorbeeld is ingesteld op de waarde 'Off', zal PHP het importeren van een PHP-script vanaf een externe locatie niet toestaan en zal het moeilijker zijn om deze RFI-kwetsbaarheid uit te buiten. Wel is het in dat geval nog steeds mogelijk om willekeurige lokale bestanden op de server (bijvoorbeeld /etc/passwd) te laten importeren door het script.

Ook als de webserver zelf geen verbinding met internet kan opzetten, is het nog steeds mogelijk een RFI-kwetsbaarheid uit te buiten. Hiervoor kan een kwaadwillende bijvoorbeeld gebruik maken van een base64 data include.

Referentie OWASP Top-10

- A6 - Security Misconfiguration
  https://www.owasp.org/index.php/Top_10_2010-A6
- A3 - Malicious File Execution (Top 10 - 2007, dropped in Top 10 - 2010)
  https://www.owasp.org/index.php/Top_10_2007-A3

Testmethodiek (OWASP Testing Guide/OWASP Code Review Guide)

OWASP Testing Guide:

- Configuration Management
  https://www.owasp.org/index.php/Testing_for_configuration_management

OWASP Application Security Verification Standard (ASVS)

- V12 - Security Configuration Verification Requirements
  http://code.google.com/p/owasp-asvs/wiki/Verification_V12

Nr.	Beveiligingslaag	Kwetsbaarheid	Referentie RBW
K3-7	Applicatiebeveiliging	Path traversal	5.2.7

Toelichting

Een webserver kent altijd een webroot waarvandaan de webserver alle bestanden voor een bepaalde webapplicatie 'serveert'. Het idee is dat gebruikers alleen toegang hebben tot bestanden onder de webroot en niet tot bestanden die zich in andere directories van het systeem bevinden. In sommige gevallen is het voor kwaadwillenden echter mogelijk om bestanden buiten de webroot te benaderen. We spreken in dit geval van een path traversal kwetsbaarheid. Path traversal kwetsbaarheden kunnen zich op twee niveaus voordoen: op het niveau van de webserver en op het niveau van de webapplicatie.

Referentie OWASP Top-10

- A4 - Insecure Direct Object References
  https://www.owasp.org/index.php/Top_10_2010-A4
- A8 - Failure to Restrict URL Access
  https://www.owasp.org/index.php/Top_10_2010-A8

Testmethodiek (OWASP Testing Guide/OWASP Code Review Guide)

OWASP Testing Guide:

- Authorization Testing
  - Testing for path traversal (OWASP-AZ-001)
    https://www.owasp.org/index.php/Testing_for_Path_Traversal_(OWASP-AZ-001)

Nr.	Beveiligingslaag	Kwetsbaarheid	Referentie RBW
K3-8	Applicatiebeveiliging	Command-injectie	5.2.8

Toelichting

Command-injectie houdt in dat een kwaadwillende in staat is om commando's uit te voeren op het niveau van het besturingssysteem. Dit kan gebeuren op het moment dat de webapplicatie OS-commando's aanroept en daarbij gebruik maakt van ongevalideerde invoer van de gebruiker.
De mogelijkheden die een kwaadwillende heeft bij een command-injectiekwetsbaarheid zijn groot. In principe kan een kwaadwillende in dit geval alle ondersteunde OS-commando's aanroepen en wordt hij alleen beperkt door de rechten waaronder de webserver draait.

Referentie OWASP Top-10

- A1-Injection
  https://www.owasp.org/index.php/Top_10_2010-A1

Testmethodiek (OWASP Testing Guide/OWASP Code Review Guide)

OWASP Testing Guide:

- Data Validation Testing
  - Testing for Command Injection (OWASP-DV-013)
    https://www.owasp.org/index.php/Testing_for_Command_Injection_(OWASP-DV-013)

OWASP Code Review Guide:

- Reviewing Code for OS Injection
  https://www.owasp.org/index.php/Reviewing_Code_for_OS_Injection

Nr.	Beveiligingslaag	Kwetsbaarheid	Referentie RBW
K3-9	Applicatiebeveiliging	Buffer overflows	5.2.9

Toelichting

Een buffer overflow doet zich voor op het moment dat een webapplicatie meer data naar een geheugenbuffer schrijft dan dat daar initieel voor was gereserveerd. Hierdoor komt data op plekken in het geheugen terecht waar dit eigenlijk niet had gemogen. Misbruik van een buffer overflow kan leiden tot het uitvoeren van code op het systeem; hierdoor kan een kwaadwillende in het ernstigste geval volledige controle over een systeem krijgen.
Buffer overflows in webapplicaties zijn niet altijd eenvoudig te ontdekken en vaak moeilijk te misbruiken.

Testmethodiek (OWASP Testing Guide/OWASP Code Review Guide)

OWASP Testing Guide:

- Data Validation Testing
  - Testing for Buffer overflow (OWASP-DV-014)
    https://www.owasp.org/index.php/Testing_for_Buffer_Overflow_(OWASP-DV-014)
    Testing for Heap overflow
    Testing for Stack overflow
    Testing for Format string
    Denial of Service Testing:
- OWASP-DS-003 Testing for DoS Buffer Overflows - Buffer Overflows
  https://www.owasp.org/index.php/Testing_for_DoS_Buffer_Overflows_(OWASP-DS-003)

OWASP Code Review Guide:

- Reviewing Code for Buffer Overruns and Overflows
  https://www.owasp.org/index.php/Reviewing_Code_for_Buffer_Overruns_and_Overflows

Nr.	Beveiligingslaag	Kwetsbaarheid	Referentie RBW
K3-10	Applicatiebeveiliging	Fouten in de applicatielogica	5.2.10

Toelichting

Fouten in de applicatielogica kunnen ertoe leiden dat kwaadwillenden ongewenste activiteiten uitvoeren via de webapplicatie met compleet legitieme verzoeken. Kortom een kwetsbare webapplicatie waar geen technische fouten aan ten grondslag liggen. Fouten in de applicatielogica kunnen zich op elke plek in de webapplicatie voordoen.

Testmethodiek (OWASP Testing Guide/OWASP Code Review Guide)

OWASP Testing Guide:

- Business Logic Testing (OWASP-BL-001)
  https://www.owasp.org/index.php/Testing_for_business_logic_(OWASP-BL-001)

Nr.	Beveiligingslaag	Kwetsbaarheid	Referentie RBW
K3-11	Applicatiebeveiliging	Configuratiefouten	5.2.11

Toelichting

De configuratie van de webapplicatie en het applicatieplatform spelen een belangrijke rol in de beveiliging van het geheel. Door een webapplicatie en/of applicatieplatform te installeren zonder daarbij aandacht te besteden aan de configuratie ervan kunnen zich verschillende beveiligingsproblemen voordoen. Enkele voorbeelden hiervan zijn:

- Gebruik van standaardpaden voor de webroot.
- Gebruik van standaard gebruikersnamen en wachtwoorden.
- Aanwezigheid van standaard plug-ins.
- Ontbreken van patches.
- Ingeschakelde 'debugging'-opties.

Referentie OWASP Top-10

- A6 - Security Misconfiguration
  https://www.owasp.org/index.php/Top_10_2010-A6

Testmethodiek (OWASP Testing Guide/OWASP Code Review Guide)

OWASP Testing Guide:

- Configuration Management Testing
  - SSL/TLS Testing (SSL Version, Algorithms, Key length, Digital Cert. Validity) (OWASP-CM-001)
    https://www.owasp.org/index.php/Testing_for_SSL-TLS_(OWASP-CM-001)
  - DB Listener Testing (OWASP-CM-002)
    https://www.owasp.org/index.php/Testing_for_DB_Listener_(OWASP-CM-002)
  - Infrastructure Configuration Management Testing (OWASP-CM-003)
    https://www.owasp.org/index.php/Testing_for_infrastructure_configuration_management_(OWASP-CM-003)
  - Application Configuration Management Testing (OWASP-CM-004)
    https://www.owasp.org/index.php/Testing_for_application_configuration_management_(OWASP-CM-004)
  - Testing for File Extensions Handling (OWASP-CM-005)
    https://www.owasp.org/index.php/Testing_for_file_extensions_handling_(OWASP-CM-005)
  - Old, Back-up and Unreferenced Files (OWASP-CM-006)
    https://www.owasp.org/index.php/Testing_for_Old,_Back-up_and_Unreferenced_Files_(OWASP-CM-006)
  - Infrastructure and Application Admin Interfaces (OWASP-CM-007)
    https://www.owasp.org/index.php/Testing_for_Admin_Interfaces_(OWASP-CM-007)
  - Testing for HTTP Methods and Cross Site Tracing (XST) (OWASP-CM-008)
    https://www.owasp.org/index.php/Testing_for_HTTP_Methods_and_XST_(OWASP-CM-008)

Nr.	Beveiligingslaag	Kwetsbaarheid	Referentie RBW
K3-12	Applicatiebeveiliging	Geen invoervalidatie	5.3.1

Toelichting

Ongecontroleerde (ongevalideerde) invoer van gebruikers is de belangrijkste dreiging voor een webapplicatie. Als invoer van gebruikers rechtstreeks wordt gebruikt in HTML-uitvoer, cookie-waarden, SQL-queries, et cetera, bestaat er een grote kans dat een kwaadwillende de webapplicatie compromitteert. Een gebrek aan invoervalidatie leidt vaak tot XSS en SQL-injectie kwetsbaarheden.

Referentie OWASP Top-10

- A1-Injection
  https://www.owasp.org/index.php/Top_10_2010-A1
- A2-Cross Site Scripting (XSS)
  https://www.owasp.org/index.php/Top_10_2010-A2

Testmethodiek (OWASP Testing Guide/OWASP Code Review Guide)

OWASP Testing Guide:

- Data Validation Testing
  - Testing for Reflected Cross Site Scripting (OWASP-DV-001)
    https://www.owasp.org/index.php/Testing_for_Reflected_Cross_site_scripting_(OWASP-DV-001)
  - Testing for Stored Cross Site Scripting (OWASP-DV-002)
    https://www.owasp.org/index.php/Testing_for_Stored_Cross_site_scripting_(OWASP-DV-002)

- Testing for DOM based Cross Site Scripting (OWASP-DV-003)
  https://www.owasp.org/index.php/Testing_for_DOM-based_Cross_site_scripting_(OWASP-DV-003)
- Testing for SQL Injection (OWASP-DV-005)
  https://www.owasp.org/index.php/Testing_for_SQL_Injection_(OWASP-DV-005)
  Oracle Testing
  MySQL Testing
  SQL Server Testing
  MS Access Testing
  Testing PostgreSQL (from OWASP BSP)
- Testing for Command Injection (OWASP-DV-013)
  https://www.owasp.org/index.php/Testing_for_Command_Injection_(OWASP-DV-013)

OWASP Code Review Guide:

- Reviewing Code for OS Injection
  https://www.owasp.org/index.php/Reviewing_Code_for_OS_Injection
- Reviewing Code for SQL Injection
  https://www.owasp.org/index.php/Reviewing_Code_for_SQL_Injection
- Reviewing Code for Data Validation
  https://www.owasp.org/index.php/Reviewing_Code_for_Data_Validation
- Reviewing Code for Cross-Site Scripting
  https://www.owasp.org/index.php/Reviewing_Code_for_Cross-site_scripting

OWASP Application Security Verification Standard (ASVS)

- V5 - Input Validation Verification Requirements
  http://code.google.com/p/owasp-asvs/wiki/Verification_V5

Nr.	Beveiligingslaag	Kwetsbaarheid	Referentie RBW
K3-13	Applicatiebeveiliging	Geen uitvoervalidatie	5.3.2

Toelichting

Naast het ontbreken van validatie van invoer ontbreekt het bij sommige webapplicaties ook aan de validatie van uitvoer. Als een webapplicatie onvoldoende controles uitvoert op de uitvoer die het terugstuurt naar de eindgebruiker, kan het gebeuren dat er zich onbedoelde of ongewenste inhoud in de uitvoer bevindt. Denk hierbij aan scriptingcode die een aanvaller gebruikt in XSS-aanvallen, informatie over gebruikte technologieën op de server en uitgebreide foutmeldingen.

Referentie OWASP Top-10

- A6 - Security Misconfiguration
  https://www.owasp.org/index.php/Top_10_2010-A6
- A6 - Information Leakage and Improper Error Handling (Top 10 - 2007, dropped in Top 10 - 2010)
  https://www.owasp.org/index.php/Top_10_2007-A6

Testmethodiek (OWASP Testing Guide/OWASP Code Review Guide)

OWASP Testing Guide:

- Configuration Management
  - SSL/TLS Testing (SSL Version, Algorithms, Key length, Digital Cert. Validity) (OWASP-CM-001)
    https://www.owasp.org/index.php/Testing_for_SSL-TLS_(OWASP-CM-001)
  - DB Listener Testing (OWASP-CM-002)
    https://www.owasp.org/index.php/Testing_for_DB_Listener_(OWASP-CM-002)

- Infrastructure Configuration Management Testing (OWASP-CM-003)
  https://www.owasp.org/index.php/Testing_for_infrastructure_configuration_management_(OWASP-CM-003)
- Application Configuration Management Testing (OWASP-CM-004)
  https://www.owasp.org/index.php/Testing_for_application_configuration_management_(OWASP-CM-004)
- Testing for File Extensions Handling (OWASP-CM-005)
  https://www.owasp.org/index.php/Testing_for_file_extensions_handling_(OWASP-CM-005)
- Old, Back-up and Unreferenced Files (OWASP-CM-006)
  https://www.owasp.org/index.php/Testing_for_Old,_Back-up_and_Unreferenced_Files_(OWASP-CM-006)
- Infrastructure and Application Admin Interfaces (OWASP-CM-007)
  https://www.owasp.org/index.php/Testing_for_Admin_Interfaces_(OWASP-CM-007)
- Testing for HTTP Methods and Cross Site Tracing (XST) (OWASP-CM-008)
  https://www.owasp.org/index.php/Testing_for_HTTP_Methods_and_XST_(OWASP-CM-008)

- Information Gathering
  - Spiders, Robots and Crawlers (OWASP-IG-001)
    https://www.owasp.org/index.php/Testing:_Spiders,_Robots,_and_Crawlers_(OWASP-IG-001)
  - Search Engine Discovery/Reconnaissance (OWASP-IG-002)
    https://www.owasp.org/index.php/Testing:_Search_engine_discovery/reconnaissance_(OWASP-IG-002)
  - Identify application entry points (OWASP-IG-003)
    https://www.owasp.org/index.php/Testing:_Identify_application_entry_points_(OWASP-IG-003)
  - Testing for Web Application Fingerprint (OWASP-IG-004)
    https://www.owasp.org/index.php/Testing_for_Web_Application_Fingerprint_(OWASP-IG-004)
  - Application Discovery (OWASP-IG-005)
    https://www.owasp.org/index.php/Testing_for_Application_Discovery_(OWASP-IG-005)
  - Analysis of Error Codes (OWASP-IG-006)
    https://www.owasp.org/index.php/Testing_for_Error_Code_%28OWASP-IG-006%29

OWASP Application Security Verification Standard (ASVS)

V6 - Output Encoding/Escaping Verification Requirements

Nr.	Beveiligingslaag	Kwetsbaarheid	Referentie RBW
K3-14	Applicatiebeveiliging	Ineffectieve filters	5.3.3

Toelichting

In veel gevallen voert een webapplicatie wel invoervalidatie en filtering uit, maar blijkt deze filtering niet voldoende effectief genoeg om alle mogelijke aanvallen op de webapplicatie te blokkeren. Dit is voornamelijk het geval op het moment dat de webapplicatie gebruik maakt van blacklisting om mogelijk gevaarlijke strings uit de invoer te verwijderen.

Referentie OWASP Top-10

Zie kwetsbaarheid ‘Geen invoervalidatie’.

Testmethodiek (OWASP Testing Guide/OWASP Code Review Guide)

Zie kwetsbaarheid ‘Geen invoervalidatie’.

Nr.	Beveiligingslaag	Kwetsbaarheid	Referentie RBW
K3-15	Applicatiebeveiliging	Onveilige opslag van informatie	5.3.4

Toelichting
Onveilige opslag van informatie verhoogt niet zozeer de kans op een kwetsbaarheid, maar verhoogt wel de schade die een kwetsbaarheid teweeg kan brengen. Informatie die niet versleuteld opgeslagen is, kan bijvoorbeeld een probleem vormen op het moment dat de webapplicatie een path traversal of command-injectie kwetsbaarheid bevat. Het niet versleuteld opslaan van gevoelige informatie in een database is ook een probleem op het moment dat de webapplicatie kwetsbaar is voor SQL-injectie.

Nr.	Beveiligingslaag	Kwetsbaarheid	Referentie RBW
K3-16	Applicatiebeveiliging	Extern ontwikkelde, kwetsbare webapplicaties	5.3.5

Toelichting
Bij het nemen van maatregelen voor webapplicaties bestaat de kans dat de focus voornamelijk gericht is op intern ontwikkelde webapplicaties. ‘Extern ontwikkelde aangekochte webapplicaties zijn veilig’, wordt vaak gedacht. Niets is minder waar. Ook extern ontwikkelde webapplicaties kunnen kwetsbaarheden bevatten. En juist omdat deze in gebruik zijn bij meer organisaties, is de kans groter dat kwaadwillenden hun pijlen op deze webapplicaties richten en bijvoorbeeld exploits voor deze producten publiceren.

Nr.	Beveiligingslaag	Kwetsbaarheid	Referentie RBW
K3-17	Applicatiebeveiliging	Gebruik van voorbeeldscripts van internet	5.3.6

Toelichting
Op internet zijn veel voorbeeldscripts beschikbaar die beschrijven op welke manier ontwikkelaars bepaalde functionaliteiten in hun webapplicatie kunnen implementeren. Vaak is in deze voorbeeldscripts onvoldoende aandacht besteed aan het aspect beveiliging. Het gevaar bestaat dat ontwikkelaars deze voorbeeldscripts één-op-één verwerken in hun eigen webapplicatie, waardoor automatisch een kwetsbaarheid in hun webapplicatie introduceren.

Nr.	Beveiligingslaag	Kwetsbaarheid	Referentie RBW
K3-18	Applicatiebeveiliging	Onvoldoende hardening en patching	5.3.7

Toelichting
Het ontbreken van hardeningsmaatregelen en patches leidt tot veel van de hiervoor beschreven kwetsbaarheden. Het ontbreken van patches kan er bijvoorbeeld toe leiden dat allerhande kwetsbaarheden aanwezig blijven in extern ontwikkelde webapplicaties en in web- en applicatieservers.
Verder kan het ontbreken van hardeningsmaatregelen ertoe leiden dat succesvol misbruik van kwetsbaarheden leidt tot grote schade. Zo zijn de mogelijkheden van een command-injectie kwetsbaarheid vaak beperkt tot de rechten van het account waaronder de webserver draait. Maakt de webserver gebruik van een account dat zeer hoge rechten heeft, dan kan de kwaadwillende nog meer schade aanrichten.

Referentie OWASP Top-10

- A6 - Security Misconfiguration
  https://www.owasp.org/index.php/Top_10_2010-A6

Testmethodiek (OWASP Testing Guide/OWASP Code Review Guide)

OWASP Testing Guide:

- Configuration Management Testing
  - SSL/TLS Testing (SSL Version, Algorithms, Key length, Digital Cert. Validity) (OWASP-CM-001)
    https://www.owasp.org/index.php/Testing_for_SSL-TLS_(OWASP-CM-001)
  - DB Listener Testing (OWASP-CM-002)
    https://www.owasp.org/index.php/Testing_for_DB_Listener_(OWASP-CM-002)
  - Infrastructure Configuration Management Testing (OWASP-CM-003)
    https://www.owasp.org/index.php/Testing_for_infrastructure_configuration_management_(OWASP-CM-003)
  - Application Configuration Management Testing (OWASP-CM-004)
    https://www.owasp.org/index.php/Testing_for_application_configuration_management_(OWASP-CM-004)
  - Testing for File Extensions Handling (OWASP-CM-005)
    https://www.owasp.org/index.php/Testing_for_file_extensions_handling_(OWASP-CM-005)
  - Old, Back-up and Unreferenced Files (OWASP-CM-006)
    https://www.owasp.org/index.php/Testing_for_Old,_Back-up_and_Unreferenced_Files_(OWASP-CM-006)
  - Infrastructure and Application Admin Interfaces (OWASP-CM-007)
    https://www.owasp.org/index.php/Testing_for_Admin_Interfaces_(OWASP-CM-007)
  - Testing for HTTP Methods and Cross Site Tracing (XST) (OWASP-CM-008)
    https://www.owasp.org/index.php/Testing_for_HTTP_Methods_and_XST_(OWASP-CM-008)
- Information Gathering
  - Analysis of Error Codes (OWASP-IG-006)
    https://www.owasp.org/index.php/Testing_for_Error_Code_%28OWASP-IG-006%29

OWASP Code Review Guide:

- Chapter on Error Handling
  https://www.owasp.org/index.php/Error_Handling

5.2 Doelstelling

Waarborgen dat beveiliging wordt ingebouwd in webapplicaties.

5.3 Beveiligingsrichtlijnen

In de vorige paragraaf is aandacht besteedt aan de kwetsbaarheden die in een webapplicatie aanwezig kunnen zijn. Deze paragraaf kijkt naar de manier waarop deze kwetsbaarheden kunnen worden voorkomen of de schade door misbruik van de kwetsbaarheden kan worden beperkt.

Softwareontwikkeling

Veel van de bekendste kwetsbaarheden in webapplicaties zoals XSS en SQL-injectie vinden hun oorsprong in fouten die programmeurs maken tijdens het ontwikkelen van software. Er bestaat een aantal maatregelen dat de aanwezigheid van deze kwetsbaarheden grotendeels kan voorkomen. Deze paragraaf besteedt aandacht aan de belangrijkste maatregelen op het gebied van softwareontwikkeling die de aanwezigheid van deze kwetsbaarheden voorkomen en de kans op en schade door de aanwezigheid van ernstige kwetsbaarheden in webapplicaties voorkomen.

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B3-1	Applicatiebeveiliging	De webapplicatie valideert de inhoud van een HTTP-request voor die wordt gebruikt.	6.2.1

Doelstelling

- Voorkom het verlies, wijziging of misbruik van gegevens door onbetrouwbare (malafide) invoer
- Voorkom dat de applicatielogica wordt beïnvloed.

Rationale

De belangrijkste vuistregel voor invoer in een webapplicatie is dat de applicatie alle invoer nooit mag vertrouwen en daarom moet valideren. Dit betekent dat de webapplicatie in ieder geval de volgende onderdelen van een HTTP-request moet valideren, voor die te gebruiken binnen de webapplicatie:

- URL's;
- Query parameters (variabelen die de client via GET requests doorgeeft);
- Form parameters (variabelen die de client via POST requests doorgeeft);
- Cookies;
- HTTP-headers;
- XML (hieronder vallen ook protocollen als SOAP, JSON en REST);
- Bestanden.

De webapplicatie valideert de inhoud van alle onderdelen van een HTTP-request op basis van verwerkbare invoer.

Elke invoer waarvan de webapplicatie gebruik maakt, moet gecontroleerd worden op type, lengte, formaat en karakters. De inhoud van HTTP-requests wordt op basis van verwerkbare invoer (whitelist) gevalideerd om te voorkomen dat malafide inhoud het mogelijk maakt om de applicatielogica te beïnvloeden. Voldoet de invoer niet aan wat kan worden verwerkt, dan moet deze invoer worden geweigerd.

De webapplicatie valideert de inhoud van alle onderdelen van een HTTP-request op basis van ongewenste invoer.

In sommige gevallen is het op basis van de whitelist moeilijk om alle mogelijke malafide invoer uit te filteren. Denk aan invoervelden waar de gebruiker vrije tekst kan invoeren. In dit soort gevallen kan de webapplicatie de invoer aanvullend controleren op malafide sleutelwoorden, tekens en patronen (blacklist).

De webapplicatie maakt risicovolle karakters uit de invoer 'onschadelijk'.
Karakters uit de invoer die verwerkbaar en niet ongewenst zijn kunnen nog steeds risicovol zijn bij het gebruik hiervan binnen de programmalogica. Om problemen hiermee te voorkomen moet de webapplicatie deze karakters 'onschadelijk' maken.
Risicovolle karakters kunnen onderdeel uitmaken van legitieme invoer. Neem onderstaand voorbeeld waarbij de plaatsnaam ('s-Gravenhage) tot een syntactische incorrecte query leidt

```
SELECT * FROM nieuws WHERE titel LIKE '%'s-gravenhage%';
```

Door een escape voor de apostrof te plaatsen, beschouwt de database de apostrof als onderdeel van de invoer en niet als onderdeel van de query. Veel programmeertalen ondersteunen standaardfuncties voor het escapen van gevaarlijke karakters.

Vereiste succescriteria (conformiteitvereisten)

- Beschikken over de broncode van de programmatuur.

Onderstaande criteria gelden voor het valideren van de inhoud van een HTTP-request op basis van ongewenste invoer:

- Validatie vindt plaats op in ieders geval dynamische onderdelen van de URL, query parameters, form parameters, cookies, HTTP-headers, XML en bestanden.
- De webapplicatie voert deze validatie uit op basis van:
  - Typecontrole (bijvoorbeeld string of integer).
  - Lengtecontrole
  - Formaatcontrole (op basis van bijvoorbeeld een reguliere expressie)
  - Controle op valide karakters (bijvoorbeeld alleen 'A-Z' en 'a-z')
- In het geval de invoer niet voldoet aan één of meerdere van bovenstaande controles, weigert de webapplicatie deze invoer.

Onderstaande criteria gelden voor het filteren van de inhoud van een HTTP-request op basis van ongewenste invoer:

- De webapplicatie filtert de invoer op basis van:
  - Malafide sleutelwoorden (bijvoorbeeld 'DROP' of ' rm ')
  - Malafide tekens (bijvoorbeeld '' of '')
  - Malafide patronen (bijvoorbeeld '/**/' of '..\..\')
- De filtering is toegespitst op de programmaonderdelen waarin de invoer wordt verwerkt. Bij het gebruik van invoer voor het samenstellen van een databasequery zijn andere filters vereist dan voor het samenstellen van een LDAP-query.
- In het geval de invoer één of meerdere sleutelwoorden, tekens of patronen van de blacklist bevat, verwijdert de webapplicatie deze uit de invoer alvorens deze invoer verder te gebruiken binnen de webapplicatielogica.

De volgende risicovolle karakters uit de invoer worden 'onschadelijk' gemaakt:

- De webapplicatie voert escaping uit op de invoer na het toepassen van whitelists en eventueel blacklists.
- De escaping is toegespitst op de programmaonderdelen waarin de invoer wordt verwerkt.

Classificatie

Hoog

Bewijsvoering

Het vaststellen is goed mogelijk, als je betrokken bent bij het ontwikkeltraject en/of beschikt over de broncode van de programmatuur, door het uitvoeren van code reviews.

Relatie met andere normen en standaarden

Zie maatregel B3-14 'Voer een code review uit'

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B3-2	Applicatiebeveiliging	De webapplicatie controleert voor elk HTTP verzoek of de initiator geauthenticeerd is en de juiste autorisaties heeft.	6.2.2

Doelstelling
Valideer de initiator van een HTTP-request om te voorkomen dat kwaadwillenden transacties uit naam van een valide gebruiker uitvoeren.

Rationale
Via het stelen van cookies of via Cross-Site Request Forgery (CSRF) kunnen kwaadwillenden ongewild transacties uitvoeren uit naam van een gevalideerde gebruiker. Voor CSRF kan dit via links op malafide websites of in e-mails. De kans op misbruik van gestolen cookies kan de webapplicatie minimaliseren door de inhoud van een cookie te koppelen aan het IP-adres waaraan deze inhoud is toegekend. De kans op CSRF kan de webapplicatie minimaliseren door gebruik te maken van dynamische tokens en het uitvoeren van een controle op de 'Referer'-header.

Vereiste succescriteria (conformiteitvereisten)
- Beschikken over de broncode van de programmatuur.
- De waarde van cookies is gekoppeld aan het IP-adres waarnaar deze waarde is verstuurd.
- Voor onderdelen van de webapplicatie waarmee transacties door een gevalideerde gebruiker kunnen worden uitgevoerd:
  - zijn formulierpagina's voorzien van een dynamisch token;
  - accepteert de webapplicatie alleen verzoeken waarbij de inhoud van de Referer-header overeenkomt met de URL van de betreffende webapplicatie.

Classificatie
Hoog

Bewijsvoering
- Het is niet mogelijk om een cookie te gebruiken vanaf een IP-adres anders dan het IP-adres aan wie het cookie verstrekt is.
- Het is niet mogelijk om transacties voor gevalideerde gebruikers uit te voeren vanaf een andere website dan de website waarop de gebruiker is gevalideerd.
- Het vaststellen is goed mogelijk, als je betrokken bent bij het ontwikkeltraject en/of beschikt over de broncode van de programmatuur, door het uitvoeren van code reviews.

Relatie met andere normen en standaarden
Zie maatregel B3-14 'Voer een code review uit'

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B3-3	Applicatiebeveiliging	De webapplicatie normaliseert invoerdata voor validatie.	6.2.3

Doelstelling
Normaliseer alle invoerdata voor deze te valideren om te voorkomen dat filtering-mechanismen ongewenste patronen niet herkennen.

Rationale
Voordat een webapplicatie invoer gaat valideren, moet deze de data eerst normaliseren. Hiermee voorkomt de webapplicatie dat malafide verzoeken voorbij filters kunnen komen. Normalisatie staat ook wel bekend als anti-evasion of canonicalization.

Voorbeelden van normalisatie zijn:
- Omzetten van NULL karakters naar spaties.
- Coderen van bijzondere karakters in een uniforme codering (bijvoorbeeld UTF-8).
- Normaliseren van padverwijzingen als '/./' en '/../'.
- Verwijderen van overbodige spaties en regeleinden.
- Verwijderen van onnodige witruimtes.
- Omzetten van backslashes naar forward slashes.
- Omzetten van mixed case strings naar lower case strings.
- et cetera.

Vereiste succescriteria (conformiteitvereisten)
- Beschikken over de broncode van de programmatuur.

Classificatie
Hoog

Bewijsvoering
Het vaststellen is goed mogelijk, als je betrokken bent bij het ontwikkeltraject en/of beschikt over de broncode van de programmatuur, door het uitvoeren van code reviews.

Relatie met andere normen en standaarden
Zie maatregel B3-14 'Voer een code review uit'

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B3-4	Applicatiebeveiliging	De webapplicatie codeert dynamische onderdelen in de uitvoer	6.2.4

Doelstelling
Codeer dynamische onderdelen van de uitvoer zodat er geen ongewenste tekens in de uitvoer terecht komen.

Rationale
Uitvoervalidatie voorkomt dat de webapplicatie ongewenste opdrachten geeft aan de client, bijvoorbeeld in het geval van XSS. Uitvoervalidatie kan worden geïmplementeerd door het coderen van alle dynamische inhoud van een webpagina. Vrijwel elke webpagina bevat naast statische ook dynamische informatie. Deze dynamische informatie kan bijvoorbeeld afkomstig zijn uit databases of externe bronnen maar kan ook gebaseerd zijn op invoer van de gebruiker. Zeker in het laatste geval bestaat de kans dat aanvallers misbruik maken van onvoldoende filtering of codering.
Het coderen van dynamische pagina-inhoud houdt in dat de webapplicatie mogelijk 'gevaarlijke' karakters codeert. Hoe de webapplicatie deze informatie moet coderen is afhankelijk van de plek in de pagina waar deze dynamische inhoud verschijnt. Zo moet men speciale karakters in HTML, JavaScript, HTML-attributen en URL's allemaal op een andere wijze coderen. Neem bijvoorbeeld het 'groter dan'-teken (>). Afhankelijk van de plek waar dit teken wordt gebruikt, ziet de gecodeerde versie van dit teken er als volgt uit:
- HTML gecodeerd : <
- HTML-attribuut gecodeerd : >
- JavaScript gecodeerd : \x3E
- CSS gecodeerd : \3E
- URL gecodeerd : %3E

Veel scripting- en programmeertalen hebben standaard bibliotheken waarmee deze codering kan worden uitgevoerd.

Vereiste succescriteria (conformiteitvereisten)

- Beschikken over de broncode van de programmatuur.

Classificatie

Hoog

Bewijsvoering

Het vaststellen is goed mogelijk, als je betrokken bent bij het ontwikkeltraject en/of beschikt over de broncode van de programmatuur, door het uitvoeren van code reviews.

Relatie met andere normen en standaarden

Zie maatregel B3-14 'Voer een code review uit'

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B3-5	Applicatiebeveiliging	Voor het raadplegen en/of wijzigen van gegevens in de database gebruikt de webapplicatie alleen geparametriseerde queries.	6.2.5 en 6.2.6

Doelstelling

Verklein de kans op SQL-injectie aanvallen.

Rationale

Grofweg bestaan er twee methoden om vanuit een webapplicatie een query te genereren die gebruik maakt van invoer van gebruikers: via dynamische strings of via parameters. Bij dynamische strings plakt de ontwikkelaar een vaste string (bijvoorbeeld de start van een SELECT-statement) aan een variabele (bijvoorbeeld de inhoud van de WHERE-clause). Via deze methode bestaat de mogelijkheid dat de invoer de syntax van de query verandert. Bij gebruik van parameters gebruikt de ontwikkelaar een vaste string waarbij alleen een vaste plek is ingeruimd voor variabelen. Bij het gebruik van geparameteriseerde queries is de syntax van de query statisch en wordt invoer alleen gebruikt om vooraf gedefinieerde variabelen te vullen. Door te voorkomen dat de syntax van de query wijzigt, blokkeert de webapplicatie SQL-injectieaanvallen.

Vereiste succescriteria (conformiteitvereisten)

- Beschikken over de broncode van de programmatuur.
- De webapplicatie maakt gebruik van geparameteriseerde queries bij het benaderen van databases.

Classificatie

Hoog

Bewijsvoering

Het vaststellen is goed mogelijk, als je betrokken bent bij het ontwikkeltraject en/of beschikt over de broncode van de programmatuur, door het uitvoeren van code reviews.

Relatie met andere normen en standaarden

Zie maatregel B3-14 'Voer een code review uit'

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B3-6	Applicatiebeveiliging	De webapplicatie valideert alle invoer, gegevens die aan de webapplicatie worden aangeboden, aan de serverzijde.	6.2.7

Doelstelling
Voorkom dat invoercontroles kunnen worden omzeild.

Rationale
Het uitgangspunt bij het ontwikkelen van een webapplicatie moet zijn dat de client niet te vertrouwen is. Het is mogelijk dat de gebruiker werkt vanaf een geïnfecteerde PC of dat de gebruiker een kwaadwillende is die probeert in te breken op de webapplicatie. In het laatste geval is de kans groot dat de kwaadwillende geen gebruik maakt van een browser voor het aanvallen van de webapplicatie maar van eigen tools. Eventuele beperkingen die een kwaadwillende via de webapplicatie probeert af te dwingen op een client, kunnen dan ook eenvoudig worden omzeild. Denk aan het beperken van de lengte van een string die in een veld kan worden ingevoerd, het disablen van invoervelden of het verbergen van variabelen in hidden parameters. De vuistregel is dus om de invoer van gebruikers niet te vertrouwen en deze invoer daarom altijd te valideren.

Vereiste succescriteria (conformiteitvereisten)
- Beschikken over de broncode van de programmatuur.
- Voor elke controle die de webapplicatie uitvoert aan de clientzijde, is een equivalent aanwezig aan de serverzijde.

Classificatie
Hoog

Bewijsvoering
Het vaststellen is goed mogelijk, als je betrokken bent bij het ontwikkeltraject en/of beschikt over de broncode van de programmatuur, door het uitvoeren van code reviews.

Relatie met andere normen en standaarden
Zie maatregel B3-14 ‘Voer een code review uit’

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B3-7	Applicatiebeveiliging	De webapplicatie staat geen dynamische file includes toe of beperkt de keuze mogelijkheid (whitelisting).	6.2.8

Doelstelling
Voorkom dat ongewenste bestanden worden geïncorporeerd in een webapplicatie.

Rationale
Wanneer kwaadwillenden via malafide invoer willekeurige bestanden kunnen verwerken in de webapplicatie, bestaat daarmee de mogelijkheid dat zij willekeurige webapplicatie code kunnen uitvoeren op de server. Hiermee is het bijvoorbeeld mogelijk om ongeautoriseerd de database op een server te benaderen.
Mocht men toch op basis van keuzes van de gebruiker bestanden willen inlezen dan moet worden voorkomen dat de eindgebruiker directe invloed heeft op het bestand dat kan worden gebruikt (bijvoorbeeld door een whitelisting).

Vereiste succescriteria (conformiteitvereisten)

- Beschikken over de broncode van de programmatuur.
- De webapplicatie maakt geen gebruik van dynamische file includes.

Classificatie

Hoog

Bewijsvoering

Het vaststellen is goed mogelijk, als je betrokken bent bij het ontwikkeltraject en/of beschikt over de broncode van de programmatuur, door het uitvoeren van code reviews.

Relatie met andere normen en standaarden

Zie maatregel B3-14 'Voer een code review uit'

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B3-8	Applicatiebeveiliging	De webserver verstuurt alleen HTTP-headers die voor het functioneren van HTTP van belang zijn.	6.3.2

Doelstelling

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

Rationale

Het lekken van informatie moet zoveel mogelijk worden voorkomen, middels HTTP-headers kan onnodig informatie worden vrijgegeven. Het gebruik dient dus waar mogelijk te worden beperkt.
Alleen headers die voor het functioneren van HTTP van belang zijn, moeten opgenomen worden in de HTTP-responses aan gebruikers. Alle overige HTTP-headers kan de applicatie in de regel zonder gevolgen uit een HTTP-response verwijderen. Hoe HTTP-headers uit antwoorden kunnen worden verwijderd, is afhankelijk van het gebruikte type webserver.

Vereiste succescriteria (conformiteitvereisten)

Alleen headers die voor het functioneren van HTTP van belang zijn, worden opgenomen in de HTTP antwoorden aan gebruikers.

Classificatie

Hoog

Bewijsvoering

- In de ontwerp- c.q configuratie documentatie is vastgelegd welke HTTP-headers worden gebruikt.
- In de ontwerp- c.q. configuratie documentatie is vastgelegd hoe HTTP-headers uit de antwoorden worden verwijderd.
- Eventuele noodzakelijke afwijkingen van bovenstaande, omdat de webapplicatie anders niet kan functioneren, zijn vastgelegd en onderbouwd.

Relatie met andere normen en standaarden

- RFC 2616 voor http/1.1
- RFC 1945 voor http/1.0

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B3-9	Applicatiebeveiliging	De webserver toont alleen de hoogst noodzakelijke informatie in HTTP-headers die voor het functioneren van belang zijn.	6.3.2

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

Rationale
Informatie in standaard HTTP-headers (bijvoorbeeld type webserver of versienummer) kan misbruikt worden door een kwaadwillende.
Voorbeeld: Het is voor een client niet van belang om te weten welk type webserver antwoord heeft gegeven op het HTTP-request. De 'Server'-header kan dan ook uit het antwoord worden verwijderd of worden voorzien van een nietszeggende inhoud.

Vereiste succescriteria (conformiteitvereisten)
Informatie van software en systemen wordt uit de HTTP-header van het antwoord verwijderd

Classificatie
Hoog

Bewijsvoering
- In de ontwerp- c.q. configuratie documentatie is vastgelegd hoe informatie uit de antwoorden wordt verwijderd of tot een minimum wordt beperkt.
- Eventuele noodzakelijke afwijkingen van bovenstaande, omdat de webapplicatie anders niet kan functioneren, zijn vastgelegd en onderbouwd.

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B3-10	Applicatiebeveiliging	De webserver beperkt de informatie, bij het optreden van een fout, aan de gebruiker tot een minimum in een HTTP-response.	6.3.2

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

Rationale
Op het moment dat zich een probleem voordoet binnen een webapplicatie zal de webserver veelal een statuscode '500 Internal Server Error' terugsturen. Dit wijst op een exceptie en de mogelijkheid dat de webserver mogelijk gevoelige informatie over de webapplicatie openbaart (databasenamen, gebruikersnamen, bestandsnamen, interne IP-adressen, et cetera).
Een application-level firewall zou een dergelijke statuscode kunnen detecteren en een standaard foutmelding (bijvoorbeeld 'Er heeft zich een onbekende fout voorgedaan.') terugsturen naar de gebruiker en het gedetailleerde antwoord van de webserver negeren. Ook webservers zelf bieden functionaliteit om standaard meldingen te laten genereren aan de hand van specifieke statuscodes.

Vereiste succescriteria (conformiteitvereisten)
De client krijgt alleen een standaard foutmelding te zien.

Classificatie
Hoog

Bewijsvoering
- In de ontwerp- c.q. configuratie documentatie is vastgelegd welke standaard foutmelding(en) worden getoond/verstuurd.
- In de ontwerp- c.q. configuratie documentatie is vastgelegd op welke wijze dit gerealiseerd is (bijvoorbeeld door de webserver afgedwongen, een application-level firewall die gedetailleerde meldingen blokkeert et cetera).

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B3-11	Applicatiebeveiliging	Commentaarregels zijn uit de scripts (code) verwijderd.	6.3.2

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

Rationale
Commentaarregels in scripts gedurende de ontwikkel- en testfase zijn normaal, maar in een productieomgeving ongewenst omdat de commentaarregels onnodig informatie vrijgeeft waarvan een kwaadwillende misbruik van kan maken.
Application-level firewalls zijn in staat om commentaarregels uit HTML- en scriptcode te verwijderen en zodoende 'gefilterde' antwoorden terug te geven aan de client.

Vereiste succescriteria (conformiteitvereisten)
Er is een scan uitgevoerd op de scripts voordat deze in de productieomgeving zijn geplaatst. Alle commentaarregels zijn verwijderd. De application level firewall is zo geconfigureerd dat commentaarregels uit de HTML- en scriptcode worden verwijderd en een gefilterd antwoord wordt teruggegeven aan de client.

Classificatie
Hoog

Bewijsvoering
- De resultaten van de scan zijn vastgelegd.
- (Indien aanwezig) er is vastgelegd op welke wijze de application level firewall gefilterde antwoorden teruggeeft aan de client.

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B3-12	Applicatiebeveiliging	De webserver maakt alleen gebruik van de hoogst noodzakelijke HTTP-methoden.	6.3.3

Doelstelling
Voorkom (onnodige) beveiligingsrisico's door het blokkeren van niet noodzakelijke HTTP-methoden.

Rationale
HTTP ondersteunt verschillende methoden (zie RFC 2616 voor http/1.1). In de praktijk gebruikt een webapplicatie alleen de methoden GET en POST. Voor veel scripts en objecten op een webserver geldt zelfs dat alleen de GET-methode nodig is. Methoden anders dan GET en POST zijn vrijwel nooit nodig binnen traditionele webapplicaties en vormen alleen een extra beveiligingsrisico. Voor 'Web 2.0' zijn vaak wel aanvullende methoden nodig. Het is in alle gevallen aan te raden om niet benodigde methoden via configuratie van de webserver of via de application-level firewall blokkeren.

Vereiste succescriteria (conformiteitvereisten)
Niet noodzakelijke HTTP-methoden zijn geblokkeerd.

Classificatie
Hoog

Bewijsvoering
- In de ontwerp- c.q. configuratie documentatie is vastgelegd hoe de webserver is geconfigureerd om alleen noodzakelijke HTTP-methoden toe te staan.
- (indien van toepassing) in de ontwerp- c.q. configuratiedocumentatie is vastgelegd op welke wijze de application-level firewall is geconfigureerd.

Relatie met andere normen en standaarden
RFC 2616 voor http/1.1

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B3-13	Applicatiebeveiliging	Directory-listings zijn uitgeschakeld.	6.3.4

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

Rationale
Via een zogenaamde 'directory listing' kan een gebruiker via internet de inhoud van een directory bekijken. Het opvragen van een 'directory listing' via internet komt overeen met het lokaal uitvoeren van een dir-commando onder Windows of een ls-commando onder UNIX/Linux. Zodra een webserver de mogelijkheid biedt om 'directory listings' uit te voeren, bestaat de mogelijkheid dat een kwaadwillende de inhoud van 'vertrouwelijke' directories raadpleegt (zoals de '/etc/'-directory onder UNIX/Linux-systemen). De toegang tot bestanden in directories moet altijd verlopen via de webapplicatie: de webapplicatie bepaalt absolute paden voor bestanden die de gebruiker rechtstreeks mag benaderen (bijvoorbeeld afbeeldingen) en fungeert als medium voor bestanden die de gebruiker niet rechtstreeks mag benaderen (bijvoorbeeld gegevensbestanden).

Vereiste succescriteria (conformiteitvereisten)
De toegang tot bestanden in directories moet altijd verlopen via de webapplicatie.

Classificatie
Hoog

Bewijsvoering
- In de ontwerp- c.q. configuratie documentatie is vastgelegd hoe directory-listings zijn uitgeschakeld.

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B3-14	Applicatiebeveiliging	Voer een code review uit	6.4.2

Doelstelling
In een vroegtijdig stadium ontdekken van potentiële kwetsbaarheden

Rationale
Om een code review uit te voeren zijn op hoofdlijnen twee mogelijkheden:
- Geautomatiseerd scannen van de broncode
  Met behulp van geautomatiseerde tools scannen van de broncode (ook bekend als 'statische analyse') op zoek naar patronen die mogelijke kwetsbaarheden en zwakheden vormen.
- Handmatige code review
  Handmatige code review bestaat uit het zoeken in en analyseren van de broncode op zoek naar patronen die mogelijke kwetsbaarheden en zwakheden vormen. Bij een handmatige code review wordt de broncode gescand door een ander persoon dan de ontwikkelaar.

Deze aanpak, ook wel een whitebox scan of statische analyse genoemd, kan problemen aan het licht brengen die men via een blackbox scan (zie maatregel B3-15) niet zal ontdekken. Beter nog is het om de code review in verschillende stadia van het ontwikkelproces uit te voeren om op die manier fouten in een vroeg stadium en dus vaak gemakkelijker, te kunnen verhelpen. Een code review vergt over het algemeen meer inspanning dan een blackbox scan.
Tools voor het uitvoeren van geautomatiseerde code reviews bestaan er in vele soorten en maten. Onderstaande - niet uitputtende - lijst geeft enkele punten weer waarop een geautomatiseerde tool kan controleren:
- Het afvangen van excepties.
- De mogelijkheid tot het genereren van buffer overflows.
- De aanwezigheid van type mismatches.
- Gebruik van potentieel gevaarlijke functies.
- Juiste toepassing van invoervalidatie.
- Datastromen door een webapplicatie.

De noodzaak van de beveiligingsrichtlijn neemt toe naar mate de complexiteit van de webapplicatie toeneemt.

Identificeren en verwijderen van 'dode code' [47]**.**
In de broncode verwijst dode code of onbereikbare code naar stukken code die nooit uitgevoerd (kunnen) worden maar wel in de broncode aanwezig zijn. Deze code kan worden verwijderd zonder dat daarbij semantische eigenschappen van de applicatie veranderen, denk hierbij aan onverwijderde code die gebruikt is voor debuggen. Deze code zou door kwaadwillende kunnen worden misbruikt en zou verwijderd moeten worden. Het verwijderen van dode code heeft zowel voordelen tijdens het compileren als het uitvoeren van de applicatie en tevens wordt de onderhoudbaarheid van de applicatie verbeterd.
Voor het opsporen van dode code is het nodig om de broncode te analyseren. Dit kan met behulp van statische of dynamische codeanalyse en een analyse van de control flow om te kijken welke stukken code niet uitgevoerd kunnen worden.

Standaardsoftware, Software-as-a-Service (SaaS) of ontwikkeling van software is uitbesteed
Als het gaat om standaardsoftware, Software-as-a-Service (SaaS) of de ontwikkeling van de software is uitbesteed en er geen handmatige code review uitgevoerd kan/mag worden, kan worden gedacht aan de volgende aandachtspunten:
- Externe certificering van de extern ontwikkelde software.
- Afspraken in een overeenkomst vastleggen om de software te auditen.
- Afspraken over het dynamisch scannen. Bij het dynamisch scannen wordt met met behulp van geautomatiseerde tools via de (web)interface van de applicatie, terwijl de applicatie draait, gezocht naar kwetsbaarheden en zwakheden in de applicatie.
- Afspraken over het uitvoeren van andere tests, bijvoorbeeld penetratietest (zie maatregel B0-8) of blackbox scan (zie maatregel B3-15), om mogelijke kwetsbaarheden op te sporen.

Vereiste succescriteria (conformiteitvereisten)
- Beschikken over de broncode van de programmatuur.

Classificatie
Midden

Bewijsvoering
Het scannen is mogelijk, als je betrokken bent bij het ontwikkeltraject en/of beschikt over de broncode van de programmatuur, door het uitvoeren van code reviews.
Documentatie waaruit blijkt:
- dat er een code review is uitgevoerd.
- de bevindingen/rapportage van de code review.
- op welke wijze de bevindingen verwerkt zijn.

Relatie met andere normen en standaarden
- OWASP Application Security Verification Standard (ASVS)

47. Bron: 'The revival transformation, Proceedings of the 21st ACM SIGPLANSIGACT symposium on Principles of programming language', The Association, d.d. 1994.

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B3-15	Applicatiebeveiliging	Een (geautomatiseerde) blackbox scan wordt periodiek uitgevoerd.	6.4.3

Doelstelling

Testen of er kwetsbaarheden in de webapplicatie bestaan.[48]

Rationale

Een blackbox scan benadert de aanpak van een kwaadwillende het best, aangezien een tester zonder voorkennis gaat kijken of er kwetsbaarheden in de webapplicatie bestaan. Tools om blackbox scans uit te voeren zijn bekend onder de noemer Web Application Scanner (WAS). Een WAS voert een groot aantal tests uit op een webapplicatie zoals het uitproberen van verschillende varianten van SQL-injectie en XSS.
Een WAS kent enkele beperkingen die belangrijk zijn om in het achterhoofd te houden. Zo is het voor een WAS vaak moeilijk om ingelogd te blijven in webapplicaties die authenticatie vereisen. Door de grote verscheidenheid aan tests die een WAS uitvoert, bestaat de mogelijkheid dat de webapplicatie na een aantal tests de sessie beëindigt. Het is voor een WAS vaak moeilijk om te bepalen dat deze sessie is beëindigd en een cookie bijvoorbeeld niet meer geldig is. Gevolg is dat het testen van websites die authenticatie vereisen problematisch en onbetrouwbaar kan zijn. Daarnaast kunnen sterk dynamische websites voor uitdagingen zorgen. Zo zal een WAS JavaScript moeten begrijpen om effectieve tests uit te kunnen voeren. In het bijzonder nieuwe technologieën als Ajax kunnen in dit kader moeilijk testbaar zijn. Tot slot kunnen de scans die een WAS uitvoert, leiden tot een groot aantal false positives. Het is dus belangrijk dat een persoon met kennis van zaken beoordeelt in hoeverre een gemelde kwetsbaarheid ook daadwerkelijk een kwetsbaarheid is, hoe eenvoudig deze uit te buiten is en wat de schade zou zijn als gevolg van misbruik.

Wanneer blackbox scans?

Er kunnen meerdere momenten zijn waarop een blackbox scan zinvol is:

- De frequentie dient vastgesteld te worden op basis van het risicoprofiel.
- In de acceptatiefase van een nieuw systeem of een nieuwe applicatie.
- Bij significante wijzigingen van een belangrijk systeem of een belangrijke applicatie.
- Periodiek (jaarlijks/tweejaarlijks), om bestaande systemen te testen op nieuwe inbraaktechnieken en/of als onderdeel van de PDCA-cyclus (zie maatregel B0-1).
- Als er een andere reden is om te denken dat de beveiliging van een systeem minder goed is dan gedacht.

Opvolging

Er moet actie worden ondernomen indien geïmplementeerde maatregelen niet voldoen aan de gestelde eisen en/of verwachtingen of tekortkomingen opleveren.

Vereiste succescriteria (conformiteitvereisten)

- Er moet aantoonbaar follow-up worden gegeven in casu verbeteringen worden doorgevoerd indien geïmplementeerde maatregelen niet voldoen aan de gestelde eisen en/of verwachtingen of tekortkomingen opleveren.
- Zorg voor afspraken, met de leverancier, over het uitvoeren van een blackbox scan.

Classificatie

Hoog

48. Noot vooraf: dit is (dus) wat anders dan een pentest?

Bewijsvoering

Documentatie waaruit blijkt:

- dat er een blackbox scan is uitgevoerd.
- de bevindingen/rapportage van de blackbox scan.
- plan met daarin de activiteiten die worden uitgevoerd (wie, wat en wanneer) indien geïmplementeerde maatregelen niet aan de gestelde eisen en/of verwachtingen hebben voldaan of tekortkomingen hebben opgeleverd.

Relatie met andere normen en standaarden

- OWASP Application Security Verification Standard (ASVS)

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B3-16	Applicatiebeveiliging	Zet de cookie attributen 'HttpOnly' en 'Secure'	

Doelstelling

- Voorkom dat cookie communicatie kan worden afgeluisterd.
- Voorkom dat cookies gestolen kunnen worden via cross site scripting.

Rationale

HttpOnly zorgt dat de cookie uitsluitend via HTTP verbindingen gebruikt kan worden en niet via bijvoorbeeld java scripts. Secure limiteert de communicatie van cookies tot beveiligde verbindingen en voorkomt dat de cookie-inhoud voor onbevoegden zichtbaar wordt.

Vereiste succescriteria (conformiteitvereisten)

Het set cookie command bevat de secure flag en de HTTPOnly flag.

Classificatie

Hoog

Bewijsvoering

- Code review.
- Code principes (programmeer conventies).
- Documentatie.

HOOFDSTUK 6

Identiteit- en toegangsbeheer

Identiteitbeheer en toegangsbeheer zijn onlosmakelijk met elkaar verbonden. Toegangsbeheer is niet mogelijk zonder dat een correcte invulling is gegeven aan identiteitbeheer. In dit hoofdstuk worden daarom deze twee lagen uit het RBW gezamenlijk behandeld.

Onder identiteitbeheer vallen alle activiteiten die nodig zijn in het kader van identiteiten. Het gaat hierbij om het toevoegen, verwijderen en wijzigen van identiteiten (beheren van identiteiten) maar zeker ook het authenticeren van identiteiten op basis van hun authenticator. Toegangsbeheer betreft alle activiteiten die webapplicaties moeten uitvoeren om de autorisaties voor webapplicaties in te regelen en af te dwingen (runtime verifiëren van autorisaties op basis van een autorisatietabel: mag een gebruiker wel of geen gebruik maken van (delen van) de webapplicatie).

6.1 Inleiding

Een identiteit bestaat uit een identifier, een authenticator en een profiel.

De **identifier** representeert de gebruiker of de applicatie. Hierbij kun je denken aan een gebruikersnaam of een persoonsnummer als identifier. De identifier is uniek binnen een bepaald domein: zo is een gebruikersnaam (identifier) uniek binnen een applicatie (domein) en is een Burgerservicenummer (BSN) (identifier) uniek binnen Nederland (domein). Daarnaast is de identifier over het algemeen niet onderhevig aan een lifecycle. De gebruikersnaam van een medewerker voor een bepaalde applicatie wijzigt bijvoorbeeld vrijwel nooit en het BSN dat een inwoner van Nederland krijgt, verandert nooit meer.

De **authenticator** gebruikt iemand om de identifier te 'bewijzen'. Om bijvoorbeeld te bewijzen dat een gebruikersnaam een valide identifier is, moet een gebruiker ook zijn wachtwoord (authenticator) opgeven. Om te bewijzen dat het persoonsnummer inderdaad aan een bepaalde persoon toebehoort, moet deze persoon zijn paspoort (authenticator) tonen. Authenticatoren verschillen vaak in sterkte. Zo is een wachtwoord van drie letters een minder sterke authenticator dan een certificaat dat is opgeslagen op een smartcard. Daarnaast moet je de authenticator beveiligd opslaan. Een paspoort hoort normaal gesproken in de kluis, een wachtwoord in het hoofd (en soms ook in de kluis). Doordat een gebruiker zijn wachtwoord bijvoorbeeld kan opschrijven op een 'geeltje' is deze authenticator een stuk minder sterk. Tot slot is een authenticator onderhevig aan een lifecycle. Een wachtwoord moet je periodiek (bijvoorbeeld eens per maand) aanpassen, een paspoort elke 10 jaar.

Het **profiel** bevat tot slot bepaalde kenmerken (attributen en rollen) die toebehoren aan de identiteit. Hierbij moet je denken aan de rol die een medewerker vervult (bijvoorbeeld manager) of de datum waarop een medewerker in dienst is getreden. De gegevens uit het profiel slaan web-applicaties veelal in verschillende directories op (bijvoorbeeld in een personeelssysteem en op het intranet). Daarnaast kunnen de gegevens uit het profiel regelmatig wijzigen en is de informatie uit het profiel vaak privacygevoelig.

De identifier en/of het profiel bepaalt vervolgens welke autorisaties een gebruiker krijgt binnen de webapplicatie. Er bestaan verschillende mechanismen om deze autorisatie op te baseren. Enkele van de meest bekende autorisatiemechanismen zijn:

- **Role-based Access Control** (**RBAC**). Toegang tot (onderdelen van) de webapplicatie is afgeschermd door het toekennen van rollen aan gebruikers en het toekennen van rechten aan rollen.
- **Rule-based Access Control.** Dit model beschrijft specifieke regels waaraan een gebruiker moet voldoen, voordat deze toegang krijgt op basis van gegevens uit zijn profiel. Bij rule-based access control verleent het mechanisme toegang op basis van de waarden van de attributen bij een gebruiker (bijvoorbeeld attribuut securityclearance - 'yes'). Daarom kan, afhankelijk van de implementatie, rule-based access control performancevoordelen geven boven control-mechanismen waarbij de server vaak een grote groep moet nalopen op een mogelijk lidmaatschap van een bepaalde gebruiker.
- **Mandatory Access Control** (**MAC**)**.** Dit model baseert de autorisaties op classificaties of labels aan een object, gecombineerd met het classificatieniveau of de labels van de gebruiker.
- **Discretionary Access Control** (**DAC**)**.** Toegang tot bestanden wordt bij DAC bepaald door de rechten die een gebruiker heeft toegewezen gekregen. De eigenaar van het bestand kan vervolgens zelf weer rechten uitdelen aan andere gebruikers.

6.2 Kwetsbaarheden en bedreigingen

Deze paragraaf beschrijft kwetsbaarheden en bedreigingen die zich voor kunnen doen op het gebied van identiteit- en toegangsbeheer.

Mogelijke kwetsbaarheden en bedreigingen zijn:

Nr.	Beveiligingslaag	Kwetsbaarheid	Referentie RBW
K4-1	Identiteit- en toegangsbeheer	Foutieve implementatie van authenticatie en sessiemanagement	8.2.1

Toelichting

HTTP kent geen mechanisme om de status van een sessie te behouden. Wanneer een gebruiker zich heeft geauthenticeerd tot een webapplicatie, is het wenselijk dat de web-applicatie onthoudt dat de gebruiker zich succesvol heeft geauthenticeerd. Anders zou de gebruiker zich bij elk volgend verzoek opnieuw moeten authenticeren en de historie van zijn acties binnen de webapplicatie verloren gaan.
Om de sessie tussen een gebruiker en een webapplicatie te 'fixeren' heeft de systeem-ontwikkelaar de volgende mechanismen ter beschikking:

- Sessiefixatie op basis van argumenten in de URL.
- Sessiefixatie op basis van verborgen velden.
- Sessiefixatie op basis van cookies.

Ongeacht de toegepaste manier van sessiefixatie kunnen problemen ontstaan. Hieronder worden twee van deze problemen beschreven:

- Een kwaadwillende ontdekt dat een webapplicatie gebruik maakt van het verborgen veld genaamd 'userid'. Bij het initieel benaderen van de webapplicatie is dit verborgen veld leeg. Nadat de kwaadwillende probeert in te loggen met een standaard gebruikersnaam en wachtwoord mislukt dit en het veld 'userid' blijft leeg. De kwaadwillende probeert vervolgens om het inlogscherm te omzeilen en een verzoek aan de webapplicatie te richten waarin hij het verborgen veld 'userid' de waarde 'Blackhat' geeft. Hierna krijgt de kwaadwillende de melding 'Welkom Blackhat' en kan hij gebruik maken van de webapplicatie zonder zich geauthenticeerd te hebben. De webapplicatie vertrouwt in dit geval volledig op de waarde van het verborgen veld 'userid'.
- Een reguliere gebruiker logt in op de webapplicatie en ziet vervolgens dat in de URL continu de parameter 'sessieid=9001' terug te vinden is. De gebruiker vraagt zich af of hij deze parameter kan misbruiken door een andere waarde op te geven voor de sessieid. Nadat hij de waarde van de parameter verandert in 'sessieid=9000' is hij nog steeds geauthenticeerd en krijgt hij de gegevens te zien van een ander persoon die op dat moment ook is ingelogd. De webapplicatie blijkt gebruik te maken van oplopende sessie-ID's die zeer eenvoudig te voorspellen zijn.

Authenticatie- en sessiemanagement zijn lastige onderdelen van een webapplicatie. Niet alleen het fixeren van een sessie maar ook het uiteindelijk beëindigen van een sessie kan problemen met zich meebrengen. De volgende vraag doet zich in dit kader voor: hoe zorgen we ervoor dat de webapplicatie een sessie uiteindelijk ook weer afsluit? Sessies kunnen immers niet oneindig lang blijven bestaan. De aanwezigheid van een sessie zorgt aan de ene kant voor onnodig resourcegebruik op de server (de server moet alle sessies bijhouden en hiervoor geheugen reserveren) en daarnaast voor een beveiligingslek.
Hoe meer sessies een webserver op enig moment open heeft staan, hoe groter de kans dat een kwaadwillende erin slaagt één van deze sessies te kraken. En ook: hoe langer een sessie actief blijft, hoe langer eventueel onderschepte sessiegegevens bruikbaar blijven voor een kwaadwillende (denk bijvoorbeeld aan misbruik van een cookie in een internetcafé).

Referentie OWASP Top-10
A3 - Broken Authentication and Session Management
https://www.owasp.org/index.php/Top_10_2010-A3

OWASP Application Security Verification Standard (ASVS)
- V2 - Authentication Verification Requirement
  http://code.google.com/p/owasp-asvs/wiki/Verification_V2
- V3 - Session Management Verification Requirements
  http://code.google.com/p/owasp-asvs/wiki/Verification_V3

Nr.	Beveiligingslaag	Kwetsbaarheid	Referentie RBW
K4-2	Identiteit- en toegangsbeheer	Foutieve implementatie van toegangsbeheer	8.2.2

Toelichting
Vergelijkbare problemen als bij authenticatie en sessiemanagement (zie vorige kwetsbaarheid) kunnen zich voordoen bij toegangsbeheer. Toegangsbeheer volgt op authenticatie en houdt in dat de webapplicatie controleert of een gebruiker gerechtigd is om bepaalde acties uit te voeren. Denk hierbij aan het mogen uitvoeren van een bepaalde transactie of het mogen bekijken van een specifieke webpagina.
De volgende voorbeelden illustreren implementatiefouten die ertoe kunnen leiden dat de webapplicatie deze autorisaties niet goed afhandelt:
- De webapplicatie voert geen normalisatie van het verzoek vanaf de gebruiker uit.
- De webapplicatie baseert de toegang tot de beveiligde directory op basis van de waarde van een cookie.
- Een kwetsbaar script binnen de webapplicatie voert geen goede invoervalidatie uit.

OWASP Application Security Verification Standard (ASVS)
- V4 - Access Control Verification Requirements
  http://code.google.com/p/owasp-asvs/wiki/Verification_V4

Nr.	Beveiligingslaag	Kwetsbaarheid	Referentie RBW
K4-3	Identiteit- en toegangsbeheer	Ongeautoriseerde directe objectreferenties	8.2.3

Toelichting
Zodra een gebruiker zich via een authenticatiemechanisme heeft geauthenticeerd op een webapplicatie, krijgt deze vervolgens de beschikking over de toegang tot verschillende typen objecten. Denk aan databaserecords, bestanden en directories. Een webapplicatie gaat goed om met de objecten die het de gebruiker aanbiedt, maar 'faalt' in het autoriseren wanneer de gebruiker de referenties naar objecten handmatig wijzigt.

Nr.	Beveiligingslaag	Kwetsbaarheid	Referentie RBW
K4-4	Identiteit- en toegangsbeheer	Onveilige authenticatiemechanismen	8.2.4

Toelichting
Niet alle authenticatiemechanismen die een webapplicatie kan gebruiken, zijn even veilig. Een belangrijk gevaar dat verbonden is aan het gebruik van authenticatiemechanismen, is de mogelijkheid tot het achterhalen casu quo onderscheppen hiervan. Als een kwaadwillende erin slaagt om authenticatiegegevens te achterhalen, kan deze zich voordoen als iemand anders.

Voor het onderscheppen van authenticatiegegevens heeft de kwaadwillende een aantal mogelijkheden:

- Phishing
- Social engineering
- Sniffing
- Cross-Site Scripting (XSS)

Ook standaard - en veel gebruikte -authenticatiemechanismen zijn niet per definitie veilig. Denk aan gebruikersauthenticatie op basis van het basic authentication mechanisme binnen HTTP. Dit authenticatiemechanisme maakt gebruik van base64 encoding. Strings die op basis van base64 zijn gecodeerd, zijn ook eenvoudig weer te decoderen. Het is eenvoudig om via een simpele tool (base64 decoder) een gebruikersnaam en een wachtwoord uit deze string te 'toveren'. Als een kwaadwillende deze gegevens weet te sniffen, dan is het voor deze kwaadwillende zeer eenvoudig om de inhoud ervan te misbruiken.

Nr.	Beveiligingslaag	Kwetsbaarheid	Referentie RBW
K4-5	Identiteit- en toegangsbeheer	Discrepantie tussen authenticatiemechanisme en beveiligingsbeleid	8.2.5

Toelichting

Bij veel projecten besteedt men, als gevolg van bijvoorbeeld tijdsdruk, onvoldoende aandacht aan het projecteren van het beveiligingsbeleid van de organisatie op de webapplicatie en de bijbehorende data. Gevolg: de authenticatie is veel te 'zwaar' voor de data die de webapplicatie gebruikt, of de authenticatie is veel te 'zwak'. In geen van de gevallen is er sprake van een ideale situatie. In het tweede geval is er zelfs sprake van een beveiligingsrisico, omdat data onvoldoende beschermd bereikbaar is via internet. Discrepantie tussen het authenticatiemechanisme en het beveiligingsbeleid kan ook gedurende de levenscyclus van een webapplicatie ontstaan. Op het moment dat een nieuwe webapplicatie het levenslicht ziet, voert de organisatie bijvoorbeeld een risicoanalyse uit, waaruit voortvloeit dat de webapplicatie voldoende beschermd is op basis van gebruikersnaam/wachtwoord authenticatie. De webapplicatie groeit vervolgens een aantal jaren door waarbij de organisatie steeds meer functionaliteiten en data aan de webapplicatie toevoegt. Wat een organisatie vaak nalaat is, om regelmatig een risicoanalyse uit te voeren op de webapplicatie. Op een gegeven moment voldoet het gebruikte authenticatiemechanisme niet meer voor de gestaag doorgegroeide webapplicatie.

Nr.	Beveiligingslaag	Kwetsbaarheid	Referentie RBW
K4-6	Identiteit- en toegangsbeheer	Het wiel opnieuw uitvinden	8.2.6

Toelichting

De implementatie van authenticatie- en toegangsmechanismen is niet altijd triviaal. De implementatie ervan kan veel tijd en moeite in beslag nemen als het gaat om complexe authenticatiemechanismen (digitale certificaten, tokens) en complexe toegangsmatrices (veel rollen, veel resources). Bij iedere implementatie bestaat de kans op (beveiligings-) fouten, moet je beheermechanismen inregelen, moeten diepgaande testen worden uitgevoerd, et cetera.

Het is reëel dat een authenticatiemechanisme meerdere malen wordt uitgevonden, zeker als verschillende webapplicaties op verschillende manieren worden ontsloten en daarbij verschillende protocollen en technologieën worden gebruikt. Stel dat een organisatie start met een webapplicatie die gebruikers benaderen via hun webbrowser (op basis van HTML).

De webapplicatie is beschermd met een gebruikersnaam en een wachtwoord. Vervolgens besluit de organisatie om delen van de webapplicatie ook beschikbaar te stellen via een webservice (op basis van XML). Ook deze webservice wil men beschermen op basis van een gebruikersnaam en een wachtwoord. In veel gevallen moet je voor deze webservice een nieuw authenticatieproces inrichten. Dit terwijl het grootste gedeelte van het bestaande authenticatiemechanisme (in veel gevallen) herbruikt kan worden.

Nr.	Beveiligingslaag	Kwetsbaarheid	Referentie RBW
K4-7	Identiteit- en toegangsbeheer	Incompatibele authenticatiemechanismen	8.2.7

Toelichting

Wanneer je het wiel voor elke webapplicatie opnieuw uitvindt (§8.2.6), bestaat de kans dat webapplicaties een groot aantal verschillende authenticatiemechanismen implementeren om deze te beschermen. Deze incompatibiliteit kan tot verschillende problemen leiden.

Enkele van de meest voorkomende zijn:

- Bij het 'in elkaar schuiven' van verschillende webapplicaties (bijvoorbeeld verschillende bestaande webapplicaties achter een nieuw te ontwikkelen portaal) ontstaan problemen, omdat de verschillende authenticatiemechanismen ervoor zorgen dat gebruikers op elke afzonderlijke webapplicatie opnieuw moeten inloggen. Het is, met andere woorden, niet mogelijk om via één account toegang te verkrijgen tot de afzonderlijke webapplicaties (Single Sign-On).

- De beheertooling voor het ene authenticatiemechanisme is niet bruikbaar voor het andere. Gevolg hiervan is dat voor elk authenticatiemechanisme een apart beheerproces (inclusief achterliggende techniek) ingericht moet worden voor gebruikersbeheer, rollenbeheer, et cetera.
- Het is niet mogelijk een goed profiel op te bouwen van een gebruiker. Wanneer persoon A account A1 in webapplicatie 1 krijgt en account A2 in webapplicatie 2, zijn deze twee identiteiten veelal niet met elkaar te combineren of moeten hiervoor onevenredig veel activiteiten worden ondernomen. Hierdoor kun je geen geheel omvattend profiel van deze persoon maken en moeten webapplicaties overlappende gegevens ieder apart bijhouden (denk hierbij bijvoorbeeld aan een adreswijziging die elke webapplicatie afzonderlijk moet doorvoeren).

6.3 Doelstelling

Het beheersen van de identiteit en toegang, zodat ongeautoriseerde toegang tot informatie, informatiesystemen en -diensten wordt voorkomen.

Deze toegang dient te worden beheerst op grond van zakelijke behoeften en maatregelen. Er moet een balans zijn tussen risicobeheersing, efficiënte bedrijfsprocessen (door het automatiseren van arbeidsintensieve taken, zoals het aanmaken/wijzigen en verwijderen van accounts en bijbehorende autorisaties wordt de beheeromgeving ontlast), kostenbeheersing en het voldoen aan wet- en regelgeving.

6.4 Beveiligingsrichtlijnen

De paragraaf besteedt aandacht aan de maatregelen om identiteit- en toegangsbeheer voor webapplicaties en de onderliggende infrastructuur in te richten.

Onderstaande maatregelen zijn onderdeel van maatregel B0-10 maar vanwege de beperkte adressering in hoofdstuk 11 'Toegangsbeveiliging' uit de NEN-ISO /IEC 27002 'Code voor informatiebeveiliging' worden ze ook afzonderlijk geadresseerd.

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B4-1	Identiteit- en toegangsbeheer	Maak gebruik van Identity & Access Management tooling.	8.3.2

Doelstelling

Het efficiënter maken van het identiteit- en toegangsbeheer.
Denk hierbij aan het automatiseren van arbeidsintensieve taken (workflow), zoals het aanmaken, wijzigen en verwijderen van gebruikersinformatie en bijbehorende autorisaties (de complete levenscyclus). Hierdoor is het op- en afvoeren van gebruikers eenvoudiger te regelen en te beheren.

Rationale

Als het ontwerp met betrekking tot identiteit- en toegangsbeheer is vastgesteld (zie maatregel B0-10), kan worden bepaald/bekeken waar tooling kan worden ingezet. Denk hierbij aan I&AM (Identity & Access Management) tooling.
De keuze voor dergelijke tooling wordt mede bepaald door de keuze om delen van identiteit- en toegangsbeheer buiten webapplicatie(s) te plaatsen (te centraliseren).
Door het inzetten van tooling 'vermindert' de complexiteit van webapplicatie omdat het authenticeren en autoriseren van gebruikers uit de webapplicatie wordt gehaald.
Door de authenticatie los te trekken van de webapplicatie, is het eenvoudiger om in de toekomst andere authenticatoren in te zetten voor het beveiligen van de webapplicatie.
Hiervoor voer je wijzigingen door in de tooling en hoeft de achterliggende webapplicatie hier 'in principe' niets van te merken.

Vereiste succescriteria (conformiteitvereisten)

- Er moet een beleid zijn ten aanzien van identiteit- en toegangsbeheer.
- Er moeten procedures zijn voor identiteit- en toegangsbeheer.
- De inrichting van het identiteit- en toegangsbeheer is gebaseerd op een vastgesteld inrichtingsdocument/ontwerp, waarin is vastgelegd welke functies (identiteit-, authenticator, profiel- en toegangsbeheer), waar (centraal/decentraal) worden uitgevoerd.
- Zorg dat het inrichtingsdocument/ontwerp onderdeel is van het proces wijzigingsbeheer.
- Het inrichtingsdocument/ontwerp:
  - heeft een eigenaar.
  - is voorzien van een datum en versienummer.
  - is actueel.
  - is op het juiste niveau geaccordeerd.

Classificatie

Midden

Bewijsvoering

- Beleid ten aanzien van identiteit- en toegangsbeheer.
- Procedures voor identiteit- en toegangsbeheer.
- Ontwerp/architectuur van identiteit- en toegangsbeheer, inclusief de besluitvorming.

Relatie met andere normen en standaarden

- NEN-ISO /IEC 27002 'Code voor informatiebeveiliging'.
  - hoofdstuk 11 Toegangsbeveiliging.

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B4-2	Identiteit- en toegangsbeheer	Daar waar de gebruiker en/of beheerder kan inloggen op de webapplicatie is expliciete functionaliteit aanwezig om uit te loggen (het verbreken van de sessie).	8.3.4

Doelstelling

Voorkom misbruik van een niet meer gebruikte sessie.

Rationale

Een webapplicatie moet ook de mogelijkheid bieden om een bestaande sessie weer te verbreken (logout).
Bij het authenticeren van gebruikers wordt aandacht besteed aan het inloggen van gebruikers, maar wordt geen aandacht besteed aan het uitloggen. Tijdens het uitloggen van een gebruiker wordt zijn sessie onklaar gemaakt en kan een kwaadwillende met eventuele onderschepte sessiegegevens geen verbinding meer opzetten.
Verder is het van belang aandacht te besteden aan de idle time-out en de verbindingstijd per sessie. Hoe lang mag een gebruiker verbonden (geauthenticeerd) blijven zonder zichtbare activiteit? Stel een idle time-out in dat gebruikers automatisch worden uitgelogd op het moment dat zij geen gebruik meer (lijken te) maken van de webapplicatie. Ook de beperking van de sessieduur (verbindingstijd) biedt aanvullende beveiliging voor webapplicaties. Door de sessieduur te beperken, neemt de kans op ongeautoriseerde toegang af. Deze functionaliteiten zijn niet alleen aanwezig, maar worden ook toegepast/afgedwongen.
Op deze manier wordt het risico verminderd dat een kwaadwillende een webapplicatie ongeautoriseerd kan benaderen, doordat een vorige gebruiker vergeten is uit te loggen.

Vereiste succescriteria (conformiteitvereisten)

- Gebruikers hebben de mogelijkheid om uit te loggen van een webapplicatie.
- Na een bepaalde periode van inactiviteit worden de netwerkverbinding (sessie) automatisch verbroken (idle time-out).
- Na een bepaalde verbindingstijd wordt de netwerkverbinding (sessie) automatisch verbroken.

Classificatie

Hoog

Bewijsvoering

- Ontwerp van de webapplicatie.
- Configuratie van de webapplicatie waaruit blijkt dat een idle time-out en sessieduur is toegepast/afgedwongen.

Relatie met andere normen en standaarden

- NEN-ISO /IEC 27002 'Code voor informatiebeveiliging'.
  - paragraaf 11.5.5 'Time-out van sessies'.
  - paragraaf 11.5.6 'Beperking van verbindingstijd'.

HOOFDSTUK 7

Vertrouwelijkheid en onweerlegbaarheid

Vertrouwelijkheid en onweerlegbaarheid zijn nauw aan elkaar verbonden door het gebruik van cryptografische sleutels. Als gebruik wordt gemaakt van asymmetrische versleuteling (verschillende sleutels voor versleuteling en ontsleuteling), is het publieke deel van de sleutel bestemd voor versleuteling (vertrouwelijkheid) van gegevens. Het privédeel van de sleutel is bestemd voor ontsleuteling en het plaatsen van digitale handtekeningen (onweerlegbaarheid/onloochenbaarheid). Dit hoofdstuk gaat dieper in op de begrippen vertrouwelijkheid en onweerlegbaarheid in het kader van webapplicaties.

De laag 'Vertrouwelijkheid en onweerlegbaarheid' vormt de laatste schakel (laag) in het contact tussen een client en een webapplicatie. Deze laag is vooral sterk afhankelijk van de inrichting van identiteit-beheer (zie hoofdstuk 6 'Identiteit- en toegangsbeheer').
Voor het kunnen versleutelen van gegevens en het vaststellen van onweerlegbaarheid is het namelijk van belang dat er wederzijdse authenticatie heeft plaatsgevonden. Dit hoofdstuk gaat eerst in op kwetsbaarheden en bedreigingen op dit gebied om vervolgens de maatregelen te beschrijven.

7.1 Kwetsbaarheden en bedreigingen

Deze paragraaf beschrijft kwetsbaarheden en bedreigingen die zich voor kunnen doen op het gebied van vertrouwelijkheid en onweerlegbaarheid. De belangrijkste kwetsbaarheden en bedreigingen zijn de twee tegenpolen van de begrippen vertrouwelijkheid en onweerlegbaarheid: lekken van informatie en weerlegbaarheid.
Tevens wordt in deze paragraaf misbruik van certificaten en de gevolgen daarvan beschreven.
Mogelijke kwetsbaarheden en bedreigingen zijn:

Nr.	Beveiligingslaag	Kwetsbaarheid	Referentie RBW
K5-1	Vertrouwelijkheid en onweerlegbaarheid	Lekken van informatie	9.2.1

Toelichting

Van lekken van informatie is sprake wanneer vertrouwelijke informatie onbedoeld terecht komt bij ongeautoriseerde personen of als informatie onnodig wordt verstrekt. Dit hoeft dus niet noodzakelijk vertrouwelijke informatie te zijn.
De volgende voorbeelden beschrijven situaties waarin de webapplicatie onnodig(e) informatie verstrekt:

- Een webserver toont de gebruikte versies van software en plug-ins.
- Een script bevat commentaar waarin details over de werking van het script zijn opgenomen.
- Een foutmelding bevat informatie over de gebruikte database met bijbehorende gebruikersnamen en wachtwoorden.

De volgende voorbeelden beschrijven situaties waarin gevoelige informatie wordt gelekt richting ongeautoriseerde personen:

- Een kwaadwillende slaagt erin vertrouwelijke gegevens uit de database van de web-applicatie op te halen.
- Een kwaadwillende slaagt erin bestanden met vertrouwelijke informatie (bijvoorbeeld Word-documenten en tekstbestanden) op de webserver te benaderen.
- Een kwaadwillende slaagt erin om vertrouwelijke gegevens te onderscheppen, die vrij leesbaar over het internet worden uitgewisseld.
- Een kwaadwillende slaagt erin bestanden met vertrouwelijke informatie uit het interne netwerk te benaderen, terwijl deze bestanden niet bedoeld zijn voor ontsluiting via de webapplicatie.

Nr.	Beveiligingslaag	Kwetsbaarheid	Referentie RBW
K5-2	Vertrouwelijkheid en onweerlegbaarheid	Weerlegbaarheid	9.2.1

Toelichting

Er is sprake van weerlegbaarheid als de webapplicatie geen mogelijkheden biedt om belangrijke zaken rondom een transactie te bewijzen. De volgende zaken vallen onder de weerlegbaarheid van een transactie:
De bron van een transactie.
Een zendende partij kan ontkennen dat een bepaald bericht van hem afkomstig is.

- Het tijdstip van een transactie.
  Een zendende of ontvangende partij kan ontkennen dat een transactie op een bepaald tijdstip heeft plaatsgevonden.
- De ontvangst van een transactie.
  Een ontvangende partij kan ontkennen dat deze een bepaalde transactie heeft ontvangen.

- De inhoud van een transactie (integriteit).
  Een zendende of ontvangende partij kan ontkennen dat een transactie een bepaalde inhoud bevatte.

Misbruik van certificaten en de gevolgen daarvan zijn:

Nr.	Beveiligingslaag	Kwetsbaarheid	Referentie RBW
K5-3	Vertrouwelijkheid en onweerlegbaarheid	Misbruik van een vals subcertificaat voor een specifiek domein	

Toelichting
Misbruik van een vals subcertificaat voor een specifiek domein (bijvoorbeeld google.com). Dit kan bijvoorbeeld verkregen worden door toegang tot een filesysteem van een webdienst waarop dit certificaat wordt of door toegang tot een server die deze certificaten kan genereren.
Misbruik kan tot gevolg hebben dat de authenticiteit, vertrouwelijkheid en integriteit van de dragers van deze certificaten (websites, berichten, documenten, et cetera) niet meer gegarandeerd zijn en dat gevoelige informatie kan worden ontfutseld en schade kan worden geleden.

Nr.	Beveiligingslaag	Kwetsbaarheid	Referentie RBW
K5-4	Vertrouwelijkheid en onweerlegbaarheid	Misbruik van een vals rootcertificaat	

Toelichting
Misbruik van een vals rootcertificaat, waardoor alle sub certificaten van deze root niet meer vertrouwd zijn. Dit kan verkregen worden wanneer kwaadwillenden toegang hebben tot de servers van CA's die root certificaten genereren of opslaan.
Misbruik kan tot gevolg hebben dat de authenticiteit, vertrouwelijkheid en integriteit van de dragers van deze certificaten (websites, berichten, documenten, et cetera) niet meer gegarandeerd zijn en dat gevoelige informatie kan worden ontfutseld en schade kan worden geleden. Deze vorm is daarbij ernstiger omdat de reikwijdte groter is: kwaadwillenden kunnen in dat geval voor elk willekeurig domein certificaten genereren. Ook kunnen wellicht valse certificaten voor code signing of document signing gegenereerd worden.

7.2 Doelstelling

Zorgen dat geen informatie wordt gelekt en dat onweerlegbaarheid wordt ondersteund.

7.3 Beveiligingsrichtlijnen

De paragraaf besteedt aandacht aan maatregelen die zorgen dat bij transacties via webapplicaties geen gegevens uitlekken en dat daarnaast zender en ontvanger niet kunnen betwisten dat deze transacties hebben plaatsgevonden.

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B5-1	Vertrouwelijkheid en onweerlegbaarheid	Voer sleutelbeheer in waarbij minimaal gegarandeerd wordt dat sleutels niet onversleuteld op de servers te vinden zijn.	9.3

Doelstelling

Doelmatig gebruik van cryptografische technieken door het beheren van cryptografische sleutels.

Rationale

Het beheer van cryptografische sleutels is van essentieel belang voor een doelmatig en veilig gebruik van cryptografische technieken. Compromittering of verlies van cryptografische sleutels kan de vertrouwelijkheid, authenticiteit en/of integriteit van informatie in gevaar brengen.

Een sleutelbeheersysteem moet er minimaal voor zorgen dat sleutels niet onversteuteld op de servers te vinden zijn. Daarnaast kan gedacht worden aan de volgende procedures en beveiligingsmethoden:

- Hoe worden sleutels gegenereerd voor verschillende toepassingen?
- Hoe worden certificaten voor publieke sleutels gegenereerd en verkregen?
- Hoe sleutels worden bewaard, inclusief een instructie hoe geautoriseerde gebruikers toegang tot sleutels kunnen krijgen?
- Hoe het wijzigen of actualiseren van sleutels moet geschieden?
- Hoe wordt omgaan met sleutels die zij gecompromitteerd?
- Hoe sleutels moeten worden herroepen, ingetrokken of gedeactiveerd?
- Hoe sleutels hersteld moeten worden die verloren of gecompromitteerd zijn?
- Hoe sleutels worden gearchiveerd?
- Hoe sleutels worden vernietigd?
- Hoe activiteiten in verband met sleutelbeheer worden vastgelegd en gecontroleerd?
- Welke minimale sleutellengtes moeten worden toegepast?
- Welke encryptie-algoritmen moeten worden toegepast?

Vereiste succescriteria (conformiteitvereisten)

- Er moet beheerproces rondom sleutels en certificaten zijn ingevoerd.
- Het inrichtingsdocument/ontwerp:
  - heeft een eigenaar.
  - is voorzien van een datum en versienummer.
  - is actueel.
  - is op het juiste niveau geaccordeerd.
  - maakt onderdeel uit van het standaard wijzigingsbeheerproces.

Classificatie

Hoog

Bewijsvoering

- Procedure en procesbeschrijving rondom het beheer van certificaten.
- inrichtingsdocument/ontwerp.

Relatie met andere normen en standaarden

- NEN-ISO /IEC 27002 ‘Code voor informatiebeveiliging’.
  - paragraaf 12.3.2 ‘Sleutelbeheer’.

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B5-2	Vertrouwelijkheid en onweerlegbaarheid	Maak gebruik van versleutelde (HTTPS) verbindingen.	9.3.1

Doelstelling

Voorkom misbruik van (vertrouwelijke) gegevens die tijdens transport zijn onderschept.

Rationale

HTTP biedt standaard ondersteuning om een versleutelde verbinding op te zetten tussen de client en server. Voor de versleuteling maakt HTTP gebruik van het Secure Sockets Layer protocol (SSL) of het Transport Layer Security (TLS) protocol. Door de verbinding richting de webapplicatie te versleutelen via SSL of TLS wordt voorkomen dat kwaadwillenden eenvoudig de verkeersstromen tussen client en server kunnen inzien. Bij het gebruik van SSL en TLS betreft het versleuteling op transportniveau. Op de server zorgt het webserverproces voor ontsleuteling van de informatie, waarna de webapplicatie met onversleutelde informatie aan de slag gaat. Om informatie aan de serverzijde versleuteld op te slaan in bestanden en databases, moeten aparte maatregelen worden getroffen (zie maatregel B5-3).
Bij de inzet van een Web Application Firewall handelt niet de webserver, maar de WAF de SSL-verbinding af. Zodra de SSL-verbinding tot stand is gekomen, zal de WAF de verbinding doorgeven naar de achterliggende webserver. De verbinding tussen de WAF en de achterliggende webserver hoeft niet per definitie op basis van SSL of TLS tot stand te komen, maar hier kan voor een onversleutelde HTTP worden gekozen. Dit laatste geldt als deze laatste verbinding zich binnen een vertrouwde en afgeschermde omgeving bevindt (de DMZ, zie maatregel B1-1). Het voordeel van een dergelijke aanpak is, dat de achterliggende webserver niet wordt belast met SSL-versleuteling en dat daarnaast de mogelijkheid bestaat om het netwerkverkeer te bekijken met aanwezige Intrusion Detection Systemen (IDS).

Bij gebruik van SSL kan worden gekozen tussen verschillende versleutelingprotocollen voor (1) het uitwisselen van sleutels, (2) het authenticeren van de eindgebruiker en de server en (3) het versleutelen van de gegevens. Belangrijk is om voor elk van deze functionaliteiten een sterk protocol te kiezen, zodat kwaadwillenden niet in staat zijn de SSL-beveiliging te breken.
Het is belangrijk om een goed beheerproces rondom de certificaten in te voeren. Zodra een certificaat bijvoorbeeld niet meer geldig is, krijgen gebruikers een waarschuwing te zien bij het bezoeken van de site of werkt de webapplicatie in zijn geheel niet meer.

Verzend (contact)formulieren over versleutelde verbindingen.
(Contact)formulieren waarmee bijvoorbeeld vragen gesteld kunnen worden verplichten vaak het invullen van persoonsgegevens, in sommige gevallen moet ook vertrouwelijke informatie zoals het burgerservicenummer worden ingevuld. Door deze formulieren over een onversleutelde verbinding (HTTP in plaats van HTTPS) te verzenden bestaat de mogelijkheid dat de ingevulde gegevens door derden onderschept kunnen worden.

Vereiste succescriteria (conformiteitvereisten)

- De inrichting is gebaseerd op een vastgesteld inrichtingsdocument/ontwerp, waarin is vastgelegd welke uitgangspunten gelden voor de toepassing van versleutelde verbindingen (SSL/TLS).
- Er vindt een redirect plaats van HTTP naar HTTPS op het moment dat een (contact) formulier wordt opgevraagd.

Classificatie

Hoog

Bewijsvoering

- In de ontwerp- c.q. configuratie documentatie is vastgelegd hoe de webserver is geconfigureerd met betrekking tot versleutelde verbindingen (SSL/TLS).
- De zakelijke behoeften en beveiligingseisen. Rapportage van de risicoanalyse waarop de beslissing is gebaseerd.
- Configuratie van de webserver

Relatie met andere normen en standaarden

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B5-3	Vertrouwelijkheid en onweerlegbaarheid	Sla gevoelige gegevens versleuteld of gehashed op	9.3.2

Doelstelling

Voorkom misbruik van opgeslagen vertrouwelijke gegevens.

Rationale

Sla gevoelige gegevens versleuteld of gehashed op. Zorg ook voor versleuteling op web-applicatieniveau, door gebruik te maken van versleuteling of hashing in de database en/of bestanden. Wat gevoelige (vertrouwelijke) gegevens zijn, moet door de organisatie op basis van een risicoanalyse/classificatieschema worden vastgesteld.Het is niet nodig om alle informatie in een database te versleutelen. Alleen de informatie die waardevol kan zijn voor een aanvaller, moet extra worden beveiligd. Maakt een database gebruik van encryptiemechanismen, dan betekent dit niet automatisch dat versleutelde gegevens niet meer zichtbaar zijn voor aanvallers. Vaak vindt encryptie plaats op bestandsniveau. Op logisch niveau verandert er niets: queries die een webapplicatie op een database afvuurt, worden door de database nog steeds met dezelfde resultaten beantwoord. Het is van belang dat bij gebruik van encryptie, de webapplicatie zelf functies aanroept voor het ver- en ontsleutelen van de veldwaarden. Doet de webapplicatie dit niet, dan kan de webapplicatie niet voorkomen dat SQL-injectie leidt tot het onbedoeld vrijgeven van alle vertrouwelijke informatie uit de database.

Een alternatief voor het versleutelen van informatie is het gebruik van hashes[49].
Het verschil met encryptie is dat uit een hash nooit de originele tekst kan worden bepaald. Het wordt dan ook vaak gebruikt in gevallen waarbij de webapplicatie geen inzicht in de originele invoer hoeft te hebben. Een populaire toepassing van hashing is het opslaan van wachtwoorden. De webapplicatie maakt een hash van het wachtwoord dat de gebruiker heeft ingevoerd en controleert vervolgens of deze hash overeenkomt met de hash in de database. Slaagt een kwaadwillende er via SQL-injectie in om de tabel met gebruikers en wachtwoorden uit te lezen, dan heeft deze alleen de beschikking over de hashes van wachtwoorden en niet de wachtwoorden zelf. Dit is zeker het geval als de webapplicatie het wachtwoord ook nog eens voorziet van een zogenoemde salt, een willekeurige string die de webapplicatie aan elk wachtwoord plakt voordat de hash gemaakt wordt. Hierbij dient wel opgemerkt te worden dat een kwaadwillende via een brute-force-aanval of via vooraf berekende hash-waarden van wachtwoorden (rainbow tables) het originele wachtwoord kan bepalen. Een rainbow-tables-aanval kan zeer snel verlopen. Een brute-force-aanval duurt lang en wordt vooral gebruikt om minder makkelijke wachtwoorden te achterhalen. Bovenop (of in plaats van) transportversleuteling via SSL/TLS kan ook worden gekozen om specifieke onderdelen van een bericht te versleutelen. Hiermee wordt voorkomen dat een kwaadwillende, via een man-in-the-middle aanval, de SSL/TLS-sessie onderbreekt en daarmee toegang krijgt tot de inhoud van HTML- en XML-berichten. Voor het versleutelen

49. Hashing wordt over het algemeen gebruikt om de integriteit van gegevens te waarborgen.

van specifieke onderdelen uit een XML-bericht bestaat een aantal standaarden; voor HTML-berichten is dat niet het geval. De XML-Encryption standaard is een voorbeeld van de versleuteling van gegevens in een XML-bestand. Met deze standaard is het mogelijk om een gedeelte van het XML-bericht te versleutelen en sleutelinformatie te versturen.
Bij een architectuur waar gebruik wordt gemaakt van een messagebroker (webapplicatie communiceert via een messagebroker met de eindgebruiker en niet rechtstreeks) kan ook worden gekozen om onderdelen van een bericht te versleutelen. Door onderdelen van het bericht te versleutelen, wordt voorkomen dat een messagebroker inzage krijgt in mogelijk vertrouwelijke gegevens.

Maak gebruik van beschikbare standaardbibliotheken om versleuteling van gegevens te bereiken, boven zelf ontwikkelde versleuteling toe te passen.
Maak zoveel mogelijk gebruik van standaard encryptie programmatuur, zodat fouten worden voorkomen en voorkomen wordt dat de toepassing van encryptie een vals gevoel van veiligheid geeft (vindt het wiel niet opnieuw uit).
Stel eisen op het gebied van sleutelbeheer, sleutellengtes, toegepaste algoritmes (zie maatregel B5-1).

- Kwetsbaarheid: SQL-injectie.

Vereiste succescriteria (conformiteitvereisten)
De inrichting is gebaseerd op een vastgesteld inrichtingsdocument/ontwerp waarin is vastgelegd welke uitgangspunten gelden voor versleutelen van gegevens.

Classificatie
Hoog

Bewijsvoering
- In de ontwerp- c.q. configuratiedocumentatie is vastgelegd welke gegevens en hoe de gegevens worden versleuteld of gehashed.
- De zakelijke behoeften en beveiligingseisen. Rapportage van de risicoanalyse waarop de beslissing is gebaseerd.

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B5-4	Vertrouwelijkheid en onweerlegbaarheid	Versleutel cookies	9.3.3

Doelstelling
Voorkom dat kwaadwillende de inhoud van cookies kunnen inzien en/of aanpassen, zodat de vertrouwelijkheid en integriteit van de inhoud van cookies wordt gewaarborgd.

Rationale
Cookies bevatten doorgaans informatie over de sessie die een gebruiker heeft met een bepaalde webapplicatie en mogelijk ook authenticatiegegevens. Door tijdens het bezoek aan een webapplicatie continu het cookie aan de webapplicatie te tonen, weet de webapplicatie dat een gebruiker al geauthenticeerd is en dat dit niet opnieuw hoeft te gebeuren. Misbruik van informatie uit de cookies leidt ertoe dat kwaadwillenden zich ongeautoriseerd toegang verschaffen tot een webapplicatie. Een kwaadwillende kan dit doen door een cookie op te vangen (door het netwerkverkeer te sniffen) of door een achtergebleven cookie van een werkstation te halen (bijvoorbeeld in een internetcafé). Veel van deze problemen kunnen worden voorkomen door het cookie te versleutelen of door extra controles uit te voeren op cookies (zie maatregel B3-18). Een cookie moet versleuteld worden met een sleutel die alleen bekend is bij de webapplicatie. De gebruiker

(en ook de kwaadwillende) kan hierdoor vrijwel niets met het cookie (hij beschikt immers niet over de geheime sleutel) behalve dan dit cookie aan te bieden aan de webapplicatie. Een restrisico is dat een kwaadwillende zich op basis van het cookie toegang verschaft tot de webapplicatie (authentication replay). Om dit restrisico te verkleinen kan de webapplicatie werken met dynamische sleutels. Door bijvoorbeeld elke 2 minuten een nieuwe sleutel te generen, blijft het cookie op het werkstation ook maar 2 minuten geldig. Zolang de gebruiker ingelogd blijft op de webapplicatie , ontvangt deze elke 2 minuten een nieuw cookie. Op het moment dat een kwaadwillende een dergelijk cookie in handen krijgt, is de geldigheid van de sleutel naar alle waarschijnlijkheid al verlopen en kan deze niets meer met dit cookie beginnen.

Vereiste succescriteria (conformiteitvereisten)

- Er moet een beleid met betrekking tot het toepassen van cookies zijn.
- Er moeten procedures zijn met betrekking tot het beheren van cookies.
- De inrichting is gebaseerd op een vastgesteld inrichtingsdocument/ontwerp waarin is vastgelegd welke uitgangspunten gelden voor versleutelen van gegevens.

Classificatie

Hoog

Bewijsvoering

- Beleidsdocument
- Procedurebeschrijving

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B5-5	Vertrouwelijkheid en onweerlegbaarheid	Maak gebruik van digitale handtekeningen	9.3.4

Doelstelling

Voorkom dat transacties weerlegd kunnen worden.

Rationale

Als het noodzakelijk is dat transacties onweerlegbaar zijn, moet gebruik worden gemaakt van digitale handtekeningen. Bij een digitale handtekening maakt de ondertekenaar gebruik van het privédeel van een cryptografische sleutel.
Er bestaan verschillende mogelijkheden om een digitale handtekening te implementeren. Voor een belangrijk gedeelte is de technische oplossing ook afhankelijk van het gebruikte ‘transportprotocol’: XML of HTML. Voor XML bestaan standaarden waarmee een digitale handtekening op de inhoud van een bericht (of delen daarvan) kan worden geplaatst; XML Signature is een voorbeeld van een dergelijke standaard.
Er bestaan geen standaard mechanismen om gebruik te kunnen maken van digitale handtekeningen op HTML-gebaseerde webapplicaties. Er is een plug-in in de webbrowser nodig om functionaliteiten op het gebied van digitale handtekeningen te kunnen implementeren.

Wetgeving rondom het gebruik van digitale handtekeningen is in Nederland vastgelegd in de Wet Elektronische Handtekeningen (WEH)[50]. Deze wet beschrijft bijvoorbeeld aan welke voorwaarden een digitale handtekening moet voldoen om dezelfde rechtsgevolgen te kunnen hebben als een handgeschreven handtekening. Wanneer een organisatie besluit om gebruik te maken van een digitale handtekening voor de onweerlegbaarheid van transacties, moet het gebruikte mechanisme aan deze wet worden getoetst.

50. http://www.e-overheid.nl/e-overheid-2.0/live/binaries/e-overheid/juridisch/wet-elektronische-handtekening.pdf

Vereiste succescriteria (conformiteitvereisten)

- De inrichting is gebaseerd op een vastgesteld inrichtingsdocument/ontwerp waarin is vastgelegd welke uitgangspunten gelden voor het zetten van digitale handtekeningen.
- Het gebruikte mechanisme moet worden getoetst aan de Wet Elektronische Handtekeningen.

Classificatie

Midden

Bewijsvoering

- Resultaat van de toets ven het gebruikte mechanisme aan de Wet Elektronische Handtekeningen.

Relatie met andere normen en standaarden

- Programma van Eisen (PvE) van PKIOverheid[51]

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B5-6	Vertrouwelijkheid en onweerlegbaarheid	Zorg voor een extra set 'back-up' certificaten van een andere CA	

Doelstelling

Voorkom (langdurige) disruptie van de dienstverlening door risicospreiding.

Rationale

Zorg dat u een plan heeft voor een 'soepele' migratie. Vervang zo snel mogelijk de gecompromitteerde certificaten.
Overweeg de aanschaf van een extra set 'back-up' certificaten van een andere CA.
Mocht uw primaire certificaat leverancier gecompromitteerd worden, dan heeft u een snelle uitwijkmogelijkheid. Vooral het aanvragen van EV SSL certificaten kost tijd en gaat ten koste van een soepele migratie in geval van incidenten.

Zorg dat de reseller en zijn leverancier niet als primaire en secundaire CA wordt gekozen. In dit geval wordt twee keer hetzelfde certificaat gebruikt en is er uiteraard geen sprake van risicospreiding.

Vereiste succescriteria (conformiteitvereisten)

- De reseller en zijn leverancier zijn niet als primaire en secundaire CA gekozen.
- Migratieplan met betrekking tot het vervangen van certificaten.

Classificatie

Laag

Bewijsvoering

Migratieplan met betrekking tot het vervangen van certificaten.

Relatie met andere normen en standaarden

- Programma van Eisen (PvE) van PKIOverheid.

51. Dit programma is gebaseerd op Europese standaarden en Nederlandse wetgeving. Hiermee kunnen gebruikers er op vertrouwen dat zij gebruikmaken van een kwalitatief hoogwaardige en betrouwbare PKI-infrastructuur, die tevens voldoet aan internationaal geaccepteerde richtlijnen. <https://www.logius.nl/producten/toegang/pkioverheid/aansluiten/programma-van-eisen/>

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B5-7	Vertrouwelijkheid en onweerlegbaarheid	Tref maatregelen voor het patchen van systemen waarbij certificaten van de lijst met vertrouwde certificaten worden gehaald	

Doelstelling

Voorkom (langdurige) disruptie van de dienstverlening door risicospreiding.

Rationale

Zorg dat u een plan heeft voor een 'soepele' migratie.
Tref maatregelen voor het patchen van systemen waarbij certificaten van de lijst met vertrouwde certificaten worden gehaald. Dit kan betekenen dat deze patches worden uitgesteld als nog niet alle certificaten van de systemen vervangen zijn (zie ook maatregel B0-7).

Vereiste succescriteria (conformiteitvereisten)

- Migratieplan met betrekking tot het vervangen van certificaten
- zie maatregel B0-7

Classificatie

Laag

Bewijsvoering

- Migratieplan met betrekking tot het vervangen van certificaten
- zie maatregel B0-7

Relatie met andere normen en standaarden

- zie maatregel B0-7
- Programma van Eisen (PvE) van PKIOverheid

HOOFDSTUK 8

Beveiligingsintegratie

De beveiligingsintegratielaag is een laag die erop geënt is om samenwerking tussen verschillende componenten op het gebied van beveiliging mogelijk te maken. Deze samenwerking komt tot stand via interfaces op allerlei webapplicaties die zich bezighouden met beveiliging. Deze interfaces zoals firewalls, systemen voor toegangsbeheer en web application firewalls, vatten we in dit hoofdstuk samen onder de noemer beveiligingscomponent. Dit hoofdstuk gaat in op de manier waarop beveiligingsintegratie tussen webapplicaties en beveiligingscomponenten (en beveiligingscomponenten onderling) tot stand kan komen.

Beveiligingsintegratie houdt in dat een webapplicatie de beschikking krijgt over informatie die aanwezig is binnen de beveiligingscomponenten. Hierdoor kan een beveiligingsoplossing binnen een webapplicatie worden hergebruikt en hoeven ontwikkelaars de betreffende functionaliteit niet in elke webapplicatie afzonderlijk in te bouwen. Een voorbeeld hiervan is het scheiden van functionaliteiten op het gebied van autorisatie- en toegangsbeheer tussen de webapplicatie en generieke beveiligingscomponenten (zie hoofdstuk 6 'Identiteit- en toegangsbeheer').

Enkele voorbeelden van beveiligingsintegratie die voor het functioneren van een webapplicatie vereist kunnen zijn:

- Een webapplicatie wil de gebruikersnaam achterhalen van een gebruiker die door de (I&AM) tooling is geauthenticeerd.
- Een webapplicatie wil de rollen casu quo autorisaties achterhalen van een gebruiker die door de (I&AM) tooling is geauthenticeerd (en mogelijk geautoriseerd).
- De (I&AM) tooling wil de certificaatgegevens achterhalen van een SSL-sessie die de WAF met de eindgebruiker heeft.
- Een webapplicatie wil een load balancer opdracht geven geen verkeer meer naar een specifieke webserver te versturen (omdat er bijvoorbeeld onderhoud op deze webserver gaat plaatsvinden).

In hoofdlijnen bestaan er twee mechanismen om beveiligingsintegratie te bereiken: passief en actief.

- **Passief**
  Passieve beveiligingsintegratie betekent dat een beveiligingscomponent bepaalde informatie bij voorbaat aanbiedt aan de achterliggende webapplicatie, zonder dat de webapplicatie hier specifiek om vraagt. De webapplicatie hoeft deze informatie niet te gebruiken.
  Bij passieve beveiligingsintegratie doorlopen gebruikers, beveiligingscomponent en webapplicatie altijd de volgende drie stappen:
  1. De gebruiker maakt contact met het beveiligingscomponent.
  2. De beveiligingscomponent voert zijn beveiligingsacties uit.
  3. De beveiligingscomponent stelt de resultaten van deze beveiligingsactie beschikbaar aan achterliggende componenten. De mogelijkheid bestaat dat achterliggende componenten geen gebruik maken van deze informatie.

- **Actief**
  Actieve beveiligingsintegratie houdt in dat de webapplicatie actief contact legt met de beveiligingscomponent om informatie op te vragen of opdrachten te geven.
  Bij actieve beveiligingsintegratie bevraagt een webapplicatie actief een beveiligings-component om informatie over uitgevoerde beveiligingsacties te achterhalen óf om een nieuwe beveiligingsactie uit te laten voeren. Bij actieve beveiligingsintegratie hoeft de beveiligingscomponent dus niet inline (dat wil zeggen tussen de client en achterliggende webapplicatie) geplaatst te zijn.

8.1 Doelstelling

Zorgen dat een omgeving ontstaat van nauw verwante (netwerk) componenten die moeiteloos met elkaar kunnen communiceren

8.2 Beveiligingsrichtlijnen

Met de invoer van elk nieuw beveiligingscomponent moet de volgende vraag worden gesteld:
hoe integreer ik deze component binnen mijn omgeving?
Belangrijk is vast te stellen:

- Welke services de omgeving van de component zal afnemen.
- Op welke manier de omgeving deze services zal afnemen (actief of passief, welke protocollen).

De vereisten die uit deze overwegingen naar voren komen, dienen vervolgens als input voor een productselectie. Door bij elk nieuw of te vervangen beveiligingscomponent deze vereisten in ogenschouw te nemen, ontstaat een omgeving van nauw verwante componenten die moeiteloos met elkaar kunnen communiceren.

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B6-1	Beveiligingsintegratie	Stel vast welke beveiligingsservices een component zal afnemen en aanbieden	10.3

Doelstelling

Zorgen voor een effectieve integratie van verschillende (netwerk) componenten.

Rationale

Beveiligingsintegratie houdt in dat een webapplicatie de beschikking krijgt over informatie die aanwezig is binnen de beveiligingscomponenten. Hierdoor kan een beveiligingsoplossing binnen een webapplicatie worden hergebruikt en hoeven ontwikkelaars de betreffende functionaliteit niet in elke webapplicatie afzonderlijk in te bouwen.
Hieronder een overzicht van de verschillende manieren waarop een beveiligings-component informatie beschikbaar kan stellen aan de achterliggende webservers:

- Opslaan van gegevens in een tussenliggende datastore.
  Hierbij plaatst de beveiligingscomponent beveiligingsgegevens in een database. Achterliggende applicaties die deze gegevens willen gebruiken, kunnen de gegevens vervolgens weer uit de database halen. In feite is deze manier van beveiligingsintegratie een combinatie van passieve integratie (beveiligingscomponent plaatst de gegevens altijd in de database) en actieve integratie (de achterliggende applicatie moet de gegevens zelf weer actief uit de database halen).
- Doorgeven van waarden via een querystring.
  Bij deze oplossing plakt de beveiligingscomponent belangrijke gegevens achter de gebruikte URL in de vorm van een querystring. De achterliggende applicatie kan vervolgens de gegevens uit de querystring gebruiken.
- Doorgeven van waarden via HTTP-headers.
  De informatie die de beveiligingscomponent wil aanbieden, kan de component ook meesturen via HTTP-headers. De achterliggende applicatie kan besluiten om de gegevens uit deze headers te gebruiken.

Met de invoer van elk nieuw beveiligingscomponent dient men zich af te vragen:
hoe integreer ik deze component binnen mijn omgeving?
Belangrijk is vast te stellen:

- Welke services de omgeving van de component zal afnemen.
- Op welke manier de omgeving deze services zal afnemen (actief of passief, welke protocollen).

De vereisten die uit deze overwegingen naar voren komen, dienen vervolgens als input voor een productselectie. Door bij elk nieuw of te vervangen beveiligingscomponent deze vereisten in ogenschouw te nemen, ontstaat een omgeving van nauw verwante componenten die moeiteloos met elkaar kunnen communiceren.

Vereiste succescriteria (conformiteitvereisten)

Programma van eisen met betrekking tot de productselectie. Hierin moeten de volgende vragen worden beantwoord:

- Welke services worden door de component afgenomen?
- Op welke manier de omgeving deze services zal afnemen?

Classificatie

Midden

Bewijsvoering

Programma van eisen.

HOOFDSTUK 9

Monitoring, auditing en alerting

Monitoring, auditing en alerting zijn van toepassing op elke laag van het RBW. Voor zowel monitoring, auditing als alerting geldt dat de verschillende technologieën die zich binnen de RBW-lagen bevinden, informatie aanleveren die monitoring, auditing en alerting mogelijk maken. Heel belangrijk is dat ze niet los op elke laag beschouwd worden, maar dat (causale) verbanden kunnen worden gelegd tussen de afzonderlijke logging- en monitoringmechanismen. Dit soort denken is vooral van belang door de steeds verder voortschrijdende ketenintegratie, waarbij componenten aan elkaar gekoppeld worden en de sterkte en het functioneren van de keten bepaald worden door de zwakste schakel.

Bij een aanval op een webapplicatie binnen het RBW, moet de gelogde gebeurtenissen op de verschillende lagen van het RBW worden gecombineerd om zodoende een duidelijk aanvalspatroon (met bijbehorend bewijsmateriaal) te kunnen verzamelen. Complicerende factor daarbij is dat de functionaliteiten uit de verschillende lagen van het RBW verdeeld kunnen zijn over diverse ketencomponenten. Door gebeurtenissen op verschillende lagen van het RBW en verschillende ketencomponenten te combineren, kan worden bepaald welke actie op een specifiek tijdstip werd uitgevoerd (applicatiebeveiliging), wie deze actie uitvoerde (identiteitbeheer) en vanaf welke plek deze actie afkomstig was (netwerkbeveiliging).

Voor monitoring geldt eenzelfde soort redenering. Hoewel het hierbij belangrijk is dat afzonderlijke componenten worden gemonitord, is het tevens relevant om de verschillende componenten in een 'monitoringketen' te plaatsen. Op het moment dat één component uit de keten niet meer goed blijkt te functioneren, heeft dit gevolgen voor de hele keten en moet dit ook als zodanig worden opgemerkt. Dat betekent dat bij een verstoring de impact voor de hele keten wordt vastgesteld. Stel bijvoorbeeld dat een webapplicatie beschermd is door een WAF. Uit de afzonderlijke monitoring van de WAF en webapplicatie komt naar voren dat beiden goed functioneren. Echter, wanneer de webapplicatie via de WAF wordt benaderd, blijkt dit niet te werken door een probleem in de WAF. Een dergelijk probleem is alleen op te merken als de keten aan componenten wordt gemonitoord en niet alleen de afzonderlijke systemen.

9.1 Kwetsbaarheden en bedreigingen

Deze paragraaf beschrijft kwetsbaarheden en bedreigingen die op het gebied van monitoring, auditing en alerting te onderscheiden zijn.

Mogelijke kwetsbaarheden en bedreigingen zijn:

Nr.	Beveiligingslaag	Kwetsbaarheid	Referentie RBW
K7-1	Monitoring, auditing en alerting	Ontbreken van toezicht	11.1.1

Toelichting

Als een kwaadwillende een webapplicatie - of de infrastructuur hieromheen - aanvalt, kan dit kwalijke gevolgen hebben. Een organisatie kan alleen passende maatregelen nemen en de schade tot een minimum beperken, als de juiste mechanismen zijn ingezet voor het detecteren van aanvallen en deze mechanismen bovendien correct zijn geconfigureerd. Het kan hieraan ontbreken om de volgende redenen:

- Er is überhaupt geen monitoring van netwerkverkeer.
- De monitoringcomponenten leveren zoveel informatie dat de belangrijke aanvallen niet meer te onderscheiden zijn van de vele 'script kiddie'-aanvallen; men ziet met andere woorden door de bomen het bos niet meer.
- De monitoringcomponenten verzamelen wel continu data, maar er is geen medewerker beschikbaar om deze te analyseren.
- De monitoringcomponenten verzamelen wel continu data, maar de gebeurtenissen van deze componenten zijn op geen enkele manier aan elkaar te koppelen doordat de tijdstippen op de componenten uit elkaar lopen.

Het ontbreken van dit toezicht kan ertoe leiden dat kwaadwillenden misbruik maken van webapplicaties zonder dat dit wordt gedetecteerd.

Nr.	Beveiligingslaag	Kwetsbaarheid	Referentie RBW
K7-2	Monitoring, auditing en alerting	Impact: onbekend	11.1.2

Toelichting
Wanneer een component een losstaande gebeurtenis rapporteert, helpt dit in het bepalen van de technische impact: de component is bijvoorbeeld tijdelijk niet meer beschikbaar of de performance is tijdelijk verminderd. Maar wat betekent dit nu voor de gehele keten? Merkt een gebruiker niets van deze storing of leidt de storing tot een zeer ernstige onderbreking van de service aan de eindgebruiker? Om de impact van een gebeurtenis te kunnen bepalen, is het belangrijk om de gebeurtenis in een groter geheel (de keten) te bekijken. De beschouwing van de omgeving als een keten van nauw samenwerkende componenten is in dit geval de enige juiste. Op basis van dit inzicht kan worden ingeschat wat de risico's zijn en welke maatregelen moeten worden genomen.

Nr.	Beveiligingslaag	Kwetsbaarheid	Referentie RBW
K7-3	Monitoring, auditing en alerting	Gebrek aan coördinatie en samenwerking	11.1.3

Toelichting
De componenten die logging genereren vallen vaak onder verschillende teams binnen een organisatie. Een netwerkbeheerteam beheert de netwerkcomponenten, een applicatiebeheerteam de webapplicaties en een autorisatiebeheerteam de autorisaties. Het analyseren van complexe gebeurtenissen vereist dat deze verschillende teams nauw met elkaar samenwerken. Gebrek aan samenwerking en coördinatie leidt ertoe dat een complexe gebeurtenis niet volledig geanalyseerd wordt.

9.2 Doelstelling

Het ontdekken van ongeautoriseerde activiteiten.

9.3 Beveiligingsrichtlijnen

Deze paragraaf besteedt aandacht aan maatregelen die gesteld worden op het gebied van monitoring, auditing en alerting.

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B7-1	Monitoring, auditing en alerting	Maak gebruik van Intrusion Detection Systemen (IDS)	11.2.1

Doelstelling
Detecteren van aanvallen op webapplicaties.

Rationale
Intrusion Detection Systemen (IDS) helpen bij het detecteren van aanvallen op webapplicaties. IDS'en monitoren continu het verkeer dat zich door de DMZ-compartimenten verplaatst en kunnen, veelal op basis van aanvalspatronen, misbruik van webapplicaties en andere infrastructuurcomponenten detecteren. De volgende soorten IDS'en worden onderkend:

- Network-based Intrusion Detection System (NIDS). Een NIDS wordt als losstaand component in het netwerk geplaatst waarna deze component netwerkverkeer opvangt.

- Host-based Intrusion Detection System (HIDS). Een HIDS wordt op een server geïnstalleerd waarna het HIDS continu de activiteiten op deze server monitort. Het HIDS kijkt hierbij niet alleen naar het netwerkverkeer (zoals het NIDS) maar ook naar logging en veranderingen op het systeem zelf.
- Application-based IDS (APIDS). Een application-based IDS wordt specifiek ingezet voor het monitoren van misbruik van een specifieke webapplicatie of een specifiek protocol.

Het detecteren van aanvallen gebeurt veelal op basis van bekende aanvalspatronen. Deze manier van detectie, op basis van 'handtekeningen' van bekende aanvallen, wordt ook wel signature-based genoemd. Tegenover de signature-based IDS'en staan de anomaly-based systemen. Deze systemen werken niet op basis van handtekeningen, maar op basis van afwijkingen (anomalieën).
Bij het inrichten van een NIDS is het belangrijk goed te bekijken welke meetpunten interessant zijn voor het NIDS om op die manier een zo compleet mogelijk beeld te krijgen van aanvallen op de omgeving. Bekijk daarbij aan de hand van de DMZ-opbouw (zie maatregel B1-1) en de compartimentering (zie maatregel B1-2) in het algemeen wat interessante meetpunten zijn.

Om kwalitatief hoogwaardige informatie te verzamelen en deze effectief te verwerken, is het belangrijk om aandacht te schenken aan de volgende zaken:
- Voorzie signature-based systemen regelmatig van de nieuwste aanvalspatronen.
- Zorg ervoor dat databases voldoende ruimte bieden om de grote hoeveelheid gegevens die een NIDS produceert, in onder te kunnen onderbrengen.
- Beslis hoelang logging moet worden opgeslagen en hoe deze moet worden gearchiveerd.
- Tune de alarmering van het NIDS. Beheerders zullen een NIDS dat continu alarmen uitzendt, niet meer serieus nemen. Onderschat daarbij de hoeveelheid mankracht die nodig is voor het monitoren en onderzoeken van anomalieën en false positives niet. Het kan een zeer intensieve klus blijken te zijn om de filters van het IDS optimaal in te richten.

Eisen aan loginformatie
Regel een goede beheerprocedure in voor het IDS. Leg bijvoorbeeld vast wie regelmatig (bijvoorbeeld elke ochtend) de logging van het IDS bekijkt. Daarnaast is het, ter verbetering van de leesbaarheid van de logging, aan te raden filters op de logging te plaatsen.

Opvolging
Er moet actie worden ondernomen indien log records op kwaadwillend misbruik duiden, geïmplementeerde maatregelen niet voldoen aan de gestelde eisen en/of verwachtingen of tekortkomingen opleveren.

Vereiste succescriteria (conformiteitvereisten)
- De inrichting is gebaseerd op een vastgesteld inrichtingsdocument / ontwerp waarin is vastgelegd welke uitgangspunten gelden voor inzetten van IDS'en.
- Er moet aantoonbaar follow-up worden gegeven in casu verbeteringen worden doorgevoerd indien log records op kwaadwillend misbruik duiden, geïmplementeerde maatregelen niet voldoen aan de gestelde eisen en/of verwachtingen of tekortkomingen opleveren.

Classificatie
Hoog

Bewijsvoering

- In de ontwerp- c.q. configuratie documentatie is vastgelegd waar en hoe IDS'en worden ingezet.
- De zakelijke behoeften en maatregelen. Rapportage van de risicoanalyse waarop de beslissing is gebaseerd.
- Plan met daarin de activiteiten die worden uitgevoerd (wie, wat en wanneer) indien log records op kwaadwillend misbruik, duiden geïmplementeerde maatregelen niet aan de gestelde eisen en/of verwachtingen hebben voldaan of tekortkomingen hebben opgeleverd.

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B7-2	Monitoring, auditing en alerting	Breng logging op één punt samen	11.2.2

Doelstelling

Het efficiënt detecteren van aanvallen.

Rationale

Vaak worden verschillende loggingmechanismen naast elkaar gebruikt. Zo ondersteunt het ene systeem alleen logging op basis van SYSLOG, maakt een ander systeem alleen lokaal logbestanden aan en stelt weer een ander systeem alleen informatie beschikbaar via SNMP. Al deze verschillende loggingmechanismen zorgen ervoor dat logging versnipperd raakt en een organisatie het overzicht over alle gebeurtenissen gemakkelijk kwijtraakt. Om aanvallen efficiënt te kunnen detecteren is het van belang deze logging op één centraal punt weer bijeen te brengen. Beperk het aantal loggingmechanismen zoveel mogelijk. Door de logging op een centraal punt bijeen te brengen en filtering toe te passen op deze logging ontstaat een heldere blik op alle informatie vanuit de verschillende componenten uit de infrastructuur.

In een centrale loggingdatabase komt de loginformatie uit verschillende onderdelen van het RBW samen. Denk hierbij aan de volgende typen informatie: logging op het niveau van netwerk-, platform- en webapplicatiebeveiliging; logging op het niveau van identiteit- en autorisatiebeheer (zie paragraaf 10.10 'Controle' in NEN-ISO /IEC 27002 'Code voor informatiebeveiliging'); en logging op het niveau van vertrouwelijkheid en onweerlegbaarheid.

De centraal opgeslagen informatie is zeer interessant voor kwaadwillenden aangezien ze 1) veel kunnen leren over de opbouw van de infrastructuur en 2) ze via deze centrale plek eventuele sporen van misbruik kunnen wissen. Daarom is het van belang veel aandacht te besteden aan de beveiliging van deze centrale database, zodat onbevoegden hiertoe geen toegang hebben en hierin geen wijzigingen kunnen aanbrengen.

Een andere mogelijke beveiligingsmaatregel in dit kader kan ook zijn om logbestanden digitaal te ondertekenen.

Eisen aan loginformatie

- Bepaal welke gebeurtenissen worden gelogd en onderhoud deze regels.
- Onderhoud kennis van correlaties die op misbruik duiden.
- Daarnaast is het, ter verbetering van de leesbaarheid van de logging, aan te raden filters op de logging te plaatsen.
- Voorkom dat het herkennen van verdachte patronen in de logging afhangt van de kunde van de operationeel beheerder.

Opvolging

Er moet actie worden ondernomen indien log records op kwaadwillend misbruik duiden, geïmplementeerde maatregelen niet voldoen aan de gestelde eisen en/of verwachtingen of tekortkomingen opleveren.

Vereiste succescriteria (conformiteitvereisten)

- De inrichting is gebaseerd op een vastgesteld inrichtingsdocument / ontwerp waarin is vastgelegd welke uitgangspunten gelden voor logging.
- Er moet aantoonbaar follow-up worden gegeven in casu verbeteringen worden doorgevoerd indien log records op kwaadwillend misbruik duiden, geïmplementeerde maatregelen niet voldoen aan de gestelde eisen en/of verwachtingen of tekortkomingen opleveren.

Classificatie

Midden

Bewijsvoering

- In de ontwerp- c.q. configuratie documentatie is vastgelegd waar en hoe logging ingezet.
- Configuratieinstellingen.
- Plan met daarin de activiteiten die worden uitgevoerd (wie, wat en wanneer) indien log records op kwaadwillend misbruik duiden, geïmplementeerde maatregelen niet aan de gestelde eisen en/of verwachtingen hebben voldaan of tekortkomingen hebben opgeleverd.

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B7-3	Monitoring, auditing en alerting	Breng correlaties aan	11.2.3

Doelstelling

Het efficiënt detecteren van aanvallen.

Rationale

Nadat alle logginginformatie over webapplicaties bijeen gebracht is (zie maatregel B7-2), is de volgende stap het aanbrengen van correlaties tussen de verschillende gebeurtenissen. De uitdaging hierbij is om alle gebeurtenissen op de verschillende niveaus aan elkaar te correleren en aan een specifieke webapplicatie te koppelen. Op deze manier kun je het pad dat een kwaadwillende heeft doorlopen, achterhalen en tevens inzicht krijgen in de aanvallen die gedurende een bepaalde periode op een webapplicatie zijn uitgevoerd.
Een goed ingerichte Configuration Management Database (CMDB), waarin componenten en de afhankelijkheden daartussen zijn gedefinieerd, kan het leggen van correlaties voor een belangrijk gedeelte vereenvoudigen.

Eisen aan loginformatie

- Bepaal welke gebeurtenissen worden gelogd en onderhoud deze regels.
- Onderhoud kennis van correlaties die op misbruik duiden.
- Daarnaast is het, ter verbetering van de leesbaarheid van de logging, aan te raden filters op de logging te plaatsen.
- Voorkom dat het herkennen van verdachte patronen in de logging afhangt van de kunde van de operationeel beheerder.

Opvolging

Er moet actie worden ondernomen indien log records op kwaadwillend misbruik duiden, geïmplementeerde maatregelen niet voldoen aan de gestelde eisen en/of verwachtingen of tekortkomingen opleveren.

Vereiste succescriteria (conformiteitvereisten)

- De inrichting is gebaseerd op een vastgesteld inrichtingsdocument / ontwerp waarin is vastgelegd welke uitgangspunten gelden voor logging en het aanbrengen van correlaties.
- De logging dient actief beoordeeld te worden.
- Er moet aantoonbaar follow-up worden gegeven in casu verbeteringen worden doorgevoerd indien log records op kwaadwillend misbruik duiden, geïmplementeerde maatregelen niet voldoen aan de gestelde eisen en/of verwachtingen of tekortkomingen opleveren.

Classificatie

Midden

Bewijsvoering

- In de ontwerp- c.q. configuratie documentatie is vastgelegd waar en hoe correlaties worden aangebracht.
- Configuratieinstellingen.
- Plan met daarin de activiteiten die worden uitgevoerd (wie, wat en wanneer) indien log records op kwaadwillend misbruik duiden, geïmplementeerde maatregelen niet aan de gestelde eisen en/of verwachtingen hebben voldaan of tekortkomingen hebben opgeleverd.

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B7-4	Monitoring, auditing en alerting	Synchroniseer de systeemklokken	11.2.4

Doelstelling

Het efficiënt detecteren van aanvallen.

Rationale

Om gebeurtenissen uit verschillende componenten te correleren worden de timestamps van deze gebeurtenissen gebruikt. Deze timestamps zijn afhankelijk van de juiste instelling van de tijd op de betreffende componenten. Met behulp van het Network Time Protocol (NTP) kan worden bereikt dat de tijd op alle servers en andere componenten overeen komt (zie paragraaf 10.10.6 ‘Synchronisatie van systeemklokken’ in NEN-ISO /IEC 27002 ‘Code voor informatiebeveiliging’).

Vereiste succescriteria (conformiteitvereisten)

De inrichting is gebaseerd op een vastgesteld inrichtingsdocument/ontwerp waarin is vastgelegd hoe het synchroniseren van de systeemklokken is geconfigureerd.

Classificatie

Hoog

Bewijsvoering

- In de ontwerp- c.q. configuratie documentatie is vastgelegd hoe het synchroniseren van de systeemklokken is geconfigureerd.
- Configuratieinstellingen.

Relatie met andere normen en standaarden

- NEN-ISO /IEC 27002 ‘Code voor informatiebeveiliging’
  - paragraaf 10.10.6 Synchronisatie van systeemklokken

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B7-5	Monitoring, auditing en alerting	Bepaal wat te doen bij het uitvallen van loggingmechanismen	11.2.6

Doelstelling

Voorkom onopgemerkte aanvallen.

Rationale

Het gebruik van centrale loggingmechanismen brengt een belangrijk vraagstuk met zich mee: wat doen we op het moment dat dit centrale loggingmechanisme uitvalt? Op het moment dat een component zijn logging niet meer kwijt kan, bestaat de kans dat deze logging verloren gaat. Dit zou kunnen betekenen dat componenten aanvallen van kwaadwillenden niet meer registreren, of dat transacties niet meer onweerlegbaar zijn.

Bepaal daarom op voorhand welke actie een component moet nemen op het moment dat het centrale loggingmechanisme niet meer beschikbaar is. Er bestaan op dit gebied grofweg de volgende mogelijke acties:

- De component normaal laten functioneren terwijl deze de logging niet kan opslaan. Dit betekent dat logging verloren gaat.
- De component normaal laten functioneren en de logging lokaal laten opslaan. Veel componenten beschikken over een lokaal mechanisme om logging tijdelijk op te slaan. Op het moment dat het centrale loggingmechanisme weer beschikbaar komt, sluist de component de verzamelde logging alsnog door. Dit voorkomt dat de component niet meer beschikbaar is en voorkomt tevens dat logging verloren gaat. Dit is echter wel een tijdelijke oplossing. Op het moment dat de lokale opslag vol loopt, moet opnieuw besloten worden wat de component hierna doet (blijven functioneren - zie bovenstaande optie - of stoppen met functioneren - zie volgende optie).
- De component acuut laten stoppen met functioneren. Dit betekent dat gebruikers hoogst waarschijnlijk niet meer kunnen doorwerken. Dit voorkomt wel dat aanvallen op de component onopgemerkt blijven doordat de component ze niet meer logt.

Vanuit het oogpunt van beveiliging en beschikbaarheid heeft het de voorkeur om - zodra het centrale loggingmechanisme uitvalt - componenten eerst lokaal gebeurtenissen te laten opslaan om vervolgens de component te laten stoppen met functioneren zodra deze opslag vol is. Bij de selectie van een nieuw beveiligingscomponent is het daarom zaak goed te evalueren of deze voldoet aan de eisen op het gebied van logging en tijdelijke opslag van logging.

Vereiste succescriteria (conformiteitvereisten)

Er moeten eisen op het gebied van logging zijn vastgesteld. Denk hierbij aan:

- Hoe is de logging met betrekking tot webapplicaties ingericht?
- Welke actie moet een component nemen op het moment dat het centrale loggingmechanisme niet meer beschikbaar is?

Classificatie

Hoog

Bewijsvoering

Procedurebeschrijving van het logmechanisme en bewijsvoering dat dit mechanisme ook daadwerkelijk werkt.

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B7-6	Monitoring, auditing en alerting	Stel bewaartermijnen van logging vast	11.2.7

Doelstelling
Vaststellen van een bewaartermijn voor essentiële (bedrijfs)informatie.

Rationale
Er moet worden bepaald hoe lang logging online en offline beschikbaar moet en mag zijn. Online beschikbaarheid van logging kan essentieel zijn voor het efficiënt verhelpen van beveiligingsincidenten. De duur van offline beschikbaarheid kan beperkt worden door wet- en regelgeving. Voordat wordt besloten om gebeurtenissen in een omgeving te loggen, moet zijn vastgesteld hoe lang en op welke manier logging beschikbaar moet blijven. Dit bepaald welke media nodig zijn en hoeveel capaciteit je voor de logging moet reserveren. Het systeem, waarmee gegevens opgeslagen en behandeld worden, dient dusdanig te zijn dat de gegevens duidelijk geïdentificeerd kunnen worden gedurende hun wettelijke of reglementaire bewaartermijn. De gegevens dienen op een passende wijze vernietigd te kunnen worden na afloop van die termijn voorzover ze niet meer nodig zijn voor de organisatie.
In sommige gevallen is de bewaartermijn voor informatie en het type informatie dat bewaard moet worden geregeld in de nationale wetgeving of voorschriften.
Deze beveiligingseis is tevens essentieel bij reconstructie vraagstukken in relatie tot opgetreden issues/incidenten.

Vereiste succescriteria (conformiteitvereisten)
- Er moeten bewaartermijnen zijn vastgesteld voor de loginformatie.

Classificatie
Hoog

Bewijsvoering
- Configuratieinstellingen.

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B7-7	Monitoring, auditing en alerting	Beveilig logging tegen achteraf wijzigen	

Doelstelling
Voorkom dat logfiles achteraf aangepast kunnen worden.

Rationale
Om te voorkomen dat kwaadwillende sporen uitwissen moeten logfiles zo zijn ingesteld dat deze achteraf niet kunnen worden aangepast. Deze beveiligingseis is essentieel bij reconstructie vraagstukken in relatie tot opgetreden issues/incidenten.

Vereiste succescriteria (conformiteitvereisten)
- De logfiles moeten tegen wijzigen zijn beveiligd.

Classificatie
Hoog

Bewijsvoering
- Configuratieinstellingen.

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B7-8	Monitoring, auditing en alerting	Voer actief controles uit op logging	11.2.8

Doelstelling
Het detecteren van misbruik en inbraakpogingen.

Rationale
Er moeten (pro)actieve controles uitgevoerd worden op de verzamelde logging (denk hierbij aan applicatie-, database-, host- en netwerklogging), zodat misbruik van de omgeving en inbraakpogingen detecteren. De verantwoordelijke moet ondersteund worden door een deugdelijke filtering op de logging. Alleen bij een deugdelijke filtering is het mogelijk om aanvallen te detecteren uit de grote hoeveelheid logging die verschillende componenten op een dag zullen genereren. Filtering van de logging zal dynamisch zijn; door het filter continu aan te passen, ontstaat een behapbaar en bruikbaar overzicht van gebeurtenissen die zich in de omgeving hebben voorgedaan.
Deze beveiligingseis is tevens essentieel bij reconstructie vraagstukken in relatie tot opgetreden issues/incidenten.

Opvolging
Er moet actie worden ondernomen indien log records op kwaadwillend misbruik duiden, geïmplementeerde maatregelen niet voldoen aan de gestelde eisen en/of verwachtingen of tekortkomingen opleveren.

Vereiste succescriteria (conformiteitvereisten)
- Er moeten procedures zijn opgesteld, waarin staat beschreven hoe en wanneer controles op logging moeten plaatsvinden en hoe taken op dit gebied belegd zijn.
- Er moet aantoonbaar follow-up worden gegeven in casu verbeteringen worden doorgevoerd indien log records op kwaadwillend misbruik duiden, geïmplementeerde maatregelen niet voldoen aan de gestelde eisen en/of verwachtingen of tekortkomingen opleveren.

Classificatie
Hoog

Bewijsvoering
- Procedurebeschrijving met daarin beschreven hoe en wanneer controles op logging moeten plaatsvinden en hoe taken op dit gebied belegd zijn.
- Plan met daarin de activiteiten die worden uitgevoerd (wie, wat en wanneer) indien log records op kwaadwillend misbruik duiden, geïmplementeerde maatregelen niet aan de gestelde eisen en/of verwachtingen hebben voldaan of tekortkomingen hebben opgeleverd.

Nr.	Beveiligingslaag	Beschrijving van beveiligingsrichtlijn	Referentie RBW
B7-9	Monitoring, auditing en alerting	Governance, organisatie, rollen en bevoegdheden inzake preventie, detectie en response inzake informatiebeveiliging dienen adequaat te zijn vastgesteld	11.2.9

Doelstelling
Het managen van de informatiebeveiliging binnen de organisatie.

Rationale
Bij het samenbrengen van logging moeten verschillende disciplines bijeenkomen, zodat op verschillende beveiligingslagen informatie over een aanval is terug te zoeken. Ook bij onduidelijkheden rondom gebeurtenissen moeten verschillende disciplines elkaar snel weten te vinden, om op die manier problemen te verhelpen. Hoe een organisatie een dergelijke samenwerking kan bevorderen, is zeer afhankelijk van de organisatiestructuur.

Opvolging
Er moet actie worden ondernomen indien log records op kwaadwillend misbruik duiden, geïmplementeerde maatregelen niet voldoen aan de gestelde eisen en/of verwachtingen of tekortkomingen opleveren.

Vereiste succescriteria (conformiteitvereisten)
- Functies en verantwoordelijkheden voor de informatiebeveiliging moeten zijn toegekend.
- Er moet overeenstemming over de benodigde methodologieën en processen worden bereikt. Denk hierbij aan risicoanalyse en met betrekking tot het classificatiesysteem.
- Er moet aantoonbaar follow-up worden gegeven in casu verbeteringen worden doorgevoerd indien log records op kwaadwillend misbruik duiden, geïmplementeerde maatregelen niet voldoen aan de gestelde eisen en/of verwachtingen of tekortkomingen opleveren.

Classificatie
Hoog

Bewijsvoering
- Procedurebeschrijving hoe functies en verantwoordelijkheden voor de beveiliging worden toegewezen.
- Overzicht welke functies en verantwoordelijkheden aan wie zijn toegekend.
- Plan met daarin de activiteiten die worden uitgevoerd (wie, wat en wanneer) indien log records op kwaadwillend misbruik duiden, geïmplementeerde maatregelen niet aan de gestelde eisen en/of verwachtingen hebben voldaan of tekortkomingen hebben opgeleverd.

Relatie met andere normen en standaarden
- NEN-ISO /IEC 27002 ‘Code voor informatiebeveiliging’
  - hoofdstuk 6 ‘Organisatie van informatiebeveiliging’

HOOFDSTUK 10

Informatie-beveiligingsbeleid

Het informatiebeveiligingsbeleid is leidend voor de invulling van de verschillende andere onderdelen van het raamwerk en deze Richtlijn. Dit informatiebeveiligingsbeleid wordt in deze Richtlijn niet verder behandeld. Hiervoor wordt verwezen naar hoofdstuk 5 ‘Beveiligingsbeleid’ in de NEN-ISO /IEC 27002 ‘Code voor informatiebeveiliging’.

Bijlagen

Afkortingen

A	
ACL	Access Control List
AD	Active Directory
Ajax	Asynchronous JavaScript and XML
API	Application Programming Interface
APIDS	Application-based Intrusion Detection System
B	
BGP	Border Gateway Protocol
BREIN	Bescherming Rechten Entertainment Industrie Nederland
BSN	Burgerservicenummer
C	
CA	Certification Authority
CAB	Change Advisory Board
CDP	Cisco Discovery Protocol
CMDB	Configuration Management Database
CMS	Content Management System
CPU	Central Processing Unit
CSRF	Cross-Site Request Forgery
CSS	Cascading Style Sheet
D	
DAC	Discretionary Access Control
DBA	Database Administrator
(D)DoS	(Distributed) Denial-of-Service
DMZ	Demilitarised Zone
DN	Distinguished Name
DNO	Diensten Niveau Overeenkomst
DNS	Domain Name Services
DNSSEC	DNS Security Extensions
DOM	Document Object Model
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
GOVCERT.NL	Government Computer Emergency Response Team Nederland
GPO	Group Policy Object
GSLB	Global Server Load Balancing
H	
HIDS	Host-based Intrusion Detection System
HTML	Hypertext Markup Language
HTTP(S)	Hypertext Transfer Protocol (Secure)
I	
I&AM	Identity and Access Management
IANA	Internet Assigned Numbers Authority
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
K	-
L	
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LSLB	Local Server Load Balancing
M	
MAC	Mandatory Access Control 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 Standards
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	
PFW	Perimeter Firewall
PHP	PHP: Hypertext Preprocessor
PKI	Public Key Infrastructure
PL/SQL	Procedural Language/Structured Query Language
PVIB	Platform voor InformatieBeveiliging
Q	-
R	
RBW	Raamwerk Beveiliging Webapplicaties
RDP	Remote Desktop Protocol
REST	Representational State Transfer
RFC	Request For Comments Request for Change
RFI	Remote File Inclusion
RP	Reverse Proxy
RSS	Really Simple Syndication (RSS 2.0) Rich Site Summary (RSS 0.91 en RSS 1.0) RDF Site Summary (RSS 0.9 en 1.0)
S	
SaaS	Software-as-a-Service
SaBeWa	Samenwerking Belastingen en Waardebepaling
SAML	Security Assertion Markup Language
SANS	SysAdmin, Audit, Network, Security
SCP	Secure Copy
SFTP	SSH File Transfer Protocol
SIRT	Security Incident Response Team
SLA	Service Level Agreement
SMTP	Simple Mail Transfer Protocol
SN	Serial Number
SNMP	Simple Network Management Protocol
SPOF	Single Point-of-Failure
SQL	Structured Query Language
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
WebDAV	Web-based Distributed Authoring and Versioning
WEH	Wet Elektronische Handtekeningen
WSDL	Web Service Description Language
WSUS	Windows Server Update Services
X	
XML	eXtensible Markup Language
XSRF	Zie CSRF
XSS	Cross-Site Scripting
Y	-
Y	-

Literatuurlijst

Nr.	Omschrijving
[1]	**OWASP Top 10 Application Security Risks – 2010** **https://www.owasp.org/index.php/Top_10_2010-Main**
[2]	**OWASP Testing Guide v3, d.d. 2 november 2008** https://www.owasp.org/index.php/OWASP_Testing_Guide_v3_Table_of_Contents
[3]	**OWASP Code Review Guide** https://www.owasp.org/index.php/OWASP_Code_Review_Guide_Table_of_Contents
[4]	**OWASP Application Security Verification Standard (ASVS)** http://code.google.com/p/owasp-asvs/wiki/ASVS
[5]	**NEN-ISO/IEC 27001 'Managementsystemen voor informatiebeveiliging'** http://www.nen.nl/web/Normshop/Norm/NENISOIEC-270012005-nl.htm
[6]	**NEN-ISO/IEC 27002 'Code voor informatiebeveiliging'** http://www.nen.nl/web/Normshop/Norm/NENISOIEC-270022007-nl.htm
[7]	**NEN-ISO/IEC 27005 'Information security risk management'** http://www.nen.nl/web/Normshop/Norm/NENISOIEC-270052011-en.htm
[8]	**Basisnormen Beveiliging en Beheer ICT-infrastructuur** Deze norm is uitgegeven door het Platform voor InformatieBeveiliging (PVIB) in 2003, ISBN 90-5931-228-7.
[9]	**NORA Dossier Informatiebeveiliging, versie 1.3** http://e-overheid.nl/onderwerpen/architectuur-en-nora/982-dossier-informatiebeveiliging
[10]	**GOVCERT.NL whitepaper 'Aanbevelingen ter bescherming tegen Denial-of-Service-aanvallen'** http://www.govcert.nl/dienstverlening/Kennis+en+publicaties/whitepapers/bescherming-tegen-ddos-aanvallen.html
[11]	**GOVCERT.NL whitepaper "Patchmanagement"** http://www.govcert.nl/dienstverlening/Kennis+en+publicaties/whitepapers/patch-management.html
[12]	**'Raamwerk beveiliging webapplicaties', versie 2.0, d.d. 4 november 2010** https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/raamwerk-beveiliging-webapplicaties.html

BIJLAGE C

Aanvalsmethoden

Aanvalsmethoden	Omschrijving
(Distributed) Denial-of-Service-aanvallen	Denial-of-Service-aanvallen (DoS) zijn elektronische aanvallen die een systeem, dienst of netwerk zo belasten dat ze niet meer beschikbaar zijn. Dit kan door de systemen uit te schakelen of een netwerk te overladen met dataverkeer. Een Denial of Service kan van een enkel systeem afkomstig zijn, maar ook van meerdere systemen tegelijkertijd. Een DoS-aanval vanaf meerdere systemen heet in jargon een Distributed-Denial-of-Service (dDoS).
Brute force	Brute force is het gebruik van rekenkracht om een 'probleem' op te lossen. De methode bestaat uit het botweg uitproberen van alle combinaties van toegestane tekens, net zolang tot diegene gevonden is die overeenkomt met de gewenste invoer.
Buffer overflow	Buffer overflows in het platform kunnen door kwaadwillenden worden misbruikt om willekeurige code uit te voeren op de webserver. In sommige gevallen biedt een buffer overflow alleen mogelijkheden om de kwetsbare service te laten crashen. Het probleem bij een buffer overflow is dat een kwetsbare applicatie data wil opslaan buiten de geheugenbuffer die voor deze applicatie is gereserveerd. Het gevolg hiervan is dat de applicatie geheugen in aanliggende geheugengebieden overschrijft. Een kwaadwillende kan het geheugen hierdoor mogelijk vullen met een eigen programma en dit programma vervolgens laten uitvoeren. Een buffer overflow op het platform kan vooral tot grote problemen leiden wanneer deze zich bevindt in een centraal onderdeel van het platform dat bovendien moeilijk af te schermen is voor kwaadwillenden. Hierbij kun je denken aan een kwetsbaarheid in de implementatie van TCP/IP.
Cross-Site Scripting (XSS)	Een aanvalstactiek waarbij het adres van een hiervoor kwetsbare website wordt misbruikt om extra informatie te tonen of programma's uit te voeren. Er zijn diverse vormen van cross site scripting waarbij complexe aanvallen mogelijk zijn.
Guest-hopping	Guest-hopping maakt gebruik van kwetsbaarheden in de hypervISOr, die het mogelijk maken om de beveiliging, die strikte scheiding tussen verschillende virtuele machines moet garanderen, te compromitteren. Op deze manier wordt toegang verkregen tot andere virtuele machines of zelfs de hypervISOr. Over het algemeen wordt gebruik gemaakt van de zwakste schakel, de minst beveiligde virtuele machine op het systeem. Die wordt gebruikt als vertrekpunt om aanvallen op andere virtuele machines uit te voeren. Op deze manier wordt van de ene naar de andere virtuele machine gesprongen. Bijvoorbeeld: Een aanvaller is geïnteresseerd in de gegevens van virtuele machine A, maar is niet in staat om direct tot A door te dringen. Dan zal de aanvaller proberen om virtuele machine B aan te vallen en vanaf deze virtuele machine proberen om toegang te krijgen tot A.
Hyper jacking	Hyper jacking is een methode waarbij een 'rogue' hypervISOr onder de bestaande legitieme infrastructuur (hypervISOr of besturingssysteem) wordt geïnstalleerd, met controle over alle acties tussen het doelwit en de hardware. Voorbeelden van hyper jacking zijn Blue Pill[52] en Vitriol[53].
Man-in-the-middle	Bij man-in-the-middle bevindt de aanvaller zich tussen een klant en een dienst. Hierbij doet hij zich richting de klant voor als de dienst en andersom. De dienst kan hier bijvoorbeeld een internetwinkel zijn. Als tussenpersoon kan de aanvaller nu uitgewisselde gegevens afluisteren en/of manipuleren.

52. http://theinvisiblethings.blogspot.com/2006/06/introducing-blue-pill.html
53. http://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Zovi.pdf

Aanvalsmethoden	Omschrijving
Rainbow table	Een tabel met mogelijke wachtwoorden en de hash-waarden van deze wachtwoorden. Ze worden gebruikt om wachtwoorden te testen op veiligheid of om deze te kraken. De techniek is vele malen sneller dan een brute force-techniek, waarbij de hash-waarden van de wachtwoorden nog moeten worden berekend.
Replay	Bij een 'replay'-aanval wordt een legitieme sessie van een doelwit opnieuw afgespeeld (meestal vastgelegd door het afluisteren van het netwerkverkeer).
Side channel	Een 'side channel'[54]- aanval maakt gebruik van een virtuele machine, die aanvallers hebben geïnstalleerd. Deze virtuele machine kan worden geïnstalleerd door gebruik te maken van kwaadaardige software of door zelf nieuwe virtuele machines af te nemen bij de cloudleverancier. Deze 'kwaadaardige' virtuele machine kan vervolgens gedeelde resources monitoren van andere virtuele machines. Deze resources bestaan uit geheugen en processoren op de gedeelde fysieke machine. Door deze gegevens te verzamelen en te analyseren, wordt het 'makkelijker' om vast te stellen wanneer een andere virtuele machine aangevallen kan vallen. Het is zelfs mogelijk om via zogenaamde 'keystroke timing attacks'[55], wachtwoorden en andere gevoelige informatie van een virtuele machine te achterhalen.
Social engineering	Een aanvalstechniek waarbij misbruik wordt gemaakt van menselijke eigenschappen als nieuwsgierigheid, vertrouwen en hebzucht met als doel vertrouwelijke informatie te verkrijgen of het slachtoffer een bepaalde handeling te laten verrichten.
Sniffing	Sniffing is het onderscheppen en lezen van informatie, zoals e-mailberichten of gebruikersnamen en wachtwoorden. Afluisteren wordt ook wel 'sniffing' genoemd.
Spoofing	Spoofing is jezelf voordoen als een ander. Iemand kan het e-mailadres van een ander gebruiken als zogenaamd afzendadres, zodat de geadresseerde in verwarring raakt. Deze methode kan handig zijn voor de verspreiding van virussen, omdat de ontvanger zou kunnen denken dat de afzender betrouwbaar is. Spoofing gebeurt ook op netwerkniveau, veelal met het doel internetverkeer in de war te schoppen.
SQL-injectiew	Veel webapplicaties maken gebruik van een database om daarin allerlei informatie op te slaan. De informatie die een dergelijke database kan bevatten, is zeer gevarieerd. Denk bijvoorbeeld aan gebruikersnaam en wachtwoord voor besloten gedeelten van de website, nieuwsberichten, logging van bezochte pagina's, et cetera. Om de informatie uit de database beschikbaar te maken op de website, voert de code achter een website allerlei verzoeken naar de database uit, op het moment dat de gebruiker een pagina van de website opent. Dit soort verzoeken maakt in veel gevallen gebruik van de standaard databasetaal 'Structured Query Language', kortweg SQL. Vaak kan de gebruiker daarbij de inhoud van het SQL verzoek direct of indirect beïnvloeden via een zoekterm of een ander invoerveld. Kwaadwillende hebben de mogelijkheid om een extra SQL-verzoek toe te voegen (injecteren), waardoor bijvoorbeeld de inhoud van de database wordt aangepast. We noemen dit verschijnsel dan ook 'SQL-injectie'. SQL-injectie kan plaats vinden als invoer van gebruikers op onvoldoende gecontroleerde wijze wordt verwerkt in een SQL-verzoek. Deze bedreiging is niet nieuw maar wel relevant bij SaaS-diensten. De vraag is namelijk, hoe de cloudleverancier omgaat met de scheiding van data binnen databases van verschillende cloudgebruikers.

54. http://people.csail.mit.edu/tromer/papers/cloudsec.pdf
55. http://www.ece.cmu.edu/~dawnsong/papers/ssh-timing.pdf

Colofon

Uitgave
Nationaal Cyber Security Centrum, Den Haag | Januari 2012

Wilhelmina van Pruisenweg 104 | 2595 AN Den Haag
Postbus 117 | 2501 CC Den Haag

T 070-888 75 55
F 070-888 75 50

E info@ncsc.nl
I www.ncsc.nl

Deze ICT-Beveiligingsrichtlijnen voor webapplicaties zijn in 2012 gepubliceerd door het NCSC. Een groot aantal partijen heeft direct of indirect bijgedragen aan deze ICT-beveiligingsrichtlijnen, waaronder de Rijksauditdienst (RAD), Logius, OWASP Nederland, Kwaliteitsinstituut Nederlandse Gemeenten (KING), Belastingdienst, gemeente Purmerend en Amsterdam, BDO, Mazars Paardekooper Hoffman N.V., Noordbeek B.V. en PwC.

Nationaal Cyber Security Centrum

Het Nationaal Cyber Security Centrum (NCSC) draagt via samenwerking tussen bedrijfsleven, overheid en wetenschap bij aan het vergroten van de weerbaarheid van de Nederlandse samenleving in het digitale domein.

Het NCSC ondersteunt de Rijksoverheid en organisaties met een vitale functie in de samenleving met het geven van expertise en advies, response op dreigingen en het versterken van de crisisbeheersing. Daarnaast voorziet het in informatie en advies voor burger, overheid en bedrijfsleven ten behoeve van bewustwording en preventie. Het NCSC is daarmee het centrale meld- en informatiepunt voor ICT-dreigingen en -veiligheidsincidenten.

Nationaal Cyber Security Centrum
Wilhelmina van Pruisenweg 104 | 2595 AN Den Haag
Postbus 117 | 2501 CC Den Haag

T 070-888 75 55
F 070-888 75 50

E info@ncsc.nl
I www.ncsc.nl

Januari 2012