Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

ICT-Beveiligingsrichtlijnen voor webapplicaties

Deel 1

ICT-Beveiligingsrichtlijnen voor webapplicaties

Deel 1

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

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 kwaadwillenden, 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 securityadviezen van het NCSC, 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 (dit document) beschrijft de beveiligingsrichtlijnen op hoofdniveau voor webapplicaties, bijbehorend beheer en infrastructuur.

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 zijn 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 de maatregelen die genomen kunnen worden om het optreden van bedreigingen terug

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

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. Niet-technische maatregelen worden uitsluitend opgenomen wanneer deze noodzakelijk worden geacht voor de technische context of wanneer andere normenkaders of standaarden hier onvoldoende op ingaan. Indien 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 1 tot en met 11 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.

De beveiligingsmaatregelen worden allen volgens hetzelfde format beschreven:

8. Cliënt 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 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 beveiligingsrichtlijn beoogd wordt.

In deel twee 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 samenvatting van alle beveiligingsrichtlijnen en kan gebruikt worden als checklist voor de beveiligingsrichtlijnen.

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 v3 [2]
- OWASP Code Review Guide [3]
- OWASP Application Security Verification Standard (ASVS) [4]
- NEN-ISO/IEC 27001 'Managementsystemen voor informatiebeveiliging'[14] [5]
- NEN-ISO/IEC 27002 'Code voor informatiebeveiliging'[15] [6]
- NEN-ISO/IEC 27005 'Information security risk management'[16] [7]
- 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. Voor een geldige verklaring van conformiteit met de Richtlijn, moeten webapplicaties voldoen aan alle succescriteria voor alle beveiligingsrichtlijnen
12. Met behulp van het classificatiesysteem worden de maatregelen gewaardeerd.
13. 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>.
14. 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.
15. 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.
16. 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.
17. De Nederlandse Overheid Referentie Architectuur (NORA) bevat principes, beschrijvingen, modellen en standaarden voor het ontwerp en de inrichting van de elektronische overheid. Het is een instrument dat door overheidsorganisaties kan worden benut in de verbetering van de dienstverlening aan burgers en bedrijven; http://www.e-overheid.nl/onderwerpen/e-overheid/architectuur/nora-familie/nora

HOOFDSTUK 2

Inleiding in website-beveiliging

2.1 Waarom informatiebeveiliging

Informatie en de ondersteunende processen, systemen en netwerken zijn belangrijke bedrijfsmiddelen. De beschikbaarheid, integriteit en vertrouwelijkheid ervan kunnen van essentieel belang zijn voor het behoud van de concurrentiepositie, cashflow, winstgevendheid, naleving van de wet en het imago van de organisatie.2

In toenemende mate worden organisaties en hun informatiesystemen en netwerken geconfronteerd met beveiligingsrisico's. Dit omvat computerfraude, spionage, sabotage en vandalisme. Computervirussen, computer hacking en het verhinderen van dienstverlening komen steeds vaker voor, worden steeds ambitieuzer en steeds geavanceerder.

Steeds meer organisaties bieden diensten aan klanten aan via internet. Dit gebeurt bijvoorbeeld via websites, extranetten en webservices. De mogelijkheden die informatiesystemen bieden, nemen steeds verder toe, evenals de informatie die bedrijven en overheden aanbieden via dergelijke toepassingen. Afhankelijkheid van informatiesystemen en -diensten betekent dat organisaties steeds kwetsbaarder worden voor bedreigingen van de beveiliging. De onderlinge verbondenheid van openbare en private netwerken en het delen van informatie, de ketenafhankelijke elektronische dienstverlening, maken het steeds moeilijker om de beschikbaarheid, vertrouwelijkheid en integriteit van informatie te beveiligen. De informatiebeveiliging van de keten als geheel moet op orde zijn. De zwakste schakels in die ketens bepalen namelijk de veiligheid van de keten als geheel. Voldoende aandacht voor de beveiliging van deze webapplicaties is essentieel om informatie afdoende te beschermen en het vertrouwen van eindgebruikers in zulke *internet enabled* webapplicaties niet te schaden.

Aangezien een webapplicatie vaak onderdeel uitmaakt van een keten van ICT-diensten, is het belangrijk dat de aandacht bij de beveiliging van een webapplicatie niet alleen uitgaat naar de webapplicatie. Ook alle omliggende componenten (webservers, databases, logging servers, proxies, besturingssytemen, netwerken, et cetera), waarvan de webapplicatie afhankelijk is, vervullen een belangrijke rol in het functioneren van de webapplicatie. Deze componenten moeten daarom ook worden betrokken in het geheel aan beveiligingsmaatregelen. De beveiliging die met technische middelen kan worden bereikt, is begrensd en moet worden ondersteund door passend beheer en procedures.

2.2 Het opstellen van maatregelen

Het is van essentieel belang dat een organisatie haar eigen beveiligingsbehoeften bepaalt. Er zijn drie hoofdbronnen.

De eerste bron wordt ontleend aan de beoordeling van de risico's voor de organisatie. Via risicoanalyse worden de bedreigingen ten aanzien van bedrijfsmiddelen vastgesteld, de kwetsbaarheid voor en waarschijnlijkheid van het optreden hiervan beoordeeld en de potentiële effecten geschat (zie paragraaf 2.4 'Risicoanalyse').

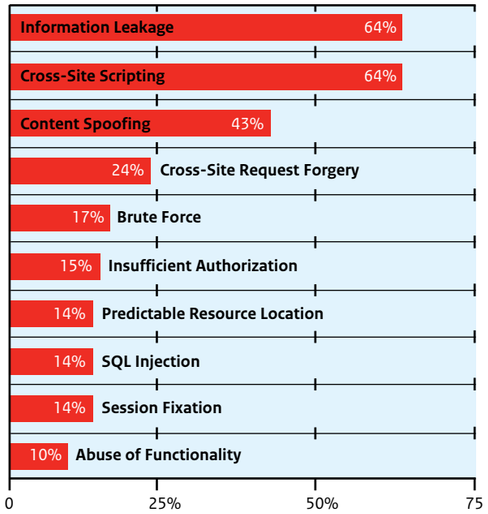
De tweede bron wordt gevormd door de wettelijke, statutaire, regulerende en contractuele eisen waaraan de organisatie, haar handelspartners, aannemers en dienstverlenende bedrijven moeten voldoen.

De derde bron van eisen wordt gevormd door het eigen stelsel van principes, doelstellingen en eisen voor het verwerken van informatie die de organisatie heeft ontwikkeld ter ondersteuning van haar bedrijfsvoering.

2.3 Mogelijke kwetsbaarheden en bedreigingen

Een webapplicatie heeft te maken met een groot aantal mogelijke kwetsbaarheden en bedreigingen. Deze kwetsbaarheden en bedreigingen bevinden zich op verschillende niveaus; denk hierbij aan kwetsbaarheden en bedreigingen op netwerkniveau (bijvoorbeeld Denial of Service (DoS)), op authenticatieniveau (bijvoorbeeld het omzeilen van authenticatiemechanismen) of op applicatieniveau (bijvoorbeeld Cross-Site Scripting (XSS)).
Figuur 2-1 toont de resultaten van een onderzoek van Whitehat Security[18] naar veel voorkomende lekken in webapplicaties. Hieruit blijkt bijvoorbeeld dat 'Cross-Site Scripting' en 'Information Leakage' de belangrijkste kwetsbaarheden zijn op applicatieniveau.

Figuur 2-1: Webapplicatie kwetsbaarheden op applicatieniveau



Percentage waarschijnlijkheid dat tenminste één kwetsbaarheid voorkomt in een website

18. Whitehat Security: Overall Top Ten Vulnerabillity Classes of 2010 https://www.whitehatsec.com/assets/WPstats_winter11_11th.pdf

Alle soorten kwetsbaarheden en bedreigingen, dus niet alleen die op applicatieniveau, worden geadresseerd in deze Richtlijnen (hoofdstuk 1 t/m 11).

Drie generieke kwetsbaarheden en bedreigingen noemen we hier alvast, omdat ze aanwezig kunnen zijn op alle afzonderlijke lagen van het raamwerk en niet gebonden zijn aan één van deze lagen:

- Configuratiefouten. Wanneer software out-of-the-box wordt uitgerold, kan dit tot beveiligingsproblemen leiden.
- Aanwezigheid van bekende kwetsbaarheden. Dagelijks verschijnen op internet beveiligingsadviezen van verschillende leveranciers waarin de leverancier een kwetsbaarheid in één van zijn softwareproducten beschrijft. Het is belangrijk geleverde updates snel te installeren om de kwetsbaarheid te verhelpen.
- Aanwezigheid van nieuwe, tot nu toe onbekende, (0-day-) kwetsbaarheden. Wanneer niet de leverancier maar een derde (bijvoorbeeld een hacker) een kwetsbaarheid bekend maakt, en de leverancier niet in staat is gesteld om updates voor zijn software uit te brengen, dan spreek je van een 0-day kwetsbaarheid. Aangezien organisaties zo'n kwetsbaarheid niet meteen kunnen verhelpen door updates te installeren, ben je afhankelijk van eventuele workarounds. Kwaadwillenden maken dankbaar misbruik van 0-day-kwetsbaarheden om aanvallen op webapplicaties uit te voeren.

Bedenk dat kwaadwillenden op basis van specifieke eigenschappen, eenvoudig op internet kunnen zoeken naar kwetsbare webapplicaties. Dit kan bijvoorbeeld via zoekmachines als Google ('Google Hacking'), waardoor de drempel voor het aanvallen van webapplicaties heel laag is.

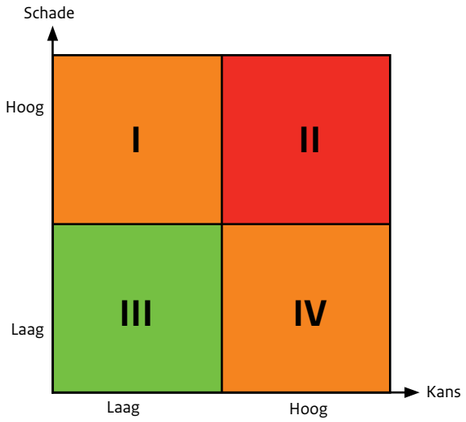
2.4 Risicoanalyse

Elke maatregel uit de Richtlijn heeft als doel om het risico met betrekking tot misbruik van webapplicaties te verlagen. Bij het treffen van beveiligingsmaatregelen, is het belangrijk om te beseffen waaruit het risico is opgebouwd. De Richtlijn gebruikt de volgende, breed geaccepteerde definitie van risico:

Risico is het product van de kans op optreden van een ongewenste gebeurtenis en de mogelijke schade als gevolg van deze ongewenste gebeurtenis (risico = kans x schade)

Bovenstaande definitie van risico betekent dat een maatregel er altijd op geënt moet zijn om de kans op een kwetsbaarheid te verminderen en de kans op schade door misbruik van een kwetsbaarheid te minimaliseren. Kans op optreden en risico kunnen in een matrix worden uitgezet, waarbij elke as de waarde hoog en laag kan aannemen. Figuur 2-2 illustreert deze matrix. Hierbij ontstaan vier kwadranten van risico: hoog risico (kwadrant I), gemiddeld risico (kwadranten II en IV) en laag risico (kwadrant III).

Figuur 2-2: Matrix risico inschaling



Neem bijvoorbeeld het risico van SQL-injectie bij een bepaalde webapplicatie. Neemt een organisatie geen beveiligingsmaatregelen tegen SQL-injectie, dan zal de kans op optreden hiervan hoog zijn. Als hierdoor bijvoorbeeld privacy-gevoelige gegevens op straat komen of de integriteit van de database kan worden aangetast, zal ook de schade door SQL-injectie hoog zijn. De combinatie van deze feiten zorgt ervoor dat dit risico wordt ingeschaald in kwadrant I (hoog risico). Wanneer de ontwikkelaar besluit om gebruik te maken van geparameteriseerde queries en een account met beperkte rechten, verlaagt de ontwikkelaar hiermee de kans dat SQL-injectie optreedt. Echter, de schade die optreedt als een kwaadwillende er toch in slaagt om een SQL-injectie aanval op de webapplicatie uit te voeren, is nog steeds hoog. Het risico komt hiermee terecht in kwadrant IV (gemiddeld risico). De gewenstheid van eisen en maatregelen om hier wat aan te doen, kan als gevolg hiervan ook als gemiddeld worden bestempeld. Om de schade door SQL-injectie te verlagen kunnen gevoelige gegevens gehashed of versleuteld in de database worden opgeslagen. De mogelijke schade wordt hierdoor verlaagd. Als al deze maatregelen worden genomen kan het risico op SQL-injectie hierdoor als laag worden gekwalificeerd (kwadrant III).

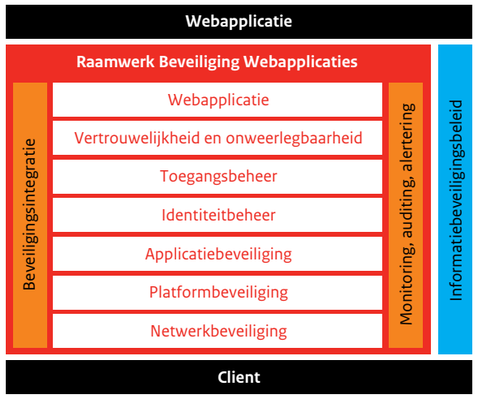
Het is belangrijk om bij het wegen van eisen en het implementeren van de beveiligingsmaatregelen om onderscheid tussen kans op optreden en mogelijke schade te maken om zodoende het risico zoveel mogelijk te kunnen verlagen. Als bijvoorbeeld alleen beveiligingsmaatregelen zijn geïmplementeerd die de kans op optreden verlagen, kan de schade als gevolg van misbruik nog steeds heel hoog zijn. Beveiligingsmaatregelen moeten dus als doel hebben om zowel de kans op optreden als de mogelijke schade terug te brengen tot een aanvaardbaar niveau.

2.5 Beveiligen van webapplicaties

Het beveiligen van webapplicaties is meer dan het versleutelen van verkeer of het gebruik van firewalls. Een webapplicatie is pas optimaal beveiligd wanneer organisaties op meerdere niveaus beveiligingsmaatregelen treffen tegen misbruik ervan (gelaagde beveiliging of in-depth security). De Richtlijn beschrijft alle lagen waaraan ontwikkelaars, beheerders en architecten bij het beveiligen van een webapplicatie aandacht aan moeten schenken.

De Richtlijn is gebaseerd op het Raamwerk Beveiliging webapplicaties (RBW) dat door het NCSC is gepubliceerd. In Figuur 2-3 is het RBW schematisch weergegeven. Zoals uit het raamwerk van Figuur 2-3 is op te maken, bestaat de beveiliging van webapplicaties uit verschillende horizontale en verticale (beveiligings-)lagen. Bekeken vanaf de client verschijnen achtereenvolgens de volgende horizontale lagen:

Figuur 2-3: Raamwerk Beveiliging Webapplicaties



- **Netwerkbeveiliging**
  Bij netwerkbeveiliging ligt de focus op het beveiligen van de infrastructuur via firewalls, routers en switches. Belangrijk is een solide DMZ-ontwerp en architectuur waarbij de organisatie aandacht besteedt aan zaken als compartimentering (waarbij de DMZ wordt opgedeeld in compartimenten met daarin diensten met gelijke functionaliteit en beveiligingsniveau), een minimale hoeveelheid componenten in de DMZ (bijvoorbeeld geen databases), scheiding van de DMZ met de achterliggende netwerksegmenten, verplichte routepaden door de DMZ en scheiding van regulier verkeer en beheerverkeer. Om te voorkomen dat kwaadwillenden een webapplicatie via de infrastructuur aanvallen, moeten organisaties voldoende beveiligingsmaatregelen treffen tegen 'Distributed Denial-of-Service' aanvallen en moeten zij tevens hardening op infrastructuurniveau doorvoeren. Denk hierbij aan het uitschakelen van onnodige services en het gebruik van veilige protocollen bij het uitvoeren van beheerwerkzaamheden.
- **Platformbeveiliging**
  Platformbeveiliging richt zich op het beveiligen van de besturingssystemen waarop webservers, databaseservers, et cetera draaien. Om te voorkomen dat kwaadwillenden misbruik maken van bekende en nieuwe kwetsbaarheden is het belangrijk een solide updatemechanisme te implementeren. Naast een technische inrichting, moet een organisatie ook aandacht besteden aan procedures hiervoor. Het inperken van rechten op het systeem, het hardenen van essentiële systeemonderdelen zoals de TCP- en IP-stacks en het gebruik van beveiligingstemplates, verlagen de kans dat kwaadwillenden misbruik van de server maken. Door auditing op OS-niveau in te richten, zorgen organisaties ervoor dat eventueel misbruik toch gedetecteerd kan worden.
- **Applicatiebeveiliging**
  De nadruk in de Richtlijn ligt voor een groot deel op webapplicatiebeveiliging. Veel problemen met webapplicaties vinden hun oorsprong in fouten die ontwikkelaars maken bij het ontwikkelen van een webapplicatie. Denk hierbij aan kwetsbaarheden als Cross-Site-Scripting (XSS), SQL-injectie en command-injectie. Veel van deze problemen ontstaan doordat ontwikkelaars in- en uitvoer onvoldoende valideren. Het valideren van alle mogelijke invoer, het coderen van gevaarlijke karakters in de uitvoer en het gebruik van geparameteriseerde queries voor communicatie met de database, kunnen deze kwetsbaarheden helpen voorkomen. Andere belangrijke zaken zijn het gebruik van accounts met beperkte rechten voor het verbinden met databases en andere systemen en het opleiden van ontwikkelaars in het veilig programmeren van webapplicaties.

  Een Web Application Firewall (WAF) is een applicatie die de beveiliging van een webapplicatie kan verhogen. Een WAF fungeert als reverse proxy of als plug-in op de webserver en is gespecialiseerd in het uitvoeren van invoervalidatie, protocolvalidatie, uitvoervalidatie en het normaliseren en loggen van alle webverzoeken. Hoewel een WAF een waardevolle toevoeging voor de beveiliging van een webomgeving kan zijn, vervangt dit zeker niet de beveiligingsmaatregelen op applicatieniveau. De toevoeging van een WAF is een voorbeeld van gelaagde beveiliging (in-depth defence).
- **Identiteit- en toegangsbeheer**
  Veel webapplicaties blijken op het gebied van identiteit- en toegangsbeheer problemen te hebben met het implementeren van een veilig mechanisme voor sessiemanagement. De vraag is of elke webapplicatie

het wiel op dit gebied telkens opnieuw moet uitvinden of dat je hiervoor een gespecialiseerde 'Identity & Access Management'(I&AM)-component kan inzetten. Belangrijk is in ieder geval om de inzet van gespecialiseerde tooling te overwegen en om vervolgens te bepalen welke authenticatie- en autorisatiefuncties op welke plek in de webomgeving worden uitgevoerd. Tot slot is het niet alleen van belang om te kijken naar de inlogfunctionaliteit, maar ook naar de mogelijkheid om de sessie expliciet of impliciet te beëindigen (uitloggen en bijvoorbeeld maximale sessieduur).

- **Vertrouwelijkheid en onweerlegbaarheid**
  In de laag 'Vertrouwelijkheid en onweerlegbaarheid' ligt de focus op het beschermen van data en het bewijzen dat bepaalde transacties daadwerkelijk hebben plaatsgevonden. Om data voldoende te beschermen is het van belang versleuteling op transportniveau toe te passen door het gebruik van Secure Sockets Layer (SSL) of Transport Layer Security (TLS). Versleuteling op transportniveau is echter niet voldoende. Zo moet gevoelige informatie ook versleuteld worden opgeslagen in databases om te voorkomen dat kwaadwillenden via aanvallen als SQL-injectie alsnog inzicht krijgen in deze informatie. Tot slot is het advies om gebruik te maken van digitale handtekeningen om de onweerlegbaarheid van transacties te kunnen bereiken.

Bij publieke webapplicaties die geen authenticatie vereisen, vormen de eerste drie lagen (netwerk, platform en applicatie) gezamenlijk de basis van de beveiliging van de webapplicatie. In sommige gevallen speelt bij een webapplicatie die geen authenticatie vereist, ook het aspect vertrouwelijkheid een belangrijke rol. Denk aan het versturen van mogelijk gevoelige informatie via een webformulier.

Bij webapplicaties die wel authenticatie vereisen, zijn ook de overgebleven twee lagen (identiteitbeheer en toegangsbeheer) van belang.

Naast de genoemde horizontale lagen bevindt zich in het raamwerk ook nog een aantal verticale lagen. Deze lagen bieden ondersteuning aan de horizontale lagen:

- **Beveiligingsintegratie**
  Binnen de diverse lagen van het RBW zijn verschillende mechanismen ingericht voor het beveiligen van de webapplicatie. Om samenwerking tussen deze mechanismen te kunnen bewerkstelligen, is het belangrijk aandacht te besteden aan de samenhang tussen deze mechanismen. Deze samenwerking maakt onderdeel uit van de laag 'Beveiligingsintegratie'. Bij elke beveiligingscomponent uit het RBW is het dan ook van belang te bekijken welke diensten deze component van andere componenten moet kunnen afnemen en welke diensten de component moet kunnen aanbieden aan andere componenten.

- **Monitoring, auditing en alerting**
  Monitoring, auditing en alerting zijn van toepassing op elke laag van het RBW en hebben als doel inzicht te behouden in het functioneren van de webomgeving en aanvallen hierop. Het is belangrijk om:
  - causale verbanden te leggen tussen gebeurtenissen op verschillende lagen.
  - verzamelde logginggegevens actief en in samenhang te bekijken. Een centrale logging is aan te bevelen.
  - samenwerking tussen verschillende afdelingen van een organisatie te bevorderen om op die manier multidisciplinair problemen te verhelpen en te detecteren.

Als laatste is in Figuur 2-3 het informatiebeveiligingsbeleid afgebeeld. Dit beleid is leidend voor de invulling van de verschillende andere onderdelen van het raamwerk. Dit informatiebeveiligingsbeleid komt in dit document verder niet of nauwelijks aan de orde, omdat een organisatie bij het implementeren van de beveiligingsmaatregelen uit het RBW al over een dergelijk beleid moet beschikken.

Naast bovenstaande technische beveiligingsmaatregelen die geïmplementeerd moeten zijn, moet ook nog aandacht worden besteedt aan personele, organisatorische en procedurele beveiligingsmaatregelen. Deze komen in dit document slechts beperkt aan de orde.

HOOFDSTUK 2 > INLEIDING IN WEBSITEBEVEILIGING

HOOFDSTUK 3

Algemene beveiligings-richtlijnen

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

Nr.	Beschrijving van beveiligingsrichtlijn	Doelstelling	Classificatie
B0-1	**Informatiebeveiliging is als een proces ingericht.**	• De effectiviteit van informatiebeveiliging (maatregelen en bijbehorende procedures) waarborgen. • Aantonen dat aan gestelde maatregelen en verwachtingen wordt voldaan.	Hoog
B0-2	**Voer actief risicomanagement uit.**	• 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.	Hoog
B0-3	**Voor elke maatregel wordt documentatie vastgelegd en onderhouden.**	• 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.	Hoog
B0-4	**Alle ICT-componenten en -diensten inclusief de onderlinge relaties worden vastgelegd en dit overzicht wordt permanent onderhouden.**	• 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.	Hoog
B0-5	**Alle wijzigingen worden altijd eerst getest voordat deze in productie worden genomen en worden via wijzigingsbeheer doorgevoerd.**	• Het garanderen van een correcte en veilige werking van ICT-voorzieningen door het op een gecontroleerde manier doorvoeren van wijzigingen.	Hoog
B0-6	**Maak gebruik van een hardeningsproces[19], zodat alle ICT-componenten zijn gehard tegen aanvallen.**	• Het tot een minimum beperken van de kans dat onnodige faciliteiten op een systeem worden misbruikt.	Hoog
B0-7	**De laatste (beveiligings)patches zijn geïnstalleerd en deze worden volgens een patchmanagement proces doorgevoerd.**	• 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.	Hoog

19. Hardenen van systemen bestaat uit verschillende stappen om een gelaagde bescherming te bieden. Met behulp 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.

Nr.	Beschrijving van beveiligingsrichtlijn	Doelstelling	Classificatie
B0-8	**Penetratietests[20] worden periodiek uitgevoerd.**	• Inzicht krijgen en houden in de mate waarin een webapplicatie weerstand kan bieden aan pogingen om het te compromitteren (binnendringen of misbruiken van webapplicatie).[21]	Hoog
B0-9	**Vulnerability assessments (security scans) worden periodiek uitgevoerd.**	• Inzicht hebben in de mate waarin de ICT-omgeving bekende kwetsbaarheden en zwakheden bevat, zodat deze waar mogelijk weggenomen kunnen worden.	Hoog
B0-10	**Policy compliance checks worden periodiek uitgevoerd.**	• 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.	Midden
B0-11	**Er moet een toereikend recovery proces zijn ingericht waar back-up en restore onderdeel vanuit maken.**	• Het waarborgen van de integriteit en beschikbaarheid van informatieverwerkende systemen of webapplicaties.	Hoog
B0-12	**Ontwerp en richt maatregelen in met betrekking tot toegangsbeveiliging/ toegangsbeheer.**	• Voorkom ongeautoriseerde toegang tot netwerken, besturingssystemen, informatie en informatiesystemen en -diensten, zodat schade bij misbruik zo beperkt mogelijk is.	Hoog
B0-13	**Niet (meer) gebruikte websites en/of informatie moet worden verwijderd.**	• Voorkom misbruik van ‘oude’ en niet meer gebruikte websites en/of informatie.	Hoog
B0-14	**Leg afspraken met leveranciers vast in een overeenkomst.**	• 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.	Hoog

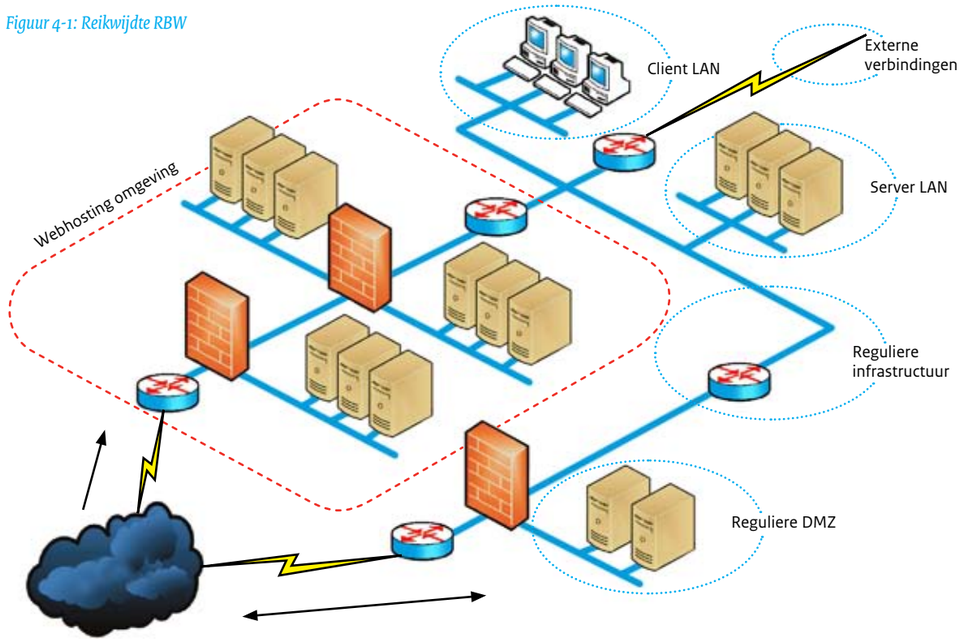
20. Andere termen die voor penetratietests gebruikt worden zijn ethical hacking test, legal hacking test, hacktest, security scan, vulnerability assessment en diverse samenstellingen van deze termen. De termen komen min of meer op hetzelfde neer.
21. Een pentest is een momentopname beperkt naar de laatste stand der techniek. Door ontwikkelingen in deze techniek kunnen er zich nieuwe risico’s voordoen of bestaande risico’s zwaarde gaan wegen.

HOOFDSTUK 3 > ALGEMENE BEVEILIGINGSRICHTLIJNEN

HOOFDSTUK 4

Netwerkbeveiliging

Figuur 4-1: Reikwijdte RBW



Het netwerk omvat zowel de infrastructuur om de website 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 4-1 illustreert deze netwerkinfrastructuur, met daarin de afbakening van deze Richtlijn (vlak binnen rode stippellijn). Het uitvallen van het netwerk, of een succesvolle aanval daarop, kan ernstige gevolgen hebben voor de beschikbaarheid van de web-applicatie en in sommige gevallen voor de integriteit en vertrouwelijkheid van het netwerkverkeer en de data.

In het kader van deze Norm 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.

4.1 Kwetsbaarheden en bedreigingen

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

- (Distributed) Denial of Service (dDoS): onbereikbaar maken van de webapplicatie via flooding (bijvoorbeeld via een SYN-aanval), Smurf-aanval, et cetera.
- Pivoting of server hopping: toegang tot servers in het netwerk door via een gecompromitteerde machine andere machines in het netwerk te benaderen.
- Domain Name System (DNS): 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
- Firewall: 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 de firewall software.
  - Onduidelijke wensen.

4.2 Doelstelling

Doelstelling is: 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 Norm richt zich op het beveiligen van de informatiestromen op het transport- en netwerkniveau.

4.3 Beveiligingsrichtlijnen

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

Nr.	Beschrijving van beveiligingsrichtlijn	Doelstelling	Classificatie
B1-1	**Er moet gebruik worden gemaakt van een Demilitarised Zone (DMZ), waarbij compartimentering[22] wordt toegepast en de verkeersstromen tussen deze compartimenten wordt beperkt tot alleen de hoogst noodzakelijke.**	• 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.	Hoog
B1-2	**Beheer- en productieverkeer zijn van elkaar gescheiden.**	• Voorkom dat misbruik kan worden gemaakt van de beheervoorzieningen vanaf het internet.	Hoog
B1-3	**Netwerktoegang tot de webapplicaties is voor alle gebruikersgroepen op een zelfde wijze ingeregeld.**	• Voorkom (nieuwe) beveiligingsrisico's omdat de webapplicaties ook bereikbaar moeten zijn vanaf het interne netwerk voor gebruikers binnen de organisaties.	Hoog
B1-4	**Netwerkcompartimenten bevatten geen fysieke koppelingen door middel van gedeelde componenten.**	• Voorkom het omzeilen van logische scheidingen door fysieke scheiding van netwerkcomponenten.	Hoog
B1-5	**Implementeer maatregelen tegen (d)DoS.**	• Beperken impact van (d)DoS aanvallen.	Midden
B1-6	**Implementeer maatregelen zodat het netwerk geen Single Points-of-Failure (SPOF) bevat.**	• Voorkom uitval (beschikbaarheid) van de (netwerk)omgeving.	Midden

22. Compartimentering wordt ook wel omschreven als zonering, segmentering of logisch domein.

HOOFDSTUK 4 > NETWERKBEVEILIGING

HOOFDSTUK 5

Platformbeveiliging

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.

5.1 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:

- Kwetsbaarheden in het besturingssysteem: voor veel kwetsbaarheden in besturingssysteem komt vaak snel exploitcode beschikbaar.
- Onveilige beheermechanismen: de informatie die via onversleutelde beheermechanismen zoals Telnet wordt uitgewisseld, is te onderscheppen.
- Onjuiste autorisaties: het gebruik van service accounts met uitgebreide rechten verhoogt de schade bij succesvol misbruik van kwetsbaarheden.
- Onnodige services: elke service die een systeem biedt, heeft mogelijk kwetsbaarheden.

5.2 Doelstelling

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

5.3 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. 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.
Specifieke maatregelen voor de verschillende besturingssystemen zoals Microsoft Windows, verschillende UNIX en Linux distributies worden aangeboden door de 'Security Benchmarks division'[23].

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 te downloaden op: HTTPs://benchmarks.cisecurity.org/en-us/?route=downloads.multiform.

Nr.	Beschrijving van beveiligingsrichtlijn	Doelstelling	Classificatie
B2-1	**Maak gebruik van veilige beheermechanismen.**	• Voorkom misbruik van beheervoorzieningen.	Hoog
B2-2	**Maak gebruik van beveiligingstemplates[24] bij de beveiliging van systemen.**	• Alle systemen worden conform een vastgestelde wijze ingericht / gehardend (en niet conform de kennis van een willekeurige beheerder).	Midden
B2-3	**Maak gebruik van jailing (sandboxing)[25].**	• Beperk de schade bij misbruik van processen.	Midden
B2-4	**Maak gebruik van lokale firewalls.**	• Het controleren van het netwerkverkeer, zowel op poort- als procesniveau, dat lokaal binnenkomt en uitgaat.	Midden

23. HTTPs://benchmarks.cisecurity.org/en-us/?route=default
24. Beveiligingstemplates bestaan uit documenten die de hardening beschrijven en worden technisch ondersteund door scripts, images, configuratiebestanden, et cetera.
25. Jailing (sandboxing) is een manier om een proces te isoleren van de rest van een besturingssysteem, bijvoorbeeld chroot.

HOOFDSTUK 6

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, maar hoeft geen geïntegreerd onderdeel van de webapplicatie zelf te zijn. Het 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.

6.1 Kwetsbaarheden en bedreigingen

Mogelijke kwetsbaarheden en bedreigingen zijn:

- SQL-injectie: mogelijkheid tot het manipuleren van toegang tot de database waardoor informatie onbedoeld kan worden ontsloten, gewijzigd of toegevoegd. Daarnaast vormt de uitgebreide functionaliteit van hedendaagse databases een gevaar.
- Cross-Site Scripting (XSS): reflected XSS, stored XSS en DOM-based XSS als vehikel voor het uitvoeren van aanvallen op gebruikers van een webapplicatie.
- Cross-Site Request Forgery (CSRF): door onvoldoende autorisatiecontroles op een transactie kan een kwaadwillende een gebruiker willekeurige acties laten uitvoeren bij het bezoeken van een malafide website.
- Lekken van informatie: foutmeldingen, header-informatie en commentaarregels kunnen waardevolle (technische) informatie aanleveren over de webapplicatie.
- HTTP Response Splitting: het injecteren van een extra HTTP-response via een onvoldoende gevalideerde HTTP-header kan leiden tot caching problemen en XSS-aanvallen.
- Remote File Inclusion (RFI): het laten uitvoeren van een malafide script op de webserver, voornamelijk een probleem onder PHP.
- Path Traversal: mogelijk probleem in zowel de webserver als de webapplicatie waarbij de mogelijkheid bestaat om bestanden buiten de webroot te benaderen.
- Command-injectie: injecteren van malafide OS-commando's op het moment dat de webapplicatie een commando aanroept zonder voldoende validatie van gebruikersinvoer.
- Buffer overflows: buffer overflows in webapplicaties zijn niet eenvoudig te ontdekken maar kunnen wel ernstige gevolgen hebben.
- Fouten in de applicatielogica: niet-technische fouten kunnen ook leiden tot beveiligingsproblemen.
- Configuratiefouten: zaken als standaard gebruikersnamen en wachtwoorden, het ontbreken van patches en ingeschakelde debugging opties kunnen leiden tot problemen.
- Geen invoervalidatie: onvoldoende controle van gebruikersinvoer kan leiden tot diverse problemen (zoals XSS en SQL-injectie).
- Geen uitvoervalidatie: een webapplicatie kan door onvoldoende validatie soms ongewenste uitvoer produceren, bijvoorbeeld in het geval van XSS.
- Ineffectieve filters: filters zijn niet in alle gevallen effectief waardoor aanvallen, ondanks deze filters, nog steeds mogelijk zijn.
- Onveilige opslag van informatie: het niet versleuteld opslaan van informatie kan ertoe leiden dat kwaadwillenden deze informatie in handen krijgen.
- Kwetsbare aangekochte webapplicaties: ook aangekochte webapplicaties kunnen kwetsbaarheden bevatten.
- Gebruik van voorbeeldscripts van internet: voorbeeldscripts op internet bevatten vaak kwetsbaarheden. Gebruik hiervan is dan ook gevaarlijk.
- Onvoldoende hardening en patching.

6.2 Doelstelling

Doelstelling is: waarborgen dat beveiliging wordt ingebouwd in webapplicaties.

6.3 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. De maatregelen zijn onderverdeeld in maatregelen op het gebied van softwareontwikkeling, configuratiemaatregelen, procedurele maatregelen en overig.

Software-ontwikkeling

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.	Beschrijving van beveiligingsrichtlijn	Doelstelling	Classificatie
B3-1	**De webapplicatie valideert de inhoud van een HTTP-request voor die wordt gebruikt.**	• Voorkomen het verlies, wijziging of misbruik van gegevens door onbetrouwbare (malafide) invoer. • Voorkom dat de applicatielogica wordt beïnvloed.	Hoog
B3-2	**De webapplicatie controleert voor elk HTTP verzoek of de initiator geauthenticeerd is en de juiste autorisaties heeft.**	• Valideer de initiator van een HTTP-request teneinde te voorkomen dat kwaadwillenden transacties uit naam van een valide gebruiker uitvoeren.	Hoog

Nr.	Beschrijving van beveiligingsrichtlijn	Doelstelling	Classificatie
B3-3	**De webapplicatie normaliseert[26] invoerdata voor validatie.**	• Normaliseer alle invoerdata voor deze te valideren om te voorkomen dat filteringmechanismen ongewenste patronen niet herkennen.	Hoog
B3-4	**De webapplicatie codeert dynamische onderdelen in de uitvoer.**	• Codeer dynamische onderdelen[27] van de uitvoer zodat er geen ongewenste tekens in de uitvoer terecht komen.	Hoog
B3-5	**Voor het raadplegen en/of wijzigen van gegevens in de database gebruikt de webapplicatie alleen geparametriseerde queries.**	• Door databasequeries samen te stellen op basis van geparameteriseerde queries (in tegenstelling tot dynamische strings), wordt de kans op SQL-injectie aanzienlijk verkleind.	Hoog
B3-6	**De webapplicatie valideert alle invoer, gegevens die aan de webapplicatie worden aangeboden, aan de serverzijde.**	• Voorkom dat controles kunnen worden omzeild.	Hoog
B3-7	**De webapplicatie staat geen dynamische file includes toe of beperkt de keuze mogelijkheid (whitelisting).**	• Voorkom dat ongewenste bestanden worden geïncorporeerd in een webapplicatie.	Hoog
B3-8	**De webserver verstuurt alleen HTTP-headers die voor het functioneren van HTTP van belang zijn.**	• Beperk het (onnodig) vrijgeven van informatie tot een minimum.	Hoog
B3-9	**De webserver toont alleen de hoogst noodzakelijke informatie in HTTP-headers die voor het functioneren van belang zijn.**	• Beperk het (onnodig) vrijgeven van informatie tot een minimum.	Hoog
B3-10	**De webserver beperkt de informatie, bij het optreden van een fout, aan de gebruiker tot een minimum in een HTTP-response.**	• Beperk het (onnodig) vrijgeven van informatie tot een minimum.	Hoog
B3-11	**Commentaarregels zijn uit de scripts (code) verwijderd.**	• Beperk het (onnodig) vrijgeven van informatie tot een minimum.	Hoog
B3-12	**De webserver maakt alleen gebruik van de hoogst noodzakelijke HTTP-methoden.**	• Voorkom onnodige beveiligingsrisico's door het blokkeren van niet noodzakelijke HTTP-methoden.	Hoog
B3-13	**Directory-listings zijn uitgeschakeld.**	• Beperk het (onnodig) vrijgeven van informatie tot een minimum.	Hoog
B3-14	**Voer een code review uit.**	• In een vroegtijdig stadium ontdekken van potentiële kwetsbaarheden.	Midden
B3-15	**Een (geautomatiseerde) blackbox scan wordt periodiek uitgevoerd.**	• Testen of er kwetsbaarheden in de webapplicatie bestaan.[28]	Hoog
B3-16	**Zet de cookie attributen 'HttpOnly' en 'Secure'.**	• Voorkom dat cookie communicatie kan worden afgeluisterd en voorkom dat cookies gestolen kunnen worden via cross site scripting.	Hoog

26. Normaliseren houdt in dat bijvoorbeeld onnodige witruimtes worden verwijderd, gecodeerde karakers worden gedecodeerd, et cetera.
27. Het coderen van dynamische pagina-inhoud houdt in dat de webapplicatie mogelijk 'gevaarlijke' karakters codeert. Deze dynamische informatie kan bijvoorbeeld afkomstig zijn uit databases of externe bronnen maar kan ook gebaseerd zijn op invoer van de gebruiker.

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

HOOFDSTUK 7

Identiteit- en toegangs-beheer

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 autorisatie-tabel, mag een gebruiker wel of geen gebruik maken van (delen van) de webapplicatie).

7.1 Kwetsbaarheden en bedreigingen

Mogelijke kwetsbaarheden en bedreigingen zijn:

- Foutieve implementatie van authenticatie en sessie management: hijacking van sessie management vormt een belangrijk probleem in veel webapplicaties.
- Foutieve implementatie van toegangsbeheer: onvoldoende controles op de acties die de gebruiker wil uitvoeren.
- Ongeautoriseerde directe objectreferenties: de mogelijkheid dat gebruikers door het aanpassen van object referenties (bijvoorbeeld een id in de URL) toegang krijgen tot de gegevens van andere gebruikers.
- Onveilige authenticatiemechanismen.
- Onveilige opslag van authenticatiegegevens.
- Discrepantie tussen authenticatiemechanisme en beveiligingsbeleid: te zware of te lichte authenticatie bij een webapplicatie.
- Het wiel opnieuw uitvinden: het steeds opnieuw zelf 'uitvinden' van authenticatie- en autorisatiemechanismen leidt tot het introduceren van kwetsbaarheden.
- Incompatibele authenticatiemechanismen: het niet kunnen integreren van verschillende authenticatiemechanismen kan leiden tot problemen op het gebied van Single Sign-On (SSO).

7.2 Doelstelling

Doelstelling is: 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.

7.3 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.	Beschrijving van beveiligingsrichtlijn	Doelstelling	Classificatie
B4-1	**Maak gebruik van Identity & Access Management tooling.**	• 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.	Midden
B4-2	**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).**	• Voorkom misbruik van een niet meer gebruikte sessie.	Hoog

HOOFDSTUK 8

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' is vooral sterk afhankelijk van de inrichting van identiteitbeheer (zie hoofdstuk 7 '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.

8.1 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:

- Lekken van informatie - het in handen komen van vertrouwelijke informatie bij ongeautoriseerde personen.
- Weerlegbaarheid - transacties zijn weerlegbaar op het moment dat een webapplicatie geen bewijs bijhoudt met betrekking tot de bron, het tijdstip, de ontvangst en de inhoud van een transactie.

Misbruik van certificaten en de gevolgen daarvan zijn:

- 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 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.

8.2 Doelstelling

Doelstelling is: Zorgen dat geen informatie wordt gelekt en dat onweerlegbaarheid wordt ondersteund.

8.3 Beveiligingsrichtlijnen

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

Nr.	Beschrijving van beveiligingsrichtlijn	Doelstelling	Classificatie
B5-1	**Voer sleutelbeheer in waarbij minimaal gegarandeerd wordt dat sleutels niet onversleuteld op de servers te vinden zijn.**	• Doelmatig gebruik van cryptografische technieken door het beheren van cryptografische sleutels.	Hoog
B5-2	**Maak gebruik van versleutelde (HTTPS) verbindingen.**	• Voorkom misbruik van (vertrouwelijke) gegevens die tijdens transport zijn onderschept.	Hoog
B5-3	**Sla gevoelige gegevens versleuteld of gehashed op.**	• Voorkom misbruik van opgeslagen vertrouwelijke gegevens.	Hoog
B5-4	**Versleutel cookies.**	• Voorkom dat kwaadwillende de inhoud van cookies kunnen inzien en/of aanpassen, zodat de vertrouwelijkheid en integriteit van de inhoud van het cookie wordt gewaarborgd.	Hoog
B5-5	**Maak gebruik van digitale handtekeningen.**	• Voorkom dat transacties weerlegd kunnen worden.	Midden
B5-6	**Zorg voor een extra set 'back-up' certificaten van een andere CA.**	• Voorkom (langdurige) disruptie van de dienstverlening door risicospreiding.	Laag
B5-7	**Tref maatregelen voor het patchen van systemen waarbij certificaten van de lijst met vertrouwde certificaten worden gehaald.**	• Voorkom (langdurige) disruptie van de dienstverlening door risicospreiding.	Laag

HOOFDSTUK 9

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 7 ‘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 beveiligingscomponent 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.

9.1 Doelstelling

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

9.2 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.	Beschrijving van beveiligingsrichtlijn	Doelstelling	Classificatie
B6-1	**Stel vast welke beveiligingsservices een component zal afnemen en aanbieden.**	• Zorgen voor een effectieve integratie van verschillende (netwerk) componenten.	Midden

HOOFDSTUK 10

Monitoring, auditing en alertering

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 gemonitoord, 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.

10.1 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:

- Ontbreken van toezicht - toezicht op gebeurtenissen in de webomgeving ontbreekt doordat geen logging wordt bijgehouden, juist te veel informatie wordt verzameld, er niet naar de logging wordt gekeken of gebeurtenissen niet aan elkaar gerelateerd kunnen worden
- Impact: onbekend - impact van een gebeurtenis op de hele webapplicatie keten is onbekend.
- Gebrek aan coördinatie en samenwerking - complexe gebeurtenissen kunnen nooit volledig geanalyseerd en gedetecteerd worden op het moment dat verschillende afdelingen binnen de organisatie als 'eilandjes' werken

10.2 Doelstelling

Doelstelling is: Het ontdekken van ongeautoriseerde activiteiten.

10.3 Beveiligingsrichtlijnen

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

Nr.	Beschrijving van beveiligingsrichtlijn	Doelstelling	Classificatie
B7-1	**Maak gebruik van Intrusion Detection Systemen (IDS).**	• Detecteren van aanvallen op webapplicaties.	Hoog
B7-2	**Breng logging op één punt samen.**	• Het efficiënt detecteren van aanvallen.	Midden
B7-3	**Breng correlaties aan.**	• Het efficiënt detecteren van aanvallen.	Midden
B7-4	**Synchroniseer de systeemklokken.**	• Het efficiënt detecteren van aanvallen.	Hoog
B7-5	**Bepaal wat te doen bij het uitvallen van loggingmechanismen.**	• Voorkom onopgemerkte aanvallen.	Hoog
B7-6	**Stel bewaartermijnen van logging vast.**	• Vaststellen van een bewaartermijn voor essentiële (bedrijfs)informatie.	Hoog
B7-7	**Beveilig logging tegen achteraf wijzigen.**	• Voorkom dat logfiles achteraf aangepast kunnen worden.	Hoog
B7-8	**Voer actief controles uit op logging.**	• Het detecteren van misbruik en inbraakpogingen.	Hoog
B7-9	**Governance, organisatie, rollen en bevoegdheden inzake preventie, detectie en response inzake informatiebeveiliging dienen adequaat te zijn vastgesteld.**	• Het managen van de informatiebeveiliging binnen de organisatie	Hoog

HOOFDSTUK 11

Informatiebeveiligings-beleid

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	-
Z	-

BIJLAGE B

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

Aanvalsmethode	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[29] en Vitriol[30].
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.
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'[31]-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'[32], 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-injectie	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.

29. HTTP://theinvisiblethings.blogspot.com/2006/06/introducing-blue-pill.html
30. HTTP://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Zovi.pdf
31. HTTP://people.csail.mit.edu/tromer/papers/cloudsec.pdf
32. HTTP://www.ece.cmu.edu/~dawnsong/papers/ssh-timing.pdf

BIJLAGE D

Samenvatting beveiligingsrichtlijnen

Nr.	Beschrijving van beveiligingsrichtlijn	Classificatie	Compliance[33]
Algemeen			
B0-1	Informatiebeveiliging is als een proces ingericht.	Hoog	
B0-2	Voer actief risicomanagement uit.	Hoog	
B0-3	Voor elke maatregel wordt documentatie vastgelegd en onderhouden.	Hoog	
B0-4	Alle ICT-componenten en -diensten inclusief de onderlinge relaties worden vastgelegd en dit overzicht wordt permanent onderhouden.	Hoog	
B0-5	Maak gebruik van een hardeningsproces, zodat alle ICT-componenten zijn gehard tegen aanvallen.	Hoog	
B0-6	Alle wijzigingen worden altijd eerst getest voordat deze in productie worden genomen en worden via wijzigingsbeheer doorgevoerd.	Hoog	
B0-7	De laatste (beveiligings)patches zijn geïnstalleerd en deze worden volgens een patchmanagement proces doorgevoerd.	Hoog	
B0-8	Penetratietests worden periodiek uitgevoerd.	Hoog	
B0-9	Vulnerability assessments (security scans) worden periodiek uitgevoerd.	Hoog	
B0-10	Policy compliance checks worden periodiek uitgevoerd.	Midden	
B0-11	Er moet een toereikend recovery proces zijn ingericht waar back-up en restore onderdeel vanuit maken.	Hoog	
B0-12	Ontwerp en richt maatregelen in met betrekking tot toegangs-beveiliging/toegangsbeheer.	Hoog	
B0-13	Niet (meer) gebruikte websites en/of informatie moet worden verwijderd.	Hoog	
B0-14	Leg afspraken met leveranciers vast in een overeenkomst.	Hoog	
Netwerkbeveiliging			
B1-1	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.	Hoog	
B1-2	Beheer- en productieverkeer zijn van elkaar gescheiden.	Hoog	
B1-3	Netwerktoegang tot de webapplicaties is voor alle gebruikersgroepen op een zelfde wijze ingeregeld.	Hoog	
B1-4	Netwerkcompartimenten bevatten geen fysieke koppelingen door middel van gedeelde componenten.	Hoog	
B1-5	Implementeer maatregelen tegen (d)DoS.	Midden	
B1-6	Implementeer maatregelen zodat het netwerk geen Single Points-of-Failure (SPOF) bevat.	Midden	
Platformbeveiliging			
B2-1	Maak gebruik van veilige beheermechanismen.	Hoog	
B2-2	Maak gebruik van beveiligingstemplates bij de beveiliging van systemen.	Midden	
B2-3	Maak gebruik van jailing (sandboxing).	Midden	
B2-4	Maak gebruik van lokale firewalls.	Midden	

33. Voor het aanduiden van de mate van compliance kan gebruik worden gemaakt van de volgende classificatieschema's:
    - Nee/Niet; Eerste aanzet; Halverwege; Voldoende; Goed; Niet van toepassing of Onbekend.
    - Nee/Niet; Gedeeltelijk; Ja/Goed; Niet van toepassing; of Onbekend.

Nr.	Beschrijving van beveiligingsrichtlijn	Classificatie	Compliance
Applicatiebeveiliging			
B3-1	De webapplicatie valideert de inhoud van een HTTP-request voor die wordt gebruikt.	Hoog	
B3-2	De webapplicatie controleert voor elk HTTP verzoek of de initiator geauthenticeerd is en de juiste autorisaties heeft.	Hoog	
B3-3	De webapplicatie normaliseert invoerdata voor validatie.	Hoog	
B3-4	De webapplicatie codeert dynamische onderdelen in de uitvoer.	Hoog	
B3-5	Voor het raadplegen en/of wijzigen van gegevens in de database gebruikt de webapplicatie alleen geparametriseerde queries.	Hoog	
B3-6	De webapplicatie valideert alle invoer, gegevens die aan de webapplicatie worden aangeboden, aan de serverzijde.	Hoog	
B3-7	De webapplicatie staat geen dynamische file includes toe of beperkt de keuze mogelijkheid (whitelisting).	Hoog	
B3-8	De webserver verstuurt alleen HTTP-headers die voor het functioneren van HTTP van belang zijn.	Hoog	
B3-9	De webserver toont alleen de hoogst noodzakelijke informatie in HTTP-headers die voor het functioneren van belang zijn.	Hoog	
B3-10	De webserver beperkt de informatie, bij het optreden van een fout, aan de gebruiker tot een minimum in een HTTP-response.	Hoog	
B3-11	Commentaarregels zijn uit de scripts (code) verwijderd.	Hoog	
B3-12	De webserver maakt alleen gebruik van de hoogst noodzakelijke HTTP-methoden.	Hoog	
B3-13	Directory-listings zijn uitgeschakeld.	Hoog	
B3-14	Voer een code review uit.	Midden	
B3-15	Een (geautomatiseerde) blackbox scan wordt periodiek uitgevoerd.	Hoog	
B3-16	Zet de cookie attributen ‘HttpOnly’ en ‘Secure’.	Hoog	
Identiteit- en toegangsbeheer			
B4-1	Maak gebruik van Identity & Access Management tooling.	Midden	
B4-2	Daar waar de gebruiker en/of beheerder kan inloggen op de web-applicatie is expliciete functionaliteit aanwezig om uit te loggen (het verbreken van de sessie).	Hoog	

Nr.	Beschrijving van beveiligingsrichtlijn	Classificatie	Compliance
Vertrouwelijkheid en onweerlegbaarheid			
B5-1	Voer sleutelbeheer in waarbij minimaal gegarandeerd wordt dat sleutels niet onversleuteld op de servers te vinden zijn.	Hoog	
B5-2	Maak gebruik van versleutelde (HTTPS) verbindingen.	Hoog	
B5-3	Sla gevoelige gegevens versleuteld of gehashed op.	Hoog	
B5-4	Versleutel cookies.	Hoog	
B5-5	Maak gebruik van digitale handtekeningen.	Midden	
B5-6	Zorg voor een extra set ‘back-up’ certificaten van een andere CA.	Laag	
B5-7	Tref maatregelen voor het patchen van systemen waarbij certificaten van de lijst met vertrouwde certificaten worden gehaald.	Laag	
Beveiligingsintegratie			
B6-1	Stel vast welke beveiligingsservices een component zal afnemen en aanbieden.	Midden	
Monitoring, auditing en alerting			
B7-1	Maak gebruik van Intrusion Detection Systemen (IDS).	Hoog	
B7-2	Breng logging op één punt samen.	Midden	
B7-3	Breng correlaties aan.	Midden	
B7-4	Synchroniseer de systeemklokken.	Hoog	
B7-5	Bepaal wat te doen bij het uitvallen van loggingmechanismen.	Hoog	
B7-6	Stel bewaartermijnen van logging vast.	Hoog	
B7-7	Beveilig logging tegen achteraf wijzigen.	Hoog	
B7-8	Voer actief controles uit op logging.	Hoog	
B7-9	Governance, organisatie, rollen en bevoegdheden inzake preventie, detectie en response inzake informatiebeveiliging dienen adequaat te zijn vastgesteld.	Hoog	

AANVULLINGEN / AANTEKENINGEN

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 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