Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

ICT-beveiligingsrichtlijnen voor webapplicaties

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.

De volgende partijen hebben in belangrijke mate bijgedragen aan de kwaliteit van deze beveiligingsrichtlijnen:

- Belastingdienst
- Centrum Informatiebeveiliging en Privacybescherming
- DICTU
- Dienst Publiek en Communicatie
- Logius
- Ministerie van Economische Zaken en Klimaat
- Nationaal Bureau Verbindingsbeveiliging
- NLnet Labs
- NOREA
- Platform Internetstandaarden
- Software Improvement Group

Inhoud

Inleiding

Vrijwel iedere organisatie gebruikt webapplicaties, zowel voor informatievoorziening als voor het ondersteunen van bedrijfsprocessen. Webapplicaties verwerken vaak persoonsgegevens of andere gevoelige informatie. De betrouwbaarheid van webapplicaties is daarom belangrijk voor het goed draaien van de organisatie. Goede beveiligingsmaatregelen dragen bij aan de betrouwbaarheid van de dienstverlening en bedrijfsvoering. Het veilig (laten) ontwikkelen van webapplicaties is een van die maatregelen. Het voorkomt digitale inbraken in uw systemen met ernstige gevolgen zoals ransomware en datalekken, en helpt uw organisatie om de digitale weerbaarheid te verhogen.

Dit is een handleiding om een veilige webapplicatie te maken

Deze beveiligingsrichtlijnen zijn concrete maatregelen die ontwikkelaars en beheerders kunnen uitvoeren om een veilige webapplicatie te maken. Iedere toepassing die via het Hypertext Transfer Protocol (http) bereikbaar is, is een webapplicatie. De functionaliteiten die een webapplicatie kan bieden zijn onbeperkt. De techniek is echter altijd gebaseerd op de http-standaard. In de hedendaagse praktijk, en ook conform de beveiligingsrichtlijnen, zal een webapplicatie via https zijn ontsloten, waarbij via hetzelfde protocol over een versleutelde verbinding wordt gecommuniceerd.

Dit document beschouwt ook de bijbehorende infrastructuur, het koppelvlak met internet, de opslag van de gegevens en de netwerkservices als aandachtsgebied.

Omdat een webapplicatie door verschillende afdelingen of partijen kan worden ontwikkeld zijn de beveiligingsrichtlijnen onderverdeeld in vier uitvoeringsdomeinen die overeenkomen met de traditionele taakverdeling. Afhankelijk van uw situatie kunt u delen aan de juiste uitvoerende verstrekken.

- Toegangsvoorzieningsmiddelen (functioneel beheer, ontwikkelaar, DevOps-engineers, SaaS-leverancier)
- Webapplicaties (ontwikkelaar, DevOps-engineers, SaaS-leverancier)
- Platformen en webservers (systeembeheer, DevOps-engineers, SaaS/PaaS-leverancier)
- Netwerken (netwerkbeheer, SaaS/PaaS/IaaS-leverancier)

In het geval van een web-api kan de clientapplicatie een mobiele app zijn. Hiervoor heeft het NCSC aparte richtlijnen uitgegeven die ingaan op dat uitvoeringsdomein, die samen met deze kunnen worden toegepast.

Deze beveiligingsrichtlijnen staan niet op zichzelf. Naast de uitvoeringsrichtlijnen is het even belangrijk voor veilige software-ontwikkeling om een beveiligingsbeleid te hebben, en beheersingsmaatregelen te nemen. Beleids- en beheersingsrichtlijnen voor de ontwikkeling van veilige software zijn in een aparte uitgave van het NCSC verschenen. In dit document wordt verwezen naar richtlijnen in het beleidsdomein met B., en het beheersingsdomein (control) met C.

[1] NCSC, “Beleids- en beheersingsrichtlijnen voor de ontwikkeling van veilige software,” [Online]. Available: https://www.ncsc.nl/preventieve-beveiligingsmaatregelen/beleids-en-beheersingsrichtlijnen-voor-de-ontwikkeling-van-veilige-software

U bent maker, opdrachtgever, tester of auditor van een webapplicatie

U kunt deze richtlijnen toepassen vanuit verschillende rollen:

- U bent een securitymanager of systeemeigenaar die verantwoordelijk is voor de beveiligingskaders en de controle op naleving ervan. U kunt deze richtlijnen als normenkader opleggen aan de ontwikkelaars en beheerders.
- U bent zelf betrokken bij de ontwikkeling, implementatie of beheer van webapplicaties. U kunt deze richtlijnen als normenkader opgelegd krijgen vanuit uw eigen organisatie of een externe opdrachtgever.
- U bent een auditor of securitytester en hebt als opdracht gekregen om te toetsen of een webapplicatie aan deze richtlijnen voldoet.

U kunt zelf de prioriteit van beveiligingsrichtlijnen afwegen

De prioriteit van elke beveiligingsrichtlijn 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, Midden een redelijk sterke mate van gewenstheid is en Laag een gewenste, maar niet noodzakelijke voorwaarde vormt. De drie waarden zijn moeilijk exact te definiëren, maar vormen een functie van kans op optreden van een bedreiging en de mogelijke schade als gevolg hiervan.

De uiteindelijke afweging voor een specifieke webapplicatie voor een specifieke organisatie is afhankelijk van de weging van risico's die uit een risicoanalyse naar voren komen. Daarbij kunt u kijken naar de kans op optreden van een bedreiging, het te verdedigen belang en de mogelijke impact hiervan op de bedrijfsvoering.

De prioritering kan ook door uw opdrachtgever zijn bepaald.

U past de richtlijnen toe in een context van andere normen

Richt de processen en omgeving in uw organisatie in volgens een algemene beveiligingsopzet, bijvoorbeeld de ISO 27002 of de Baseline Informatiebeveiliging Overheid (BIO). Wanneer overkoepelende standaarden algemeen blijven kunnen de richtlijnen helpen om specifiek webapplicaties te beveiligen. Zo geeft u concrete invulling aan eisen van uw opdrachtgever, organisatiebrede normen of wetgeving.

De relatie met andere standaarden wordt gelegd via verwijzingen naar het Open Common Requirement Enumeration (OpenCRE)-platform.[2] Hier worden beveiligingsmaatregelen van verschillende standaarden aan elkaar gekoppeld en bijgehouden via een zogenaamde 'Common requirement': een onderwerp met een enkelvoudige identificatie. Met OpenCRE kunt u doorklikken naar die standaarden en ook navigeren naar gerelateerde onderwerpen, zoals hoe requirements kunnen worden getest en de details van technische maatregelen. OpenCRE kan u daarnaasthelpen met het vaststellen van de overeenkomst tussen standaarden die door verschillende opdrachtgevers kunnen worden opgelegd.

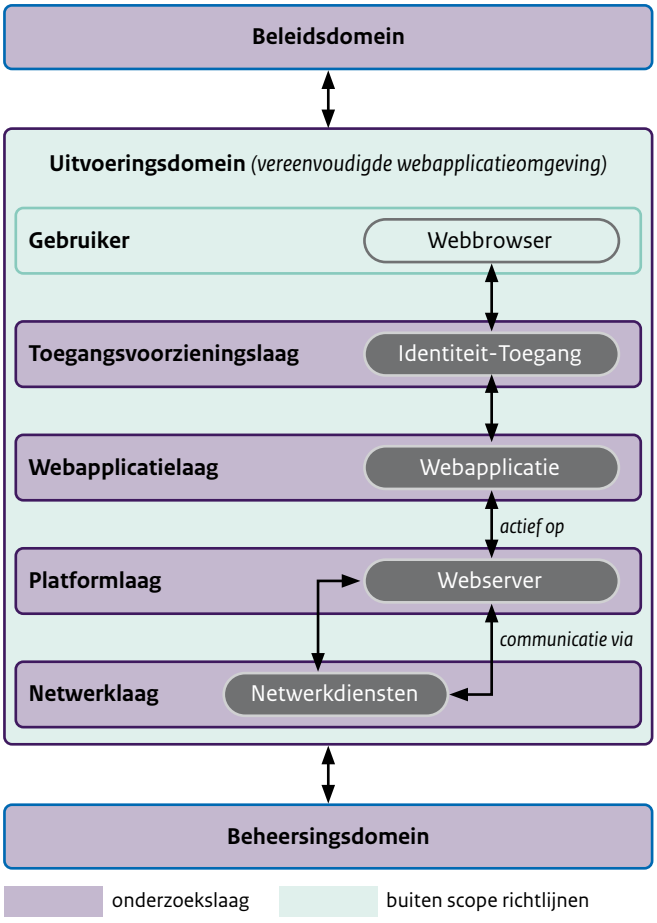
Deze richtlijnen zijn primair technisch van aard. Dit betekent dat een aantal aspecten van informatiebeveiliging geen onderdeel uitmaakt van het raamwerk dat in deze richtlijnen wordt gehanteerd. Dit document besteedt geen aandacht aan zaken als beveiligingsorganisatie, fysieke beveiliging en personeel.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

De richtlijnen zijn opgebouwd volgens het SIVA-raamwerk

De opbouw en formulering van deze richtlijnen is gebaseerd op het SIVA-raamwerk.[3] Dit raamwerk helpt bij het systematisch in kaart brengen van auditobjecten en de beschrijving van richtlijnen voor de in kaart gebrachte auditobjecten. Daarnaast zorgt het voor een betere verbinding van beleid, uitvoering en beheersing van de te nemen maatregelen.

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

Het gehele stelsel beveiligingsrichtlijnen van het NCSC is georganiseerd in drie domeinen: beleidsdomein, uitvoeringsdomein en control- of beheersingsdomein. Deze indeling komt voort uit het SIVA-raamwerk. Dit document behandelt het uitvoeringsdomein. Figuur 1 geeft de indeling van de richtlijnen in de context van een webapplicatie.



Figuur 1. Indeling van de beveiligingsrichtlijnen volgens het SIVA-raamwerk

2 Zie ook: https://opencre.org/

3 Voor achtergronden en de wetenschappelijke basis van het SIVA-raamwerk wordt verwezen naar Tewarie, W. N. B. (2014). SIVA: methodiek voor de ontwikkeling van auditreferentiekaders. VU University Press.

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

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

Beheersingsdomein
Evaluatieaspecten en meetaspecten zijn in dit domein opgenomen. Daarnaast treffen we hier ook de beheerprocessen aan, die noodzakelijk zijn voor de instandhouding van ICT-diensten. De informatie uit de evaluaties en de beheerprocessen is niet alleen gericht op het bijsturen van de geïmplementeerde webapplicaties, maar ook om het bijsturen en/of aanpassen van de eerder geformuleerde conditionele elementen die gebaseerd zijn op "onzekere" informatie en aannames, visie en uitgestippeld beleid.

Een voorbeeld van een dergelijke aanname is een inschatting van de capaciteitsbehoefte. In de praktijk kan (en zal) het gebruik anders zijn dan oorspronkelijk verondersteld. Dan is een mechanisme nodig dat de daadwerkelijke belasting meet en een proces waarin eventueel noodzakelijke veranderingen worden vastgesteld en doorgevoerd.

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

Beschrijving van de richtlijnen (Vorm)
De richtlijnen kennen een doelstelling en een risico. Hiermee is vastgelegd wat de richtlijn inhoudt en waarom deze gesteld wordt. Vervolgens worden per conformiteitsindicator uit de richtlijn (de onderstreepte trefwoorden) de maatregelen gegeven waarmee kan worden bereikt of vastgesteld dat invulling is gegeven aan de richtlijn. De conformiteitsindicatoren worden nader gedefinieerd in bijlage A.

Waar noodzakelijk zijn maatregelen voorzien van een nadere toelichting (cursief gedrukt). Bij sommige richtlijnen is een verdiepende tekst bijgevoegd die dieper ingaat op de mogelijke invulling van bepaalde maatregelen.

Met nadruk wordt gesteld dat de beschreven doelstellingen mogelijk ook met een (deels) andere invulling bereikt kunnen worden dan door de uitwerking die in deze richtlijnen bij de maatregelen wordt aangegeven. De beschreven maatregelen zijn een handreiking aan opdrachtgevers, technici en auditors. Zij zullen zelf de eindafweging moeten maken en deze verantwoorden. Voor het verantwoorden kunnen zij dan verwijzen naar de criteria en doelstellingen, met een beschrijving hoe hieraan op andere wijze invulling is gegeven.

Het NCSC zorgt ervoor dat de richtlijnen actueel zijn
Het NCSC is verantwoordelijk voor het opstellen en onderhouden van deze richtlijnen en zal ze periodiek actualiseren. Indien noodzakelijk zal het NCSC tussentijds door middel van een addendum of erratum de richtlijnen aanpassen.

Heeft u aanvullingen op, opmerkingen over of eigen ervaringen met deze Richtlijnen? Het NCSC ontvangt ze graag via info@ncsc.nl.

Uitvoeringsdomein

Het doel is een betrouwbare en veilige dienstverlening

Een organisatie wil een betrouwbare dienstverlening die ondersteund wordt door ICT-middelen die op alle lagen even betrouwbaar is. Om de betrouwbaarheid te bepalen moet worden vastgesteld of de ICT-middelen veilig zijn ingericht.

Het uitvoeringsdomein bevat richtlijnen voor specifieke ICT-lagen

In dit domein zijn richtlijnen opgenomen voor de specifieke ICT-lagen die gerelateerd zijn aan specifieke ICT-diensten. Alle richtlijnen zijn leidend voor de invulling van deze ICT-lagen, zoals het informatiebeveiligingsbeleid, cryptografiebeleid, etc. Alle afzonderlijke ICT-lagen samen bieden veilige diensten aan de organisatie en haar klanten. De specifieke diensten vormen schakels in de keten. Onder het motto “de keten is net zo sterk als de zwakste schakel” wordt er aandacht besteed aan alle specifieke ICT-diensten. Deze specifieke diensten worden in onderlinge samenhang bezien, en per specifieke ICT-dienst vanuit een bepaalde invalshoek. Deze invalshoeken zijn gerelateerd aan de volgende onderwerpen:

- operationeel beleid per specifieke dienst;
- processen, taken en verantwoordelijkheden;
- relaties en afhankelijkheden (tussen diverse typen medewerkers, systemen onderling en communicatie over en weer tussen medewerkers en systemen);
- organisatiestructuur en architectuur.

Dit domein is opgesplitst naar verschillende ICT-lagen

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

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

De betrokken maatregelen zullen binnen de specifieke lagen worden uitgewerkt.

Toegangsvoorzienings-middelen

Het doel is toegang verlenen volgens het beleid

De doelstelling van de laag toegangsvoorzieningsmiddelen is om te waarborgen dat de toegang tot objecten als data, webapplicaties, computerapparatuur en netwerken ingericht is volgens specifieke beleidsuitgangspunten van de organisatie. De werking voldoet aan de eisen die door de organisatie zijn gesteld ten aanzien van de kwaliteitsaspecten vertrouwelijkheid, integriteit, beschikbaarheid en controleerbaarheid van deze objecten.[4]

Toegangsvoorziening bestaat uit identiteitbeheer en toegangsbeheer

Toegangsvoorziening bestaat uit twee hoofdcomponenten: identiteitbeheer en toegangsbeheer. Identiteitbeheer en toegangsbeheer zijn onlosmakelijk met elkaar verbonden. Toegangsbeheer is vrijwel betekenisloos wanneer geen correcte invulling is gegeven aan identiteitbeheer. In deze richtlijnen worden deze twee lagen daarom gezamenlijk behandeld.

Binnen het authenticatieproces wordt ervoor gezorgd dat alleen onder vooraf vastgestelde voorwaarden de identiteit van een gebruiker of systeem wordt geregistreerd en autorisaties worden verleend. Binnen de technische realisatie van de toegangsvoor-zieningen worden identiteiten gecontroleerd, geregistreerd en beschikbaar gesteld aan de ICT-omgeving.

Onder identiteitbeheer vallen alle activiteiten die nodig zijn in het kader van identiteiten. Het gaat hierbij om het beheer van identiteiten: het toevoegen, verwijderen en wijzigen van identiteiten, maar zeker ook het authenticeren van identiteiten op basis van hun authenticator. Een identiteit bestaat uit een identifier, een authenticator en een gebruikersprofiel (alle informatie van de gekoppelde gebruiker).

Toegangsbeheer heeft als doel om gebruikers op een efficiënte manier te voorzien van de juiste autorisaties, op basis van 'least privilege', 'need-to-know' of 'need-to-access'. Toegangsbeheer betreft alle activiteiten die webapplicaties moeten uitvoeren om de autorisaties voor webapplicaties in te regelen en af te dwingen, zoals het in runtime verifiëren van autorisaties op basis van een autorisatietabel: mag een gebruiker wel of geen gebruik maken van (delen van) de webapplicatie.

Onjuiste toegangsvoorziening leidt tot toegang door onbevoegden

Door het ontbreken van adequate toegangsbeveiliging tot (web) applicaties, systemen en netwerken bestaat het risico dat onbevoegden zich toegang kunnen verschaffen tot deze objecten, waardoor ongewenste acties op de services kunnen plaatsvinden en informatie kan worden gestolen of gewijzigd.

Identiteiten zijn gevoelige persoonsgegevens. Wanneer een systeem onvoldoende bescherming biedt tegen misbruik of diefstal kan dit leiden tot identiteitsfraude (binnen het systeem of elders met misbruik van identiteiten uit het systeem).

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

U/TV.01 Toegangsvoorzieningsmiddelen

Als het ontwerp met betrekking tot identiteit- en toegangsbeheer is vastgesteld, kan worden bepaald waar het toegangsvoorzieningsmiddel, zogeheten identiteit- en toegangsmanagement (IAM)-tooling, wordt ingezet.

Het is mogelijk om delen van identiteit- en toegangsbeheer buiten webapplicatie(s) te plaatsen (te centraliseren). Het inzetten van tooling vermindert de complexiteit van webapplicaties omdat het authenticeren en autoriseren van gebruikers los wordt gekoppeld van de webapplicatie. Door de authenticatie los te koppelen van de webapplicatie, is het eenvoudiger om in de toekomst andere authenticatoren in te zetten voor het beveiligen van de webapplicatie. Hiervoor worden wijzigingen doorgevoerd in de tooling en hoeft de achterliggende webapplicatie hier in principe niets van te merken.

U/TV.01 Toegangsvoorzieningsmiddelen inzetten	
Richtlijn (wie en wat)	De inzet van identiteit- en toegangsmiddelen levert betrouwbare en effectieve mechanismen voor het vastleggen en vaststellen van de identiteit van de wederpartij, het toekennen van de rechten aan de wederpartij, het controleerbaar maken van het gebruik van deze middelen en het automatiseren van arbeidsintensieve taken.
Doelstelling (waarom)	Het efficiënter maken van het identiteit- en toegangsbeheer en zorgen dat functies en gegevens uitsluitend beschikbaar worden gesteld aan diegenen waarvoor deze bedoeld zijn als waarborg voor vertrouwelijkheid en integriteit.
Risico	Gegevens worden ingezien, gewijzigd of verwijderd door individuen die hiervoor (vanuit de organisatie) geen toestemming, recht of opdracht hebben.
Classificatie	Hoog
Verwijzingen	CRE 270-568 Authenticatiemechanisme CRE 247-250 Toegangscontroleprocessen CRE 724-770 Technische toegangscontrole CRE 586-842 Veilig gebruikersmanagement

Maatregelen

vastleggen van de identiteit

01 Ondersteun de initiële vaststelling en vastlegging van de identiteit van de wederpartij met het toegangsvoorzieningsmiddel.
In het toegangsvoorzieningsbeleid is vastgelegd met welke mate van zekerheid de identiteit van een natuurlijke persoon moet worden vastgesteld om deze als wederpartij (gebruiker) te mogen registreren.

02 Bied adequate bescherming van de vastgelegde gebruikers- en toegangsgegevens met het toegangsvoorzieningsmiddel.
Sla wachtwoorden altijd vercijferd op.[5] Motiveer de keuze voor het hashingalgoritme en de configuratie daarvan, zoals het aantal iteraties en de bron van de salts, in de ontwerpdocumentatie.
Sla nooit biometrische informatie op de server op. Pas biometrische authenticatie toe door het authenticatiemiddel van de gebruiker de biometrie af te laten handelen en sla op de server uitsluitend publieke sleutels voor het vaststellen van digitale handtekeningen op.

vaststellen van de identiteit (authenticatie)

03 Stel de identiteit van natuurlijke personen of andere clientsystemen vast met het authenticatiemiddel.
In het beleid is vastgelegd met welke mate van zekerheid de identiteit moet worden vastgesteld om van een geslaagde authenticatie te mogen spreken. Dit zal in de regel tot uiting komen in de keuze van (een combinatie van) authenticatiemiddelen. Het gebruik van alleen een wachtwoord als authenticatiemiddel is onvoldoende. Gebruik bij voorkeur wachtwoordloze authenticatie zoals passkeys volgens de FIDO2-standaard.
Het is mogelijk verschillende authenticatiemiddelen te accepteren, die ieder een eigen mate van zekerheid kennen. Dit kan van toepassing zijn wanneer er onderscheid wordt gemaakt tussen accounts met een normaal en hoog risiconiveau. De bijbehorende autorisaties zijn gekoppeld aan het gebruikte authenticatiemiddel.

04 Ondersteun het authenticatiebeleid met het authenticatiemiddel.
Waar de webapplicatie nog van wachtwoorden gebruikmaakt, worden de regels uit het wachtwoordbeleid afgedwongen door geprogrammeerde controles.

toekennen van de rechten (autorisatie)

05 Wijs rechten toe op basis van het toegangsvoorzieningsbeleid.

06 Houd een actueel overzicht bij van accounts en de personen die daar gebruik van maken:
- service-accounts;
- beheeraccounts;
- gebruikersaccounts;
- (web)applicatie-accounts.

07 Trek de rechten direct in en blokkeer direct het account wanneer een gebruiker geen recht op toegang meer heeft.
Dit gebeurt bijvoorbeeld door uitdiensttreding of functiewijziging.

5 Zie voor afwegingen ten aanzien van de te kiezen algoritmes de OWASP Password Storage Cheat Sheet: https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html

Maatregelen	
08	Voer periodiek een audit uit om vast te stellen of de aanwezige accounts en bijbehorende autorisaties overeenkomen met het personeels- of gebruikersbestand. *De frequentie kan, afhankelijk van het aantal gebruikers en het gemiddelde verloop, bijvoorbeeld elk kwartaal of elk halfjaar zijn. Leg de gekozen frequentie vast in het toegangsvoorzieningsbeleid.*
controleerbaar maken van het gebruik	
09	Registreer het beheren en onderhouden van identiteiten en autorisatie onweerlegbaar. *Het toegangssysteem en ondersteunde systemen maken gebruik van mechanismen om activiteiten vast te leggen (loggen).*
10	Registreer het verkrijgen van autorisatie en het gebruik van functionaliteit onweerlegbaar. *Hierbij worden minimaal het tijdstip, de gebruiker, waar toegang vandaan wordt opgevraagd en waar toegang toe wordt geautoriseerd vastgelegd.*
automatiseren van arbeidsintensieve taken	
11	Ondersteun met het ingezette identiteits- en toegangs-managementtool conform het toegangsvoorzieningsbeleid de complete levenscyclus van identiteiten en autorisaties: • aanvragen; • toekennen; • wijzigen; • intrekken/schorsen/verwijderen; • conform voorgeschreven procedures.

Webapplicaties

Het doel is een betrouwbare, veilige webapplicatie volgens het beleid

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

Webapplicaties bevatten vaak kwetsbaarheden door programmeerfouten

Veel van de bekendste kwetsbaarheden in webapplicaties, zoals cross-site scripting (XSS) en SQL-injectie, vinden hun oorsprong in fouten tijdens het ontwikkelen van software. Dit hoofdstuk besteedt aandacht aan maatregelen op het gebied van software-ontwikkeling die de aanwezigheid van deze kwetsbaarheden grotendeels voorkomen en de kans op schade door de aanwezigheid van ernstige kwetsbaarheden in webapplicaties reduceren.

Een niet goed beveiligde webapplicatie leidt tot gemanipuleerde informatie

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

De beveiligingsrichtlijnen zijn onderverdeeld

Binnen de laag Webapplicaties worden onderstaande richtlijnen beschreven en per richtlijn worden conformiteitsindicatoren en de betreffende maatregelen uitgewerkt.

- Operationeel beleid voor webapplicatie (U/WA.01)
- Webapplicatiebeheer (U/WA.02)
- Webapplicatie-invoer U/WA.03)
- Webapplicatie-uitvoer (U/WA.04)
- Vertrouwelijkheid van gegevens (U/WA.05)
- Webapplicatie-informatie (U/WA.06)
- Webapplicatie-integratie (U/WA.07)
- Webapplicatiesessie (U/WA.08)
- Webapplicatiearchitectuur (U/WA.09)

U/WA.01 Operationeel beleid voor webapplicaties

Het operationeel beleid voor webapplicaties beschrijft de manier waarop de organisatie omgaat met het inrichten en beschikbaar stellen van webapplicaties. Het operationeel beleid is een concretere uitwerking van het bovenliggende beleid. Een solide operationeel beleid is daarom een randvoorwaarde voor een veilige inrichting van een webapplicatie-omgeving.

U/WA.01 Operationeel beleid voor webapplicaties formuleren	
Richtlijn (wie en wat)	Het operationeel beleid voor webapplicaties bevat richtlijnen en instructies en procedures met betrekking tot ontwikkeling, onderhoud en uitfasering van webapplicaties.
Doelstelling (waarom)	De ontwikkeling van de webapplicatie optimaal ondersteunen en de klant betrouwbare diensten bieden.
Risico	Geen eenduidige richting voor webapplicaties, waardoor de beveiliging van de webapplicatie los staat van zijn omgeving. Dit verhoogt de kans op beveiligingsincidenten.
Classificatie	Midden
Verwijzingen	CRE 571-271 (Programmamanagement) CRE 616-305 (Security in het ontwikkelproces) CRE 787-638 (Technische instructies) CRE 862-452 (Operationele beveiligingsprocessen)

Maatregelen

richtlijnen

01 Stel richtlijnen op voor:
- ontwikkeling, onderhoud en uitfasering van webapplicaties;
- beveiliging van webapplicaties;
- verwerking van gegevens;
- koppelingen met onderliggende systemen;
- koppelingen met achterliggende systemen.

Gebruik bij de ontwikkeling van webapplicaties methodes voor Secure Software Development.[8]
Onderliggende systemen zijn alle elementen uit de hardware/software stack waarop de webapplicatie draait.
Achterliggende systemen zijn systemen die direct of indirect door de webapplicatie ontsloten of bereikt worden.

instructies en procedures

02 Stel instructies en procedures op voor:
- het werken met gescheiden ontwikkel-, test-, acceptatie- en productie-omgevingen (OTAP);
- contentmanagement.

Besteed aandacht aan het regelmatig evalueren en bijstellen van de richtlijnen.
Indien deze instructies en procedures ruimte bieden om af te wijken van de richtlijn, dient hieraan de vereiste van 'pas toe of leg uit' gekoppeld te zijn.

U/WA.02 Webapplicatiebeheer

Het (dagelijks) beheer van een webapplicatie draagt zorg voor het handhaven van alle getroffen maatregelen. Daarmee levert het een belangrijke bijdrage aan de continue beleidscompliance van de webapplicatie en is dus een stabiliserende factor.

U/WA.02 Webapplicatiebeheer inrichten

Richtlijn (wie en wat)	Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten.
Doelstelling (waarom)	Effectief en veilig realiseren van de dienstverlening.
Risico	Ongecontroleerde wijzigingen waarvan niet bekend is wie daarvoor verantwoordelijk is.
Classificatie	Midden
Verwijzingen	CRE 004-517 (Securityrequirements) CRE 862-452 (Operationele beveiligingsprocessen) CRE 247-250 (Toegangscontroleprocessen) CRE 724-770 (Technische toegangscontrole)

Maatregelen

procesmatig en procedureel

01 Voer beheerwerkzaamheden uit volgens afgesproken richtlijnen en procedures.
Hier gaat het er vooral om dat er zicht is op de vooraf bekende werkzaamheden en hoe deze worden uitgevoerd. Het reageren op en afhandelen van incidenten valt hier nadrukkelijk ook onder, hoewel voor het oplossen van beveiligingsincidenten natuurlijk geen standaardrecept te geven is.

02 Laat leidinggevenden en systeemeigenaren vooraf criteria vastleggen waaraan de operationele webapplicatie moet voldoen.
Bewaking van de criteria zal deels het werk van de webapplicatiebeheerders zijn, deels onder monitoring (C.07 [1]) vallen. De exacte verdeling verschilt per webapplicatie.

geautoriseerd

03 Voorkom dat hiertoe niet geautoriseerde gebruikers toegang krijgen tot beheerfuncties binnen de applicatie.

functieprofielen

04 Op basis van taken, verantwoordelijkheden en bevoegdheden zijn de verschillende beheerrollen geïdentificeerd.
Naast de diverse inhoudelijke taakgebieden is hierin expliciet aandacht voor ongewenste combinaties van bevoegdheden. Deze zijn in verschillende rollen ondergebracht (functiescheiding, zie ook U/TV.01/05 en U/TV.01/06).

8 Zie voor diverse handreikingen daarvoor de website van het Centrum voor Informatiebeveiliging en Privacybescherming: https://cip-overheid.nl/productcategorie%C3%ABn-en-workshops/producten/secure-software/

Maatregelen	
05	Vul in de autorisatiematrix in: • aan welke rollen welke bevoegdheden worden toegekend; • hoe functiescheiding tot uitdrukking komt. *De functiescheiding geeft bijvoorbeeld aan dat één enkele beheerder niet in staat is – direct of indirect – volledige controle over alle functies te verwerven.*
06	Richt een proces in voor het definiëren en onderhouden van de rollen. *Dit proces is afgestemd met de primaire bedrijfsprocessen.*

U/WA.03 Webapplicatie-invoer

Ongecontroleerde (ongevalideerde) invoer door gebruikers is een belangrijke dreiging voor een webapplicatie. Als invoer van gebruikers rechtstreeks wordt gebruikt in HTML-uitvoer, cookie-waarden, SQL-query's, etc. bestaat er een (grote) kans dat een kwaadwillende de webapplicatie compromitteert. Een gebrek aan invoervalidatie kan tot kwetsbaarheden zoals cross-site scripting, commando- en SQL-injectie leiden.

De belangrijkste vuistregel voor invoer in een webapplicatie is dat de applicatie geen enkele invoer mag vertrouwen en daarom moet valideren. Alle invoer moet daarom voor verwerking door de webapplicatie worden gevalideerd op juistheid, volledigheid en geldigheid. Invoervalidatie is de doorslaggevende voorwaarde voor betrouwbare gegevensverwerking en ongeldige invoer wordt door de webapplicatie geweigerd.

De richtlijnen voor invoerbehandeling zijn van toepassing voor alle invoer die van buiten de webapplicatie komt. Dus niet alleen (eind) gebruikers, maar ook externe systemen en applicaties.

Er geldt een aantal uitgangspunten met betrekking tot invoer bij het ontwikkelen van webapplicaties, deze zijn:
- De client (gebruiker of externe applicatie) is niet te vertrouwen en dus de invoer die hier vandaan komt ook niet.
- De invoer wordt voor valideren eerst genormaliseerd.
- De invoer die niet aan één of meerdere controles voldoet wordt verwijderd of geweigerd.

In het ontwikkelproces van de webapplicatie zal de software expliciet op een correcte invulling van deze uitgangspunten onderzocht moeten worden. Dit vraagt om uitgebreide testen of gerichte codereviews.

Invoercontrole kan streng worden toegepast op invoer waarvan de vorm en inhoud gestandaardiseerd zijn, zoals een datum, postcode of IBAN. Deze kunnen zowel syntactisch (volgens het gestandaardiseerde formaat) als semantisch (bijvoorbeeld: is een geboortedatum van een levende persoon niet langer dan 150 jaar geleden) worden gecontroleerd.

Bij vrije tekstvelden is het formaat niet controleerbaar, maar kan de tekenset worden beperkt tot bijvoorbeeld alleen (Latijnse) letters, cijfers en bepaalde te verwachten leestekens.[9]

9 Zie voor meer informatie over invoercontroles de OWASP Input Validation Cheat Sheet: https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html

U/WA.03 Webapplicatie-invoer beperken	
Richtlijn (wie en wat)	De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en daarna te valideren, voordat deze invoer wordt verwerkt.
Doelstelling (waarom)	Voorkom (on)opzettelijke manipulatie van de webapplicatie, waardoor de vertrouwelijkheid, integriteit en/of beschikbaarheid van de webapplicatie aangetast worden.
Risico	Inzage, wijziging, verlies, of misbruik van gegevens door bijvoorbeeld manipulatie van de webapplicatie-logica.
Classificatie	Hoog
Verwijzingen	CRE 503-455 (Invoer en uitvoerbescherming)

Maatregelen

manipulatie

01 Valideer de invoer op de server.
Uitgebreide testen kunnen aannemelijk maken dat invoercontroles niet te omzeilen zijn. Het gebruik van in de praktijk bewezen opensourcelibrary's kan een hogere mate van zekerheid bieden.

02 Verbied of beperk het gebruik van dynamische file includes.
Wanneer kwaadwillenden via malafide invoer willekeurige bestanden kunnen verwerken in de webapplicatie, bestaat de mogelijkheid dat willekeurige webapplicatiecode wordt uitgevoerd op de server. Hiermee is het bijvoorbeeld mogelijk om ongeautoriseerd de database op een server te benaderen.

normaliseren

03 Converteer alle toegestane invoer naar een veilige codering, waarbij risicovolle tekens uit de invoer worden omgezet naar een gecodeerd teken.

valideren

04 Weiger foute, ongeldige of verboden invoer.

Verdieping

Bij normalisatie worden alle tekens eerst controleerbaar gemaakt

Invoer moet eerst worden genormaliseerd voordat deze door de webapplicatie wordt gevalideerd. Hierdoor wordt voorkomen dat malafide verzoeken niet door de filtermechanismen van de webapplicatie worden herkend. Normalisatie staat ook wel bekend als anti-evasion[10] of canonicalization[11].

Kies voor een coderingsschema om alle invoer in te coderen zodat de invoervalidatie in diezelfde codering alle ongeldige tekens kan herkennen.

Tekens uit de invoer die verwerkbaar en niet ongewenst zijn kunnen nog steeds risicovol zijn bij het gebruik hiervan binnen de programmalogica. Om problemen hiermee te voorkomen moeten deze tekens onschadelijk worden gemaakt.

Risicovolle tekens kunnen onderdeel uitmaken van legitieme invoer. In onderstaand voorbeeld wordt een SQL-query onveilig opgebouwd waarbij de plaatsnaam ('s-Gravenhage) tot een syntactisch incorrecte query leidt:

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

Door een escape voor de apostrof te plaatsen, beschouwt de database de apostrof als onderdeel van de invoer en niet als onderdeel van de query. Overigens zorgt het gebruik van prepared statements ervoor dat invoer binnen SQL-query's automatisch worden geëscapet.

Voer escaping uit op de invoer na het toepassen van invoer-validatie. Escaping is toegespitst op de programmaonderdelen waar invoer wordt verwerkt.

Bij validatie wordt invoer gecontroleerd of het aan de verwachting voldoet

Valideer alle ontvangen invoer. De verdeling van validaties tussen de webserver en de webapplicatie is afhankelijk van de webserver waarmee de webapplicatie samenwerkt (zie ook U/PW.02).

De volgende onderdelen van een http-request worden minimaal gevalideerd voordat het request wordt verwerkt:
- URL's;
- cookies;
- http-headers;
- variabelen die de client in de URI van een GET-request doorgeeft;
- variabelen die de client via de body in een POST-request doorgeeft;

10 https://www.owasp.org/index.php/Virtual_Patching_Best_Practices#Anti-Evasion_Capabilities
11 https://www.owasp.org/index.php/Canonicalization,_locale_and_Unicode

- api's en formats die daarin gebruikt kunnen worden (XML, SOAP, JSON);
- bestanden.

De inhoud van alle onderdelen van een http-request wordt gevalideerd op basis van verwerkbare invoer. De validatie wordt uitgevoerd op:
- type (bijvoorbeeld string of integer);
- lengte;
- formaat (bijvoorbeeld een reguliere expressie);
- tekens (bijvoorbeeld alleen 'A-Z' en 'a-z').

De inhoud van http-requests kan ook op basis van expliciet bekende verwerkbare invoer gevalideerd worden, om te voorkomen dat malafide inhoud het mogelijk maakt om de applicatielogica te beïnvloeden.

Voldoet de invoer niet aan één of meerdere van bovenstaande controles, dan wordt de invoer geweigerd.

De inhoud van alle onderdelen van een http-request wordt gevalideerd op basis van ongewenste invoer.

Als het moeilijk is om op basis van alleen toegestane tekens (allow-listing) alle mogelijke malafide invoer uit te filteren, dan kan de invoer aanvullend worden gevalideerd op malafide tekens en patronen (deny-listing). Denk aan invoervelden waar de gebruiker vrije tekst kan invoeren.

De webapplicatie filtert de invoer op basis van:
- Malafide tekens (bijvoorbeeld '' of '"')
- Malafide patronen (bijvoorbeeld '/**/' of '..\..\')

De filtering is toegespitst op de programmaonderdelen waarin de invoer wordt verwerkt. Bij het gebruik van invoer voor het samenstellen van een databasequery zijn andere filters vereist dan voor het samenstellen van een LDAP-query.

In het geval de invoer één of meerdere sleutelwoorden, tekens of patronen van de deny-list bevat, dan wordt de invoer geweigerd.

Voor andere protocollen dan http gelden soortgelijke controles. Denk ook aan interne consistentie, zoals geldige scheiders voor bijlagen in e-mail.

U/WA.04 Webapplicatie-uitvoer

Naast het ontbreken van validatie van invoer ontbreekt het bij sommige webapplicaties ook aan de validatie van uitvoer. Als een webapplicatie onvoldoende controles uitvoert op de uitvoer die het terugstuurt naar de gebruiker, kan het gebeuren dat er zich onbedoelde of ongewenste inhoud in de uitvoer bevindt.

Uitvoervalidatie voorkomt dat de webapplicatie ongewenste opdrachten geeft aan de client, bijvoorbeeld in het geval van cross-site scripting. Implementeer uitvoervalidatie door het coderen van alle dynamische inhoud van een webpagina. Veel webpagina's bevatten naast statische ook dynamische informatie. Deze dynamische informatie kan bijvoorbeeld afkomstig zijn uit databases of externe bronnen maar kan ook gebaseerd zijn op invoer van de gebruiker. Zeker in het laatste geval bestaat de kans dat aanvallers misbruik maken van onvoldoende filtering of codering.

U/WA.04 Webapplicatie-uitvoer beperken	
Richtlijn (wie en wat)	De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren.
Doelstelling (waarom)	Voorkom manipulatie van het systeem door andere gebruikers.
Risico	Via uitvoer van de webapplicatie de werking van of informatie op het systeem van anderen manipuleren.
Classificatie	Midden
Verwijzingen	CRE 161-451 (Bescherming via uitvoerverwerking)

Maatregelen

normaliseren

01 Converteer alle dynamische uitvoer naar een veilig formaat.
Uitgebreide testen kunnen aannemelijk maken dat uitvoer altijd genormaliseerd wordt. Gerichte codereviews leveren in de regel meer zekerheid op.
Het coderen van dynamische pagina-inhoud houdt in dat de webapplicatie mogelijk 'gevaarlijke' tekens codeert. Hoe de webapplicatie deze informatie moet coderen is afhankelijk van de plek in de pagina waar deze dynamische inhoud verschijnt. Zo moet men speciale tekens in HTML, JavaScript, HTML-attributen en URL's allemaal op een andere wijze coderen. Neem bijvoorbeeld het 'groter dan'-teken (>). Afhankelijk van de plek waar dit teken wordt gebruikt, ziet de gecodeerde versie van dit teken er als volgt uit:
- *HTML-gecodeerd: >*
- *HTML-attribuut-gecodeerd: >*
- *JavaScript-gecodeerd: \x3E*
- *CSS-gecodeerd: \3E*
- *URL-gecodeerd: %3E*

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

U/WA.05 Vertrouwelijkheid van gegevens

Bescherm gevoelige (vertrouwelijke) gegevens door gebruik te maken van cryptografische technieken in de database, bestanden en/of communicatie. Bepaal op basis van een risicoanalyse en classificatieschema welke gegevens gevoelig of vertrouwelijk zijn (B.03 en B.01/03 [1]).

Beschikbare cryptografische technieken zijn versleuteling en hashing en de daarvan afgeleide digitale handtekening.

U/WA.05 Vertrouwelijkheid van gegevens garanderen	
Richtlijn (wie en wat)	De webapplicatie garandeert de vertrouwelijkheid van gegevens door toepassing van privacybevorderende en cryptografische technieken.
Doelstelling (waarom)	Gegevens in opslag en transport beschermen tegen ongeautoriseerde kennisname en manipulatie.
Risico	Onbevoegden nemen kennis van gegevens die zijn opgeslagen of worden gecommuniceerd en zijn mogelijk in staat deze te veranderen.
Classificatie	Hoog
Verwijzingen	CRE 126-668 (Veilige gegevensopslag) CRE 278-646 (Veilige communicatie) CRE 362-550 (Verwerking persoonsgegevens) CRE 170-772 (Cryptografie) CRE 716-526 (Sessietokengeneratie)

Maatregelen

privacybevorderende technieken

01 Pas de privacy-by-designprincipes toe wanneer de webapplicatie persoonsgegevens verwerkt.
Privacy by Design[12] *kent 7 uitgangspunten:*
1. *Proactief in plaats van reactief – preventief in plaats van herstellend;*
2. *Privacy als standaard;*
3. *Privacy geïntegreerd in het ontwerp;*
4. *Volledige functionaliteit – win-win in plaats van het een of het ander;*
5. *Veiligheid van begin tot eind – bescherming tijdens de volledige levenscyclus;*
6. *Zichtbaarheid en transparantie – houd het open;*
7. *Respect voor de privacy – laat de gebruiker centraal staan.*

02 Maak waar mogelijk gebruik van privacybevorderende technieken.
Denk hierbij bijvoorbeeld aan anonimisering of pseudonimisering (het gebruik van een pseudo-identiteit die niet rechtstreeks te koppelen is aan een natuurlijke persoon) van gegevens.

cryptografische technieken

03 Versleutel of hash gevoelige gegevens in databases en bestanden.
Het is niet altijd nodig een complete database te versleutelen. Soms kan volstaan worden met het versleutelen van enkele tabellen en zelfs kolommen uit tabellen.
Versleutelde gegevens kunnen tijdens communicatie versleuteld blijven, ook wanneer het communicatiekanaal zelf versleuteld is. Dit levert een extra beveiligingslaag.
Versleutel de gegevens altijd op applicatieniveau. Het versleutelen van een volledige harde schijf (full disk encryption) wordt niet ontraden, maar biedt niet tegen alle dreigingen bescherming.

04 Gebruik cryptografisch sterke sessie-identificerende cookies.
Gebruik de ingebouwde functionaliteit van de webserver om cookies te genereren die de gebruikerssessie identificeren. Genereer uitsluitend zelf sessie-identificerende cookies als dat functioneel noodzakelijk is en de gewenste functionaliteit niet op een andere manier kan worden verkregen. Deze sessie-identificerende cookies dienen dan te zijn gegenereerd door een cryptografische nummergenerator. De keuze voor de generator en de lengte van de uitvoer dienen dan in de ontwerpdocumentatie te zijn gedefinieerd. Genereer geen sessie-cookies op basis van persoonlijke of gevoelige informatie zoals een gebruikersnummer of wachtwoord.

12 Zie: https://en.wikipedia.org/wiki/Privacy_by_design

Maatregelen

05 Versleutel communicatie.
Dit zal in de regel gebeuren met TLS.
Richtlijnen voor het veilig inzetten van TLS worden besproken in de ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS).[13] *Deze algemene richtlijnen zijn onverkort van toepassing voor het beveiligen van verbindingen met webapplicaties.*
Bezoeken de meeste gebruikers de webapplicatie via een entreepagina in een andere webapplicatie (bijvoorbeeld via www.example.com naar secure.example.com), dan wordt ook deze webapplicatie via https aangeboden. Een bezoeker wordt bij elk bezoek doorverwezen van de http- naar de https-versie.
Naast deze algemene richtlijnen zijn de volgende specifieke aanwijzingen van toepassing bij het gebruiken van TLS voor http-verkeer, oftewel https:
- *Schakel, indien mogelijk, http-compressie uit. Http-compressie maakt een website vatbaar voor de BREACH-aanval.*
- *Ondersteun Http Strict Transport Security (HSTS). Als u HSTS ondersteunt, zal de browser voor elke terugkerende bezoeker vereisen dat de website opnieuw via https wordt aangeboden. Dit helpt man-in-the-middle-aanvallen te voorkomen. De instellingen voor HSTS worden in securityheaders toegepast (zie richtlijn U/PW.03).*
- *Heeft uw website meerdere subdomeinen (bijvoorbeeld met en zonder 'www.'), ondersteun dan https op elk van deze domeinnamen. Verwijs een bezoeker van de site onder een domeinnaam direct door naar de https-versie van de site onder die domeinnaam. Verwijst u domeinnamen onderling ook door (bijvoorbeeld de versie zonder 'www.' Naar de versie met 'www.'), doe die doorverwijzing dan tussen de https-versies van de site onder die domeinnamen. Verwijs geen domeinnamen naar elkaar door via http. Zorg dat elk van de domeinnamen voorkomt als SubjectAlternativeName in het TLS-certificaat.*
- *Vermijd het vermengen van inhoud van de webapplicatie die via http en via https wordt aangeboden (mixed content). Dat voorkomt dat een aanvaller de vertrouwelijke delen van uw webapplicatie alsnog weet te achterhalen of te manipuleren.*
- *Schakel, indien mogelijk, renegotiation uit. Renegotiation is slechts nodig in twee gevallen. Ten eerste is het van waarde voor webapplicaties die grote hoeveelheden data versturen van of naar de gebruiker (in de orde van gigabytes). Ten tweede wordt het gebruikt bij webapplicaties die verbindingen beveiligen met clientcertificaten.*

06 Onderteken transacties met een digitale handtekening.
Digitale handtekeningen beschermen de onweerlegbaarheid van (de herkomst van) gegevens.

U/WA.06 Webapplicatie-informatie

Webapplicaties maken soms gebruik van client-side scripts zoals JavaScript. Commentaarregels in scripts gedurende de ontwikkel- en testfase zijn normaal, maar in een productieomgeving ongewenst omdat de commentaarregels onnodig informatie vrijgeven waarvan een kwaadwillende misbruik kan maken.

Tijdens deployment van een webapplicatie kan alle code die naar clients wordt gestuurd, ontdaan worden van commentaar. Aanvullend zijn applicatiefirewalls in staat om commentaarregels uit HTML- en scriptcode te verwijderen en zodoende gefilterde antwoorden terug te geven aan de client.

U/WA.06 Webapplicatie-informatie beperken	
Richtlijn (wie en wat)	De webapplicatie beperkt de informatie in de uitvoer tot de informatie die voor het functioneren van belang is.
Doelstelling (waarom)	Beperk het (onnodig) vrijgeven van informatie tot een minimum.
Risico	Kennis nemen van de technologieën van de webapplicatie, om deze vervolgens te gebruiken om de webapplicatie aan te vallen.
Classificatie	Laag
Verwijzingen	CRE 308-515 (Voorkom onthullen van securitygevoelige informatie) CRE 843-841 (Log discreet)

Maatregelen

Uitvoer

01 Verwijder commentaarregels uit de scripts (code).

02 Verwijder of pseudonimiseer verwijzingen naar interne bestands- of systeemnamen.
De webapplicatie geeft geen informatie over de interne werking of configuratie van de webapplicatie zelf of een van de systemen waarmee de webapplicatie samenwerkt. Eenvoudige testen volstaan om aannemelijk te maken dat uitvoer geen informatie over interne werking of configuratie prijsgeeft.

13 Zie: https://www.ncsc.nl/transport-layer-security/ICT-beveiligingsrichtlijnen-voor-TLS

U/WA.07 Webapplicatie-integratie

Een webapplicatie integreert met onder- en achterliggende systemen (bijvoorbeeld het onderliggende besturingssysteem en een achterliggende database) door gebruik te maken van commando's en query's.

Grofweg bestaan er twee methoden om vanuit een webapplicatie een query of commando te genereren, die gebruik maakt van invoer van gebruikers: via dynamische strings of via parameters.

Bij dynamische strings plakt de webapplicatie een vaste string (bijvoorbeeld de start van een SELECT-statement) aan een variabele (bijvoorbeeld de inhoud van de WHERE-clause). Via deze methode bestaat de mogelijkheid dat de door een gebruiker geleverde invoer de query op ongecontroleerde wijze verandert. Hierdoor kunnen gegevens bijvoorbeeld vernietigd worden of ongefilterd bij de gebruiker komen, waardoor de vertrouwelijkheid geschonden wordt.

Bij het gebruik van geparametriseerde queries is de syntax van de query statisch en wordt invoer alleen gebruikt om vooraf gedefinieerde variabelen te vullen. Door te voorkomen dat de syntax van de query wijzigt, voorkomt de webapplicatie SQL-injectieaanvallen.

Geparametriseerde queries zijn ook efficiënter: doordat ze voorgedefinieerd zijn, gebruiken ze bekende tabelstructuren optimaal. Toch geven ze de gebruiker geen volledige vrijheid. Op dezelfde manier voorkomen statisch geprogrammeerde commando's ervoor dat de gebruiker geen mogelijkheid heeft de aard van de commando's te beïnvloeden.

U/WA.07 Webapplicatie-integratie communiceren	
Richtlijn (wie en wat)	De webapplicatie communiceert alleen met onder- en achterliggende systemen op basis van statisch geconfigureerde (geparametriseerde) commando's en query's en uitsluitend ten behoeve van de noodzakelijke functionaliteit.
Doelstelling (waarom)	Kwetsbaarheid van de onder- en achterliggende systemen voorkomen en de integriteit en vertrouwelijkheid garanderen.
Risico	Via manipulatie (bijvoorbeeld commando- of SQL-injectie) kennis nemen van de inhoud van de onder- en achterliggende systemen of deze kunnen manipuleren.
Classificatie	Hoog
Verwijzingen	CRE 732-873 (Geparametriseerde query's en commando's)

Maatregelen

commando's en query's

01 Bouw commando- en queryteksten op met uitsluitend in de code al aanwezige vaste tekstfragmenten.
Gebruik vaststaande geparameteriseerde query's, zoals prepared statements in SQL.
De leverancier van de software geeft hierover een verklaring van een onafhankelijke derde af of stelt de broncode beschikbaar voor review.

02 Geef gebruikersinvoer die gebruikt moet worden in commando's en query's op een zodanige manier door, dat de beoogde werking niet wordt gewijzigd.
Voor zover er sprake is van gebruikersinvoer in commando's en query's wordt deze als parameters doorgegeven. Het doel hiervan is te voorkomen dat de gebruiker kan bepalen welke commando's of query's worden uitgevoerd.

noodzakelijke functionaliteit

03 Houd van elke webapplicatie bij welke functionaliteit van backendsystemen nodig is.
De koppeling met backend systemen is gedocumenteerd, inclusief de aard van de koppeling en de daarvoor noodzakelijke (gebruiks)rechten. Functies die niet nodig zijn voor de functionaliteit van een (web)applicatie vormen een onnodig risico en dienen daarom achterwege te blijven.
Denk hierbij aan File Transfer Protocol (FTP), Telnet, Post Office Protocol (POP)/SMTP (postbusfunctie), et cetera.

04 Verbied directe data-toegang tot backendsystemen, tenzij andere opties niet voorhanden zijn.

U/WA.08 Webapplicatiesessie

De webapplicatie biedt expliciete functionaliteit om de sessie te verbreken:
- Daar waar de gebruiker kan inloggen op de webapplicatie is expliciete functionaliteit aanwezig om uit te loggen (het verbreken van de sessie). Tijdens het uitloggen van een gebruiker wordt de sessie onklaar gemaakt en kan een kwaadwillende met eventuele onderschepte sessiegegevens geen verbinding meer opzetten.
- Bij het aanmelden (effectief een wijziging van autorisatieniveau van de gebruiker) wordt de bestaande sessie ongeldig en een nieuwe sessie gestart. Zo kan een vooraf ingestelde sessie niet misbruikt worden na wijziging van autorisatieniveau.
- De idle time-out en de verbindingstijd per sessie zorgen ervoor dat gebruikers automatisch worden uitgelogd op het moment dat zij geen gebruik meer (lijken te) maken van de webapplicatie. Er is een limiet aan de maximale tijd dat een gebruiker inactief is.

Op deze manier wordt het risico verminderd dat een kwaadwillende een webapplicatie ongeautoriseerd kan benaderen, doordat een vorige gebruiker vergeten is uit te loggen.

Laat de applicatie het eigen sessiebeheer hetzelfde uitvoeren wanneer de applicatie wordt gebruikt in een omgeving met een single-sign-on-oplossing. Gebruik een eigen sessie-identifier die losstaat van het single-sign-on-token. Beëindig die sessie volgens dezelfde richtlijnen en vernieuw de authenticatie via de single-sign-on-toepassing. Dit zal in de praktijk niet merkbaar zijn voor de gebruiker.

De beleidsmatige keuzes over sessieverloop komen voort uit richtlijn B.02/09. [1] Zie ook U/WA.05/04 en U/PW.03/03 voor maatregelen om sessie-identifiers in cookies tegen diefstal te beschermen.

U/WA.08 Webapplicatiesessie beëindigen	
Richtlijn (wie en wat)	De (gebruikers)sessie die ontstaat na het succesvol aanmelden van een gebruiker, kent een beperkte levensduur en de gebruiker kan deze sessie zelf beëindigen.
Doelstelling (waarom)	Voorkomen dat derden de controle over een sessie kunnen krijgen.
Risico	Kennisname of wijziging van gegevens door onbevoegde derden.
Classificatie	Laag
Verwijzingen	CRE 470-731 (Minimaliseer sessieduur)

Maatregelen

aanmelden

01 Maak bij het aanmelden een nieuwe sessie aan en verbreek een eventueel al bestaande sessie van die gebruiker. Maak de oude sessie-identifier ongeldig.

levensduur

02 Beëindig de sessie na een vooraf vastgestelde en geconfigureerde tijdspanne van inactiviteit van de gebruiker (idle-time).
Voer een test van de webapplicatie uit waaruit blijkt dat beperking van de idle-time-out en sessieduur is toegepast.
De webapplicatierserver bewaakt zelf de levensduur van een sessie en mag zich hiervoor niet verlaten op de webbrowser.

zelf beëindigen

03 Bied de gebruiker de mogelijkheid de sessie op eigen initiatief te beëindigen (uitloggen).
Dit geldt zowel voor de gebruiker als voor beheerders van de webapplicatie.

04 De sessie is na beëindiging niet langer geautoriseerd binnen de webapplicatie.
Alle op de webserver geregistreerde informatie over de actieve sessie wordt verwijderd, cookies en dergelijke komen te vervallen.
Na beëindiging van een sessie zijn verdere handelingen binnen die sessie niet mogelijk.

U/WA.09 Webapplicatiearchitectuur

De architectuur van webapplicaties beschrijft de functionele en beveiligingssamenhang en legt de relatie met (de architectuur van) het algemene ICT-landschap. Vanuit een eenduidig gemeenschappelijk beeld worden webapplicaties conform deze architectuur gerealiseerd. Hiervoor worden de richtlijnen, instructies en procedures van U/WA.01/02 toegepast. Op deze manier wordt zeker gesteld dat iedere webapplicatie aan de vereiste functionele en beveiligingsdoelen bijdraagt.

U/WA.09 Webapplicatiearchitectuur beschikken	
Richtlijn (wie en wat)	Voor het implementeren, integreren en onderhouden van webapplicaties zijn architectuur- en beveiligingsvoorschriften beschikbaar.
Doelstelling (waarom)	Een webapplicatie-infrastructuur bieden die een betrouwbare verwerking garandeert.
Risico	Onvoldoende beheersing van de webapplicatie-omgeving, waardoor mogelijkheden voor misbruik ontstaan.
Classificatie	Midden
Verwijzingen	CRE 862-452 (Operationele beveiligingsprocessen) CRE 708-355 (Veilige architectuur) CRE 820-877 (Technische documentatie) CRE 402-706 (Log relevant)

Maatregelen

architectuurvoorschriften

01 Stel architectuurvoorschriften op die actief worden onderhouden.
Zorg dat dit document onderdeel is van het proces wijzigingsbeheer (zie richtlijn C.08 [1]).
Het document:
- *heeft een eigenaar;*
- *is voorzien van een datum en versienummer;*
- *bevat een documenthistorie (wat is wanneer en door wie aangepast);*
- *is actueel, juist en volledig;*
- *is door het juiste (organisatorische) niveau vastgesteld/geaccordeerd.*

De ICT-afdeling en de ICT-securitymanager zijn in ieder geval deel van 'het juiste (organisatorische) niveau'.

beveiligingsvoorschriften

02 Scheid vertrouwde en niet-vertrouwde domeinen: toepassen van scheidingen in netwerken (DMZ).
Zie U/NW.03.

Maatregelen

03 Pas het principe van 'least privilege' toe op hoe de webapplicatie van onderliggende servers gebruikmaakt.
Hiervoor moet expliciet bekend zijn welke rechten een webapplicatie minimaal moet hebben om volledig functioneel te zijn. Alleen deze rechten zijn toegewezen aan het account waaronder de webapplicatie draait. Wanneer een webapplicatie tijdens het opstarten tijdelijk hogere rechten nodig heeft (bijvoorbeeld om een TCP-poort aan te maken), dan dient het zo snel mogelijk daarna afstand te doen van deze hogere rechten.

04 Configureer webapplicaties en onderliggende servers zodanig dat ook security-gerelateerde events worden vastgelegd.
Hieronder vallen in ieder geval alle activiteiten die geblokkeerd werden omdat de rechten van de gebruiker of applicatie ontoereikend waren om de activiteiten uit te voeren.

Platformen en webservers

Het doel is een betrouwbare, veilige server volgens het beleid

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

Een besturingssysteem moet hardening ondergaan

Deze paragraaf gaat in op het ontwerpen, inrichten, beschikbaar stellen en handhaven van de beveiliging voor platformen en webservers zodat deze systemen geen onbedoelde functionaliteit bieden die kwaadwillenden kunnen misbruiken om toegang te krijgen.

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 gebruikmaakt zoals applicatieservers en databaseservers.

Het uitgangspunt bij de beveiliging van platformen en webservers is het hardenen van de ICT-omgeving (zie richtlijn B.01/05 [1]). Hardening houdt in dat het systeem zo is inricht dat het beter bestand is tegen aanvallen van kwaadwillenden. De technische stappen die nodig zijn om een systeem te hardenen verschillen per type systeem. De logische stappen verschillen echter veel minder. De richtlijnen in dit hoofdstuk zijn dan ook generiek van aard. Specifieke maatregelen voor de verschillende besturingssystemen en webservers worden aangeboden door het Center for Internet Security (CIS).[14]

Een niet goed gehardende server leidt tot volledige controle van het platform door een aanvaller

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

De beveiligingsrichtlijnen zijn onderverdeeld

Binnen de laag platformen en webservers worden onderstaande richtlijnen beschreven en per richtlijn worden conformiteitsindicatoren en maatregelen uitgewerkt.

- Operationeel beleid voor platformen en webservers (U/PW.01)
- Webprotocollen (U/PW.02)
- Webserver (U/PW.03)
- Isolatie van processen en bestanden (U/PW.04)
- Toegang tot beheermechanismen (U/PW.05)
- Platform-netwerkkoppeling (U/PW.06)
- Hardening van platformen (U/PW.07)
- Platform- en webserverarchitectuur (U/PW.08)

14 Zie: https://www.cisecurity.org/cis-benchmarks/

U/PW.01 Operationeel beleid voor platformen en webservers

Het operationeel beleid voor platformen en webservers beschrijft de manier waarop de organisatie omgaat met het inrichten en beschikbaar stellen van platformen en webservers. Het operationeel beleid is een concretere uitwerking van het bovenliggende beleid. Een solide operationeel beleid is daarom een randvoorwaarde voor een veilige inrichting van een webapplicatieomgeving.

Sluit platformen en webservers aan op centrale toegangsvoorzieningen (zie U/TV.01) voor identificatie, authenticatie en autorisatie. Wanneer het niet mogelijk is op centrale voorzieningen aan te sluiten, geef dan op serverniveau invulling aan de vereisten voor toegangsvoorzieningen.

Regel de authenticatie tot platformen en webservers zeer strikt in. Afhankelijk van het type besturingssysteem kunnen hier verschillende maatregelen voor worden getroffen. De volgende aanbevelingen zijn van toepassing op vrijwel alle besturingssystemen en kunnen in de voorschriften worden overgenomen.

- Zorg dat het systeem niet toegankelijk is op basis van anonieme generieke accounts zoals een gastaccount.
- Maak toegang op afstand alleen mogelijk voor accounts met beperkte rechten. Zorg dat de toegang op afstand tot root- of beheerderaccounts niet mogelijk is. Beheerders moeten op afstand inloggen met een gelimiteerd beheeraccount en vervolgens lokaal, daar waar nodig, gebruik maken van verhoogde rechten via mechanismen als sudo (Linux) en RunAs (Windows).
- Gebruik sterke authenticatiemechanismen voor de toegang tot systemen. Kies een authenticatiemechanisme aan de hand van het volwassenheidsmodel voor authenticatie van het NCSC.[15]
- Beperk het aantal groepen waartoe een gebruiker behoort (groepslidmaatschappen). Machtigingen en rechten die aan een groep worden toegekend, gelden ook voor de leden van die groep.
- Implementeer een strikt wachtwoordbeleid als er nog accounts met wachtwoorden worden gebruikt. In een wachtwoordbeleid worden de minimale wachtwoordlengte, lengte van de wachtwoordhistorie en account lock-outs vastgelegd.[16]
- Voorkom dat wachtwoorden in leesbare vorm worden opgeslagen. Sla alleen de (gezouten) hash op.
- Verwijder of blokkeer ongebruikte accounts en standaard aanwezige accounts.
- Wijzig het standaardwachtwoord van een systeem alvorens het in gebruik te nemen.

U/PW.01 Operationeel beleid voor platformen en webservers formuleren	
Richtlijn (wie en wat)	Het operationeel beleid voor platformen en webservers formuleert richtlijnen, instructies en procedures voor inrichting en beheer van platformen en webservers.
Doelstelling (waarom)	Betrouwbare ondersteuning van de programmatuur die op het platform draait.
Risico	De beoogde werking van het platform wordt aangetast, bijvoorbeeld doordat de beveiliging wordt doorbroken.
Classificatie	Midden
Verwijzingen	CRE 862-452 (Operationele beveiligingsprocessen)

Maatregelen

richtlijnen

01 Stel voorschriften op voor de veilige configuratie van platformen en webservers.
De baseline dient aandacht te geven aan de compartimentering van applicatiedata, software en configuratiebestanden. Deze dienen van elkaar gescheiden te zijn.
Maak gebruik van bestaande richtlijnen van leveranciers en erkende kennisinstituten als NIST, SANS, et cetera.

02 Besteed in de voorschriften expliciet aandacht aan hardening van platformen en webservers.
Dit is een inhoudelijke eis aan de richtlijn, gericht op het (on)beschikbaar maken van functionaliteiten.

03 Besteed in de voorschriften expliciet aandacht aan de configuratie en het gebruik van accounts.

instructies en procedures

04 Stel instructies en procedures op voor:
- het creëren en onderhouden van voorschriften voor de veilige configuratie van platformen en webservers;
- het toepassen van voorschriften voor de veilige configuratie van platformen en webservers.

Besteed aandacht aan het regelmatig evalueren en bijstellen van de richtlijnen. Zie de inleiding voor een aantal concrete aanbevelingen.
Indien deze instructies en procedures ruimte bieden om af te wijken van de richtlijn, dient hieraan de vereiste van 'comply or explain' gekoppeld te zijn.

15 Zie: https://www.ncsc.nl/documenten/factsheets/2022/april/24/factsheet-volwassen-authentiseren-gebruik-veilige-middelen-voor-authenticatie
16 Zie voor afwegingen ten aanzien van het wachtwoordbeleid de website van het NCSC: https://www.ncsc.nl/authenticatie

U/PW.02 Webprotocollen

Scherm de communicatie tussen de webserver en de client zodanig af dat het voor derden niet mogelijk is:
- kennis te nemen van wat er gecommuniceerd wordt;
- zich voor te doen als de betreffende client.

Voorbeelden van mogelijk misbruik zijn:
- diefstal - van cookies, bijvoorbeeld via XSS;
- fraude - transacties onder een valse identiteit aanbieden.

Hiervoor moet een kwaadwillende in staat zijn tot:
- afluisteren van de communicatie;
- misbruiken van http-methoden die niet noodzakelijk zijn voor de webapplicatie;
- manipuleren van cookies, bijvoorbeeld via JavaScript.

Http ondersteunt verschillende methoden (zie RFC 7540 voor http/2). In de praktijk gebruikt een webapplicatie vaak alleen de methoden GET en POST. Voor veel scripts en objecten op een webserver geldt zelfs dat alleen de GET-methode nodig is. Het door de server aanbieden van methoden die niet nodig zijn vergroot het aanvalsoppervlak onnodig. Beperk daarom de aangeboden methoden tot de functioneel noodzakelijke.

Door het stelen van cookies of via Cross-Site Request Forgery (CSRF) kunnen kwaadwillenden ongewild transacties uitvoeren uit naam van een gevalideerde gebruiker. Voor CSRF kan dit via links of formulieren op malafide websites. De kans op misbruik van gestolen cookies kan de webapplicatie minimaliseren door de inhoud van een cookie te koppelen aan het ip-adres waaraan deze inhoud is toegekend. Gebruik in dat geval echter nooit een opgegeven ip-adres uit een http-header. Proxy- en VPN-servers geven het bron-ip-adres soms op met de Forwarded-header, maar deze kan door aanvallers gemanipuleerd worden.

Op het moment dat zich een probleem voordoet binnen een webapplicatie zal de webserver veelal de http-statuscode[17] 500 Internal Server Error terugsturen. De mogelijkheid bestaat dat de webserver bij deze foutcode gevoelige informatie over de web-applicatie openbaart (databasenamen, gebruikersnamen, bestandsnamen, interne ip-adressen, etc.). Tref maatregelen om dit te voorkomen.

U/PW.02 Webprotocollen garanderen	
Richtlijn (wie en wat)	De webserver garandeert specifieke kenmerken van de inhoud van de protocollen.
Doelstelling (waarom)	Voorkom inzage, wijziging of verlies van gegevens door manipulatie van de logica van de webserver of webapplicatie.

U/PW.02 Webprotocollen garanderen	
Risico	De werking van de webserver of webapplicatie wordt gemanipuleerd, waardoor deze onder controle komt van een aanvaller.
Classificatie	Midden
Verwijzingen	CRE 028-727 (Bescherming tegen CSRF) CRE 483-715 (Beperken van HTTP-methodes) CRE 743-110 (Beperken van informatie in HTTP-headers of respons) CRE 612-435 (Generieke foutmeldingen)

Maatregelen

specifieke kenmerken

01 Behandel alleen http-requests waarvan de gegevens een correct type, lengte, formaat, tekens en patronen hebben.
Dit zal in de regel een producteigenschap van de betreffende webserver zijn. De leverancier van de software geeft hierover een verklaring van een onafhankelijke derde af of stelt de broncode beschikbaar voor review. Op de veelgebruikte Apache HTTP Server kan modSecurity handvatten bieden. De verdeling van controles op de specifieke kenmerken is afhankelijk van de webserver en de webapplicatie(s) waarmee de deze samenwerkt. Zie ook U/WA.03.

02 Behandel alleen http-requests van initiators met een correcte authenticatie en autorisatie.
Valideer dat transacties niet worden uitgevoerd vanaf een andere website dan de website waarop de gebruiker is geauthentiseerd.

protocollen

03 Sta alleen de voor de ondersteunde webapplicaties benodigde http-requestmethoden (GET, POST, etc.) toe en blokkeer de overige niet-noodzakelijke http-requestmethoden.
In de ontwerp- of configuratiedocumentatie is vastgelegd:
- *welke http-requestmethoden (GET, POST, etc.) voor de ondersteunde webapplicaties benodigd zijn;*
- *welke informatie in de http-headers voor het functioneren van belang zijn;*
- *welke standaardfoutmelding(en) worden getoond/verstuurd;*
- *op welke wijze bovenstaande is gerealiseerd, denk hierbij aan de configuratie van de webserver en, indien van toepassing, de application-level firewall;*
- *eventuele noodzakelijke afwijkingen van bovenstaande, omdat de webapplicatie anders niet kan functioneren zijn onderbouwd.*

Methoden anders dan GET en POST zijn vrijwel nooit nodig binnen traditionele webapplicaties en vormen alleen een extra beveiligingsrisico. Bij moderne api's worden soms wel andere methoden gebruikt. Het is in alle gevallen aan te raden om niet-benodigde http-methoden via configuratie van de webserver of via de application-level firewall te blokkeren.

04 Verstuur alleen http-headers die voor het functioneren van http en de webapplicatie van belang zijn.

17 http://nl.wikipedia.org/wiki/Lijst_van_HTTP-statuscodes

Maatregelen	
05	Toon in http-headers alleen de noodzakelijke informatie die voor het functioneren van belang is. *Informatie in standaard http-headers (bijvoorbeeld type webserver of versienummer) kan misbruikt worden door een kwaadwillende. Het weghalen van het versienummer helpt ten dele, maar met fingerprinting-technieken kan een kwaadwillende vaak alsnog de gebruikte versie vaststellen. Aan de andere kant wordt deze informatie door beveiligings-onderzoekers soms gebruikt om contact op te nemen met systeem-eigenaren om ze juist te waarschuwen voor problemen met hun versie. Maak een bewuste belangenafweging om te kiezen voor het wel of niet tonen van softwarenamen en versienummers in http-headers. Leg de keuze vast in de ontwerp- of configuratiedocumentatie.*
06	Bij het optreden van een fout wordt de informatie in een http-response tot een minimum beperkt. Een eventuele foutmelding zegt wel *dat* er iets is fout gegaan, maar niet *hoe* het is fout gegaan. *Webservers bieden functionaliteit om standaardmeldingen te laten genereren aan de hand van specifieke statuscodes. Een applicatiefirewall zou een dergelijke statuscode kunnen detecteren en een gebruiksvriende-lijke foutmelding kunnen terugsturen. Geef geen informatie over de werking van de applicatie in foutmeldingen.*

U/PW.03 Webserver

Via een directory listing kan een gebruiker via internet de inhoud van een map op de server bekijken. Het opvragen van een directory listing via internet komt overeen met het lokaal uitvoeren van een dir-commando onder Windows of een ls-commando onder UNIX/Linux. Zodra een webserver de mogelijkheid biedt om directory listings uit te voeren, bestaat het risico dat een kwaadwillende de inhoud van vertrouwelijke mappen raadpleegt. Schakel directory listings dan ook standaard uit en sta het alleen toe op mappen waarvoor dat functioneel noodzakelijk is.

Vaak vertrouwen webapplicaties op cookies om sessiegegevens, inclusief authenticatie- en autorisatiegegevens, te koppelen aan een actieve gebruiker. Bij diefstal van een sessiecookie kan een aanvaller meeliften op de sessie van die gebruiker en diens gegevens inzien. Via de attributen HttpOnly en Secure wordt de beveiliging van cookies verhoogd. HttpOnly zorgt dat de cookie uitsluitend via http-verbindingen gebruikt kan worden en niet via bijvoorbeeld JavaScript (manipulatie). Secure limiteert de communicatie van cookies tot beveiligde verbindingen en voorkomt dat de cookie-inhoud door onbevoegden wordt afgeluisterd.

Instellingen voor cookies kunnen worden afgedwongen door ze in de naamgeving met __Host- of __Secure- te laten beginnen. Mocht door een configuratiefout een attribuut ontbreken dan zal de cookie niet geaccepteerd worden door de browser, om te voorkomen dat deze als gevolg van een onbedoelde configuratie-fout alsnog uitlekt.

Bij een clickjacking-aanval wordt een webpagina in een frame op een andere website geopend waar gebruikers andere inhoud zien en daar interactie mee aangaan. De aanvaller kan deze interactie ongemerkt laten uitvoeren op de webpagina van het doelwit, misbruik makend van de sessie van de gebruiker. De webserver kan met behulp van de Content-Security-Policy het laden van de webpagina's in frames beperken.

Gebruik de Content-Security-Policy ook voor het beperken van inhoud die van buiten de webapplicatie wordt ingeladen. Hiermee worden cross-site-scriptingaanvallen sterk bemoeilijkt.

U/PW.03 Webserver inrichten	
Richtlijn (wie en wat)	De webserver is ingericht volgens een configuratie-baseline.
Doelstelling (waarom)	Ongewenste vrijgave van informatie tot een minimum beperken, met name waar het gaat om informatie die inzicht geeft in de opbouw van de beveiliging.
Risico	Lekken van informatie die op zichzelf waarde heeft of die voor verdere aanvallen gebruikt kan worden.
Classificatie	Hoog

U/PW.03 Webserver inrichten

Verwijzingen
CRE 615-744 (Beveilig tegen directory aanvallen)
CRE 110-531 (Cookieconfiguratie)
CRE 636-347 (HTTP-securityheaders)

Maatregelen

configuratiebaseline

01 Beschrijf de parametrisering van de webserver in een configuratiedocument.
Maak gebruik van bestaande richtlijnen van leveranciers en erkende kennisinstituten als NIST, SANS, et cetera.

02 Schakel directory-listings standaard uit en sta deze alleen toe waar dit functioneel noodzakelijk is.
Staat directory listing aan, dan kan de websitebezoeker de inhoud van bepaalde mappen zien. In de regel zal dit via instructies in de configuratie van de webserver gerealiseerd worden. Deze worden bij implementatie ingevuld, bij een audit gecontroleerd.

03 Stel alle cookies in volgens een baseline.
De baseline omschrijft waarop cookies voor beveiligingsdoeleinden moeten worden ingesteld en behandelt ten minste de volgende attributen:
- *Secure. Aanbevolen instelling: altijd toepassen.*
- *HttpOnly. Aanbevolen instelling: altijd toepassen.*
- *SameSite. Aanbevolen instelling: strict, indien functioneel noodzakelijk: lax.*
- *__Host-. Aanbevolen instelling: toepassen, indien functioneel noodzakelijk vervangen door __Secure-.*

Maatregelen

04 Stel alle securityheaders in volgens een baseline.
De baseline omschrijft waarop http-headers voor beveiligingsdoeleinden moeten worden ingesteld en behandelt ten minste de volgende headers:
- *Strict-Transport-Security instrueert de client dat een webpagina altijd over een versleutelde https-verbinding moet worden geladen, ook als er naar een http-link wordt verwezen. Aanbevolen waarde: max-age=31536000; includeSubDomains.*
- *Content-Security-Policy geeft een aantal opties die bepalen welke inhoud in de applicatie geladen kan worden. Aanbevolen instellingen:*
  - *default-src: none of self*
  - *Indien dit functioneel niet mogelijk is, dan minimaal script-src: self en style-src: self*
  - *base-uri: none of self*
  - *form-action: none of self*
  - *frame-ancestors: none of self*
  - *Indien functioneel noodzakelijk: frame-src: none of self*
  - *de nadrukkelijk onveilige instellingen unsafe-inline, unsafe-eval en unsafe-hashes dienen niet te worden gebruikt*
  - *in de instellingen dienen data:, http:, 127.0.0.1 en wildcards (*) niet te worden gebruikt*
- *X-Frame-Options voorkomt dat een webpagina in een frame van een andere pagina wordt geladen. Dit gebeurt bij clickjacking-aanvallen. Deze instelling is alleen nodig voor compatibiliteit met oudere browsers, de instelling voor frame-ancestors (hierboven) prevaleert bij moderne browsers. Aanbevolen waarde: DENY. Indien functioneel noodzakelijk: SAMEORIGIN.*
- *X-Content-Type-Options instrueert de browser hoe het bestandstype mag worden bepaald als er geen Content-Type is gespecificeerd. MIME-sniffing-aanvallen kunnen misbruik maken van het standaard-gedrag van browsers. Aanbevolen waarde: nosniff.*
- *X-XSS-Protection geeft aan dat de browser tegen XSS-aanvallen moet beschermen. Aanbevolen waarde: 1; mode=block. Indien functioneel noodzakelijk: 1.*
- *Referrer-Policy biedt mogelijkheden om de vorige pagina van een bezoek aan de server aan te geven. Aanbevolen waarde: no-referrer. Indien functioneel noodzakelijk: same-origin.*

U/PW.04 Isolatie van processen en bestanden

Isolatie is een manier om een proces (draaiende applicatie) af te scheiden van de rest van een besturingssysteem en andere processen. Hiermee wordt wederzijdse beïnvloeding voorkomen.

Een bekende implementatie van isolatie is chroot. Het commando chroot (change root) wijzigt de rootdirectory voor een proces. Door een proces via chroot te laten werken, heeft het proces geen toegang meer tot bestanden die zich buiten deze root-directory bevinden. Dit mechanisme kan bijvoorbeeld worden ingezet om een Apache-server geïsoleerd te laten draaien.

Naast het afschermen van directories via chroot bestaan er ook mechanismen om andere delen van het besturingssysteem af te schermen; voorbeelden zijn het beperken van I/O-rates, het beperken van het toegestane hoeveelheid geheugen en het beperken van de toegestane hoeveelheid CPU-cycles.

Virtualisatie is een vorm van afscherming van processen door volledig autonome besturingssystemen naast elkaar te laten functioneren. Jailing of sandboxing is een mechanisme dat het concept van chroot verder doorvoert tot (vrijwel) alle aspecten van een besturingssysteem. Jailing wordt voornamelijk op het BSD-platform ondersteund, maar kan ook in andere omgevingen gerealiseerd worden.

U/PW.04 Isolatie van processen en bestanden beschermen	
Richtlijn (wie en wat)	Kritieke delen van systemen (bijv. subprocessen, bestanden) beschermen door isolatie van overige delen.
Doelstelling (waarom)	Beperk de impact bij misbruik van processen.
Risico	Beïnvloeding van andere processen en het weglekken van informatie.
Classificatie	Midden
Verwijzingen	CRE 273-600 (Scheid onderdelen met verschillende vertouwensniveaus)

Maatregelen

isolatie

01 Stel een ontwerp- en configuratiedocument vast dat beschrijft op welke wijze processen worden afgeschermd van bestanden waartoe zijn geen toegang mogen hebben.
Hiervoor kan een standaard hulpmiddel als 'chroot' en de rechtenstructuur van het besturingssysteem ingezet worden.

02 Stel een ontwerp- en configuratiedocument vast dat beschrijft op welke wijze processen van elkaar worden afgeschermd.
Hiervoor zal meestal virtualisatie noodzakelijk zijn, tenzij de webserver de enige applicatie is die op het onderliggende platform draait. In dat geval moet nog wel aandacht besteed worden aan de hardening van het platform, maar kan verdere isolatie meestal achterwege blijven.

U/PW.05 Toegang tot beheermechanismen

Beheermechanismen stellen een beheerder in staat de werking van een platform of webserver te controleren en te wijzigen. Adequate bescherming van de toegang tot deze beheermechanismen is daarom essentieel voor de goede werking en beveiliging van platform, webserver en uiteindelijk de webapplicatie.

Het gebruik van backdoors voor de toegang tot beheermechanismen moet absoluut uitgesloten zijn. Een backdoor voor beheer is bijvoorbeeld een beheerinterface waarvoor geen authenticatie nodig is en draait op poort 8888 en daardoor moeilijk te ontdekken zou moeten zijn. Dat wordt security by obscurity genoemd. De kans is groot dat kwaadwillenden backdoors vroeg of laat ontdekken en erin slagen om deze te misbruiken.

In situaties waarin continue integratie en delivery (ci/cd) wordt toegepast is het uitrollen van de applicatie naar een platform verregaand geautomatiseerd en hoeft een beheerder idealiter nooit op een productiesysteem in te loggen.

U/PW.05 Toegang tot beheermechanismen gebruiken	
Richtlijn (wie en wat)	Het beheer van platformen maakt gebruik van veilige (communicatie)protocollen voor het ontsluiten van beheermechanismen en wordt uitgevoerd conform het operationeel beleid voor platformen.
Doelstelling (waarom)	Voorkomen van misbruik van beheervoorzieningen.
Risico	Een aanvaller kan de controle over het platform of de webserver overnemen.
Classificatie	Hoog
Verwijzingen	CRE 152-725 (Beperk toegang tot beheerfuncties)

Maatregelen

veilige (communicatie)protocollen

01 Gebruik uitsluitend beveiligde (communicatie)protocollen voor de toegang tot beheermechanismen.
Vermijd in ieder geval het gebruik van onbeveiligde protocollen, zoals Telnet en FTP. SSH en SFTP zijn goede vervangers.
Zorg er daarnaast voor dat beheerinterfaces alleen bereikbaar zijn vanaf een gescheiden beheernetwerk (zie richtlijn U/NW.05).

02 Gebruik sterke authenticatie voor de toegang tot de beheermechanismen.
Voor sterke authenticatie kan een combinatie gemaakt worden van de beschikbare toegangsvoorzieningsmiddelen (zie richtlijn U/TV.01).

U/PW.06 Platform-netwerkkoppeling

Binnen het domein netwerken is beschreven hoe centraal geplaatste firewalls de omgeving beschermen tegen kwaadwillenden (zie U/NW.03). Laat naast deze centrale firewalls ook decentraal, op de verschillende machines, een aparte firewall werken. Deze lokale firewalls vormen daarmee een extra laag in de beveiliging. Enkele voorbeelden van deze firewalls zijn Ipfw, Pf, Iptables en Ipfilter (ipf).

Lokale firewalls hebben als voordeel dat deze zowel op poort- als procesniveau controles uitvoeren. Verder hebben lokale firewalls vaak meer inzicht in het binnenkomende verkeer omdat op de machine zelf ontsleuteling van versleutelde tunnels plaatsvindt. Daarnaast bevatten lokale firewalls vaak veel minder regels in de rulebase waardoor fouten in de configuratie minder vaak voorkomen.

Tot slot bieden deze firewalls veelal ook uitgebreide mogelijkheden op het gebied van logging en Network Address Translation (NAT).

U/PW.06 Platform-netwerkkoppeling filteren	
Richtlijn (wie en wat)	Ieder platform filtert het netwerkverkeer met behulp van een lokale firewall, zodat het netwerkverkeer beperkt is tot de bekende, toegestane communicatiestromen.
Doelstelling (waarom)	Controleren van het netwerkverkeer, zowel op poort- als procesniveau, dat lokaal binnenkomt en uitgaat.
Risico	Een deel van de communicatie onttrekt zich aan controles, waardoor een restrisico in verschillende beveiligingsonderwerpen overblijft.
Classificatie	Midden
Verwijzingen	CRE 467-784 (Netwerkbeveiliging)

Maatregelen

bekende, toegestane communicatiestromen

01 Stel een (inrichtings)document op met de communicatiestromen van de op het systeem geïnstalleerde applicaties.
Dit document legt ook vast welke functie(s) het systeem vervult. Denk hierbij aan welke software (applicaties) geïnstalleerd zijn, welke (netwerk) protocollen noodzakelijk zijn, welke gebeurtenissen gelogd worden, etc.
Zorg dat dit (inrichtings)document onderdeel is van het proces wijzigingsbeheer (zie richtlijn C.08 [1]). De ontwerp- en inrichtingskeuzes moeten zijn onderbouwd en op het juiste (organisatorische) niveau zijn verantwoord.

02 De ingestelde firewall-regels beperken communicatiestromen tot die van het inrichtingsdocument.
Bovenstaande document bevat de configuratieregels van de firewall.
De feitelijke configuratie dient hier exact mee overeen te stemmen.

U/PW.07 Hardening van platformen

De hardening van platformen is een resultaat van de toepassing van kwetsbaarhedenbeheer (richtlijn B.01/05 [1]).

De meeste systemen voeren een beperkt aantal functies uit. Ontdoe het systeem van software, gebruikersaccounts en diensten die niet gerelateerd of niet strikt noodzakelijk zijn voor het functioneren van het systeem om de aanvalsmogelijkheden te beperken. Wanneer dat niet mogelijk is, moeten alle niet strikt noodzakelijke functionaliteiten zijn uitgeschakeld. Systeemhardening is een leverancierspecifiek proces, aangezien de verschillende leveranciers het systeem op verschillende manieren configureren en voorzien van verschillende diensten tijdens het installatieproces.

Systemen die onnodige diensten draaien en poorten open hebben die niet open hoeven te staan zijn makkelijker aan te vallen omdat deze diensten en poorten mogelijkheden bieden om het systeem aan te vallen.

Beperk de communicatiemogelijkheden van het systeem tot het strikt noodzakelijke. Eén van de manieren om dit te bereiken is door onnodige services onbereikbaar te maken door ze te verwijderen of uit te schakelen. Door benodigde services in kaart te brengen en vervolgens de afhankelijkheden te bepalen, ontstaat er een lijst van services die minimaal op het systeem moeten staan. Verwijder alle overige services, of schakel ze uit als ze niet verwijderd kunnen worden. Niet-actieve maar wel aanwezige services op een systeem kunnen uiteindelijk toch tot een kwetsbaar systeem leiden aangezien kwetsbare programmacode op het systeem aanwezig is.

U/PW.07 Hardening van platformen configureren	
Richtlijn (wie en wat)	Voor het configureren van platformen is een hardeningrichtlijn beschikbaar en toegepast.
Doelstelling (waarom)	Beperken van de functionaliteit tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.
Risico	Bedoeld of onbedoeld negatief beïnvloeden van een platform, waardoor vertrouwelijkheid, integriteit en/of beschikbaarheid van dat platform niet gegarandeerd is.
Classificatie	Hoog
Verwijzingen	CRE 233-748 (Configuratiehardening)

Maatregelen

Hardeningrichtlijn

01 Richt ICT-componenten aantoonbaar volgens de instructies en procedures van de leverancier in.
Neem in de werkinstructies het toepassen van de instructies en procedures van de leverancier op. Houd tijdens het inrichten van een component een checklist bij en teken deze af na voltooiing van het inrichten van de component.
De uitrol kan door een geautomatiseerd proces plaatvinden. Pas in dat geval de instructies en procedures toe in de gebruikte tool en zorg ervoor dat altijd aagetoond kan worden dat die instellingen overeenkomen.

02 Houd een actueel overzicht bij van de noodzakelijke protocollen, services, accounts en software voor de op het platform geïnstalleerde applicaties.
Zorg dat dit document onderdeel is van het proces wijzigingsbeheer (zie richtlijn C.08 [1]). De ontwerp- en inrichtingskeuzes moeten zijn onderbouwd en op het juiste (organisatorische) niveau zijn verantwoord.

03 Deactiveer of verwijder alle protocollen, services, accounts en software op het platform als die niet volgens het ontwerp noodzakelijk zijn.
Gebruik het ontwerp om te bepalen welke functies nodig zijn. Schakel alle andere functies uit, ook wanneer deze 'leuk' of 'handig' zijn. Verwijder zo mogelijk deze functies van de ICT-component (deïnstallatie).
Leg alle gevonden functies vast, met de vermelding of ze actief, uitgeschakeld of verwijderd zijn. Op die manier is het eenvoudiger vast te stellen of nieuwe functies zijn geïntroduceerd.

04 Toets periodiek of de in productie zijnde ICT-componenten niet meer dan de vanuit het ontwerp noodzakelijke functies bieden. Herstel afwijkingen.
Automatische controles kunnen een onderdeel van deze periodieke toetsing zijn, maar zijn in veel gevallen niet voldoende.
Leg in het operationeel beleid (U/PW.01) vast hoe vaak deze toetsing wordt uitgevoerd.

05 Pas de beveiligingsconfiguraties van netwerkservices en protocollen op het platform toe volgens richtlijnen.
Het 'tunen' van de TCP/IP-stack kan helpen in het beveiligen tegen (distributed) denial-of-service ((D)DoS)-aanvallen.

U/PW.08 Platform- en webserverarchitectuur

De architectuur van platformen en webservers beschrijft de functionele en beveiligingssamenhang en legt de relatie met (de architectuur van) het algemene ICT-landschap. Realiseer alle componenten vanuit een eenduidig gemeenschappelijk beeld conform deze architectuur. Pas hiervoor de richtlijnen, instructies en procedures van U/PW.01 toe. Op deze manier wordt zeker gesteld dat iedere component aan de vereiste functionele en beveiligingsdoelen bijdraagt.

U/PW.08 Platform- en webserverarchitectuur vastleggen	
Richtlijn (wie en wat)	Voor het implementeren, integreren en onderhouden van platformen en webservers zijn architectuurvoorschriften en beveiligingsvoorschriften beschikbaar.
Doelstelling (waarom)	Een platform bieden dat een betrouwbare verwerking garandeert.
Risico	Onvoldoende beheersing van het platform, waardoor de stabiliteit van ondersteunde applicaties niet gegarandeerd is en mogelijkheden voor misbruik ontstaan.
Classificatie	Midden
Verwijzingen	CRE 233-748 (Configuratiehardening) CRE 708-355 (Veilige architectuur) CRE 820-877 (Technische documentatie)

Maatregelen

architectuurvoorschriften

01 Stel architectuurvoorschriften op die actief worden onderhouden.
Zorg dat deze voorschriften onderdeel zijn van het proces wijzigingsbeheer (zie richtlijn C.08). De ontwerp- en inrichtingskeuzes moeten zijn onderbouwd en op het juiste (organisatorische) niveau zijn verantwoord.
Het document:
- *heeft een eigenaar;*
- *is voorzien van een datum en versienummer;*
- *bevat een documenthistorie (wat is wanneer en door wie aangepast);*
- *is actueel, juist en volledig;*
- *is op het juiste (organisatorische) niveau vastgesteld/geaccordeerd.*

De ICT-afdeling en de ICT-securitymanager zijn in ieder geval deel van 'het juiste (organisatorische) niveau'.

beveiligingsvoorschriften

02 Stel hardeningrichtlijnen op voor platformen, aantoonbaar afgeleid uit de architectuur.
Het gaat hier om de aantoonbare, navolgbare relatie tussen wat de architectuur beschrijft en de concretisering in richtlijnen. Bij de registratie van de inrichting wordt deze lijn doorgetrokken naar de daadwerkelijke configuratie en getroffen maatregelen.
Zorg dat dit document onderdeel is van het proces wijzigingsbeheer (zie richtlijn C.08 [1]*).*

Maatregelen

03 Leid de inrichtingsrichtlijnen voor registratie van (beveiligings) events (logging, zie richtlijn C.06 [1]) aantoonbaar af uit de architectuur.

Netwerken

Het doel is een betrouwbare, veilige netwerkinfrastructuur volgens het beleid

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

Het netwerk maakt de webapplicatie bereikbaar voor gebruikers, en services bereikbaar voor de webapplicatie

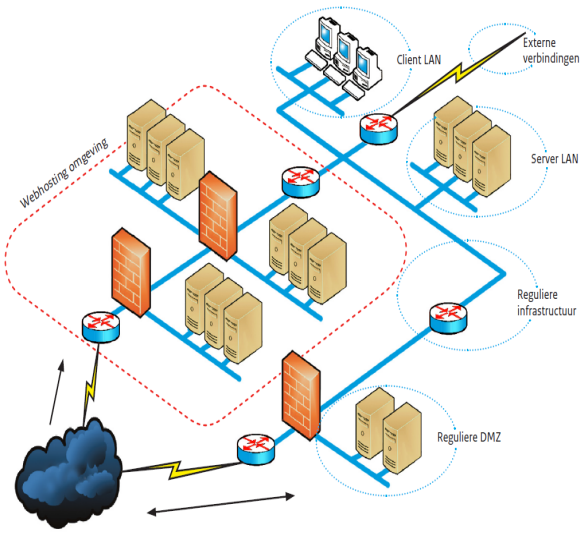
Het netwerk omvat zowel de infrastructuur om de webapplicatie bereikbaar te maken via internet, als de infrastructuur om de webserver resources op te kunnen laten vragen uit andere systemen. Figuur 3 illustreert deze netwerkinfrastructuur, met daarin de afbakening van de richtlijnen (vlak binnen rode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

In het kader van deze richtlijnen 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.

Een slecht beveiligd netwerk leidt tot een onbetrouwbare webapplicatie

De beoogde of vereiste betrouwbaarheid van de webapplicatie wordt ondermijnd door derden, doordat zij in staat zijn het netwerk te manipuleren of verstoren. Oorzaken kunnen gelegen zijn in het niet, incorrect of onvolledig toepassen van bekende richtlijnen en beveiligingstechnieken.



Figuur 3. Reikwijdte ICT-Beveiligingsrichtlijnen voor Webapplicaties

De beveiligingsrichtlijnen zijn onderverdeeld

Binnen de laag Netwerken worden onderstaande richtlijnen beschreven en per richtlijn worden conformiteitsindicatoren en de betreffende maatregelen uitgewerkt.

- Operationeel beleid voor netwerken (U/NW.01)
- Beschikbaarheid van netwerken (U/NW.02)
- Netwerkzonering (U/NW.03)
- Protectie- en detectiefunctie (U/NW.04)
- Beheer- en productieomgeving (U/NW.05)
- Hardening van netwerken (U/NW.06)
- Netwerktoegang tot webapplicaties (U/NW.07)
- Netwerkarchitectuur (U/NW.08)

U/NW.01 Operationeel beleid voor netwerken

Het operationeel beleid voor netwerken beschrijft de manier waarop de organisatie omgaat met het inrichten en beschikbaar stellen van netwerken. Configuratie van netwerken vormt de basis voor beveiligde infrastructuur. Het operationeel beleid is een concretere uitwerking van het bovenliggende beleid. Een solide operationeel beleid is daarom een randvoorwaarde voor een veilige inrichting van een webapplicatie-omgeving.

U/NW.01 Operationeel beleid voor netwerken formuleren	
Richtlijn (wie en wat)	Het operationeel beleid voor netwerken formuleert richtlijnen, instructies en procedures voor inrichting en beheer van netwerken.
Doelstelling (waarom)	Betrouwbare communicatie voor de systemen die binnen het netwerk geïnstalleerd zijn.
Risico	Ongewenst netwerkverkeer heeft een nadelige invloed op de performance en bedreigt de veiligheid van de aangesloten systemen. Het vergroot ook de hoeveelheid logverkeer waardoor afwijkingen moeilijker gezien kunnen worden.
Classificatie	Midden
Verwijzingen	CRE 467-784 (Netwerkbeveiliging)

Maatregelen

richtlijnen, instructies en procedures

01 Stel voorschriften (baselines) op voor de veilige inrichting en beheer van netwerken. De baseline dient ook aandacht te geven aan hardening, zie richtlijn U/NW.06.
Maak gebruik van bestaande richtlijnen van leveranciers en erkende kennisinstituten als NIST, SANS, et cetera.

02 Stel procedures en instructies op voor het inrichten van netwerkcomponenten aan de hand van beveiligingstemplates.
Dit is een inhoudelijke eis aan de richtlijn, gericht op configureren van netwerkcomponenten.
Besteed aandacht aan het regelmatig evalueren en bijstellen van de richtlijnen, procedures en instructies. Indien deze instructies en procedures ruimte bieden om af te wijken van de richtlijn, dient hieraan de vereiste van 'comply or explain' gekoppeld te zijn.

03 Stel aansluitvoorwaarden op die beschrijven wanneer een (nieuwe) component op het netwerk mag worden aangesloten.
De aansluitvoorwaarden kunnen verwijzen naar de beveiligingstemplates (/02).
Binnen verschillende netwerkzones (zie richtlijn U/NW.03) kunnen verschillende aansluitvoorwaarden gelden.

U/NW.02 Beschikbaarheid van netwerken

Het netwerk vormt de basisinfrastructuur voor webapplicaties, daarom is het van belang dat het netwerk te maken krijgt met een minimum aan storingen. Ontwerp het netwerk daarom zodanig dat deze zo min mogelijk single-points-of-failure bevat. Vergroot de beschikbaarheid van de infrastructuur met loadbalancing en redundantie. Naast het feit dat het ontwerp van het netwerk zo moet zijn dat er zo min mogelijk uitval zal plaatsvinden, is ook een adequate monitoring, alerting, bewaking en auditing van belang (zie het Beheersingsdomein [1]).

U/NW.02 Beschikbaarheid van netwerken garanderen	
Richtlijn (wie en wat)	Het netwerk is gebaseerd op betrouwbare netwerkcomponenten, ondersteund door redundantie.
Doelstelling (waarom)	Zekerstellen dat er geen zwakke schakels (single-points-of-failure) in voorkomen en dat het netwerk te allen tijde beschikbaar is.
Risico	Onbeschikbaarheid van netwerkcomponenten leiden tot onbeschikbaarheid van het gehele netwerk. Dit leidt tot niet optimale ondersteuning van klanten en stagnatie in zowel productie en als realisatie van bedrijfsdoelstellingen.
Classificatie	Hoog
Verwijzingen	CRE 240-464 (Planning voor onvoorziene gebeurtenissen)

Maatregelen

betrouwbare netwerkcomponenten

01 Configureer de netwerkcomponenten op basis van beveiligings-templates.
Er zijn vastgestelde configuratiebaselines en beveiligingstemplates beschikbaar.

redundantie

02 Voer vooraf gekozen en ontworpen netwerkcomponenten meervoudig uit en configureer deze zodanig dat zij automatisch (zonder menselijke interactie) enkelvoudige storingen opvangen.
De inrichting van netwerkcomponenten is gebaseerd op een vastgesteld inrichtingsdocument/ontwerp, waarin is vastgelegd welke uitgangspunten/ principes gelden voor het netwerk.
De volgende aandachtspunten moeten worden geadresseerd in het inrichtingsdocument/ontwerp:
- *Welke maatregelen zijn geïmplementeerd zodat single-points-of-failure worden voorkomen of de gevolgen worden geminimaliseerd?*
- *Het netwerk-inrichtingsdocument/ontwerp is actueel en op het juiste (organisatie)niveau vastgesteld.*
- *De zakelijke behoeften moeten zijn vastgesteld en er moet een risicoanalyse (B.03/01 [1]) zijn uitgevoerd.*

Routering of redundante netwerkcomponenten (communicatieverbindingen, firewalls, loadbalancers, proxies, routers, switches) zijn mogelijkheden. Extra redundantie kan worden verkregen door infrastructuur meervoudig uit te voeren en over meerdere datacenters te spreiden. Gezien de bijkomende kosten die een dergelijke oplossing brengt, moet vanuit de zakelijke behoefte en de risicoanalyse hiervoor een degelijke onderbouwing zijn.

03 Signaleer automatisch opgevangen storingen (failover) aan de beheerders.
Beheerders ontvangen dit signaal, om te voorkomen dat een automatische failover onopgemerkt blijft. Zij dienen dan voor herstel van de uitgevallen component te zorgen, zodat opnieuw een redundante situatie ontstaat. Zonder herstel kan een single-point-of-failure ontstaan zijn.

Verdieping

Loadbalancers verdelen het verkeer over meerdere systemen

Loadbalancers kunnen verkeer voor een webapplicatie over verschillende gelijkwaardige componenten verdelen. Voor webapplicaties bestaan twee belangrijke loadbalancing-technieken:

Local Server Load Balancing (LSLB): Een LSLB-loadbalancer verdeelt verkeer lokaal (dat wil zeggen binnen hetzelfde datacenter) over verschillende webservers. Uitval van een webserver zal in dit geval niet per definitie leiden tot het niet meer beschikbaar zijn van de website doordat een andere webserver nog wel beschikbaar is.

Global Server Load Balancing (GSLB): Een GSLB-loadbalancer heeft als doel om loadbalancing uit te voeren over geografisch gescheiden locaties. DNS functionaliteit is een mechanisme om GSLB voor webapplicaties te bewerkstelligen.

De GSLB-loadbalancer is hierbij autoritatief voor de zone waarin de webapplicatie zich bevindt en fungeert voor deze zone als DNS-server. Door verzoeken voor de zone te beantwoorden met steeds wisselende ip-adressen, komen gebruikers uit op de verschillende geografisch gescheiden locaties.

Welke loadbalancingoplossing het meest geschikt is voor een bepaalde webapplicatie, is afhankelijk van verschillende variabelen zoals het beschikbare budget, het ontwerp van het netwerk (zie richtlijn U/NW.08) en de architectuur van de webapplicatie (zie richtlijn U/WA.09).

Redundantie is het paraat hebben van extra systemen die taken kunnen overnemen

Veel netwerkcomponenten bieden standaard ondersteuning voor redundantie en bijbehorende statussynchronisatie.
Netwerkcomponenten die in aanmerking komen voor redundante uitvoering zijn:
- communicatieverbindingen;
- firewalls;
- loadbalancers;
- proxies;
- routers;
- switches.

Maar denk ook aan redundant uitvoeren van componenten zoals:
- energievoorziening;
- koeling/klimaatbeheersing;
- voeding;
- controllers.

Automatische failover beperkt de onbeschikbaarheid tot een minimum

Schakel automatisch over naar de redundante systemen als die beschikbaar zijn. Het heeft immers weinig zin om hiervoor menselijke tussenkomst te vereisen, omdat er dan nog steeds een periode van onbeschikbaarheid zal zijn. Echter, er is ook een risico dat de uitval van een component onopgemerkt blijft door de automatische failover via redundante componenten. Een goede bewaking en signalering is daarom noodzakelijk.

U/NW.03 Netwerkzonering

Een Demilitarised Zone (DMZ) is een apart stuk netwerk dat specifiek bedoeld is om webapplicaties – en andere vanaf het internet bereikbare applicaties – in onder te brengen. De DMZ vormt de scheiding tussen het internet enerzijds en het interne netwerk anderzijds. Beperk de verkeersstromen op alle snijvlakken, zodat de kans op het binnendringen van het interne netwerk via het internet zo laag mogelijk wordt gehouden.

Een DMZ kan bestaan uit meerdere compartimenten. Plaats servers, webapplicaties en toepassingen van een gelijk beveiligingsniveau in één gezamenlijk compartiment. Zo komen bijvoorbeeld webproxies in één compartiment, webservers voor internetsites in één compartiment, webservers voor extranetten in één compartiment en databases in één compartiment.

U/NW.03 Netwerkzonering toepassen	
Richtlijn (wie en wat)	Het netwerk is gescheiden in logische of fysieke domeinen (zones), in het bijzonder is er een DMZ die tussen het interne netwerk en het internet gepositioneerd is.
Doelstelling (waarom)	Een beveiligde (of robuuste) netwerkinfrastructuur bieden voor de bedrijfstoepassingen.
Risico	Een aanvaller krijgt ongelimiteerd toegang tot het interne netwerk en de daarop aangesloten systemen.
Classificatie	Hoog
Verwijzingen	CRE 273-600 (Scheid onderdelen met verschillende vertrouwensniveaus)

Maatregelen

logische of fysieke domeinen

01 Deel het netwerk op in zones, op grond van gemeenschappelijke kenmerken van de systemen binnen een domein.
De gemeenschappelijke kenmerken kunnen gekozen zijn op basis van beveiligingsniveau, functionele taakverdeling, of een combinatie van verschillende dimensies. Plaats systemen met verschillende beveiligingsniveaus niet binnen dezelfde zone. Het resulterende zone-ontwerp is actueel, gedocumenteerd en vastgesteld.

02 Sta alleen voor de beoogde diensten noodzakelijke verkeersstromen tussen zones toe.
De noodzakelijke verkeersstromen zijn bekend en gedocumenteerd. Op het koppelvlak van de zones worden andere verkeersstromen actief geblokkeerd. De manier waarop deze blokkade wordt ingevuld hangt af van de aard van het koppelvlak (router, firewall, DMZ).

03 Scheid netwerkzones fysiek of logisch van elkaar, zet een minimale hoeveelheid netwerkcomponenten in op koppelvlakken die deze scheiding handhaven.
De netwerkcomponenten op het koppelvlak van zones vormen hierin het aanvalsoppervlak. Houd dat zo klein mogelijk. Koppeling van netwerkzones kan plaatsvinden door een firewall of (reverse) proxy.

Maatregelen

04 Gebruik verschillende fysieke interfaces voor aansluiting van verschillende (logische) netwerkzones.
Het gaat erom dat een storing aan een netwerkcomponent er nooit toe mag leiden dat de (logische) indeling in zones doorbroken kan worden. De koppelingen tussen verschillende netwerkcomponenten, servers, firewall en andere apparatuur kunnen worden gerealiseerd door één connectiecomponent (switch of hub). Hiermee wordt een fysieke koppeling bewerkstelligd. Door deze fysieke koppeling tussen deze netwerkcomponenten is het in sommige gevallen mogelijk om de logische segmentering van het netwerk via deze netwerkcomponenten te omzeilen. Om te voorkomen dat logische scheidingen kunnen worden omzeild is het raadzaam om koppelingen tussen netwerkcomponenten zoveel mogelijk via separate en onafhankelijke componenten te realiseren.

DMZ

05 Scheid het interne bedrijfsnetwerk en het internet van elkaar door middel van een bufferzone ('demilitarised zone', DMZ) dat bestaat uit frontend-zones en backend-zones.
In de ontwerp- en configuratiedocumentatie is vastgelegd hoe de DMZ is ingericht en is geconfigureerd. De volgende aandachtspunten komen aan de orde:
- *welke webapplicaties worden ontsloten?*
- *welke informatie mag in de DMZ worden opgenomen?*
- *welke ondersteunende applicaties zijn noodzakelijk?*
- *welke compartimenten, koppelvlakken en verkeersstromen tussen de compartimenten zijn noodzakelijk?*
- *welke ip-adressen worden gebruikt (NAT, DHCP)?*
- *welke vaste routepaden om het verkeer door de DMZ te routeren kunnen worden toegepast?*
- *welk uitgaand verkeer vanaf de webserver is noodzakelijk?*
- *zijn aansluitvoorwaarden opgesteld?*

Om de realisatie van de koppelingen tussen netwerkcomponenten op juistheid te kunnen beoordelen kan worden uitgegaan van het ontwerpdocument van de DMZ. De inrichting van de DMZ is gebaseerd op een vastgesteld inrichtingsdocument/ontwerp waarin is vastgelegd welke uitgangspunten/principes gelden voor de toepassing van de DMZ.
Zorg dat het inrichtingsdocument of -ontwerp onderdeel is van het proces wijzigingsbeheer (zie richtlijn C.08 [1]). De ontwerp- en inrichtingskeuzes moeten zijn onderbouwd en op het juiste (organisatie) niveau zijn verantwoord.

Maatregelen	
06	Leg in een DMZ-inrichtingsdocument/ontwerp vast welke uitgangspunten en principes gelden voor de toepassing van de DMZ. *Het DMZ-inrichtingsdocument/ontwerp is actueel, onderbouwd, op het juiste (organisatie)niveau vastgesteld en onderdeel van het proces wijzigingsbeheer (zie richtlijn C.08 [1]). De volgende aandachtspunten moeten worden geadresseerd in het DMZ-inrichtingsdocument/ontwerp:* • *Hoe verloopt de interne/externe routering van webverkeer?* • *Welke vaste routepaden om het verkeer door de DMZ te routeren kunnen worden toegepast?* • *Worden koppelingen tussen netwerkcomponenten doormiddel van separate koppelmechanismen gerealiseerd?* • *Welke beheermechanismen worden toegepast?*
07	Plaats alleen de systemen, (web)applicaties en diensten in de DMZ die in het DMZ-ontwerp voorkomen.
08	Configureer de filters en regels binnen een DMZ conform het DMZ-ontwerp.
09	Laat verkeersstromen tussen interne netwerken en externe netwerken lopen via een DMZ, en controleer en ontkoppel deze op applicatieniveau (sessiescheiding).
10	Sta alleen de voor de beoogde diensten noodzakelijke verkeersstromen tussen internet en de DMZ en tussen de DMZ en het interne netwerk toe. *Dit betekent bijvoorbeeld dat protocollen als RIP, OSPF, Proxy-ARP en ip-pakketten met source-routing en ICMP-redirect/-unreachable berichten vanaf het internet geblokkeerd worden.*

Verdieping

Een netwerk kan topologisch fysiek en logisch worden beschreven. Een topologie illustreert de wijze waarop netwerkcomponenten met elkaar zijn verbonden. Er bestaan verschillende soorten typologieën: vermaasd netwerk (mesh), sternetwerk (star), busstructuur (bus), ringnetwerk (ring) en boomstructuur (tree).

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

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

1. Netwerkzones zijn gescheiden door een firewall en interfaces naar verschillende netwerkzones (bijvoorbeeld naar de DMZ en naar de backoffice) gebruiken verschillende (fysieke) netwerkcomponenten.
2. Er worden (reverse) proxy's inline geplaatst. Inline plaatsing houdt in dat de proxy's twee interfaces krijgen: één interface voor het externe netwerk (buitenkant) en één interface voor het interne netwerk (binnenkant). Al het verkeer van en naar de webapplicatie is in dit geval verplicht om via de proxy te lopen. Het nadeel van een dergelijke plaatsing van een proxy is dat alle webapplicaties via deze proxy moeten verlopen, waardoor men afhankelijk is van ondersteuning van de proxy voor het specifieke type verkeer (bijvoorbeeld een http-proxy voor webverkeer, een SMTP-proxy voor e-mailverkeer, etc.).
   De mogelijkheid tot het inline plaatsen van een proxy is dan ook zeer afhankelijk van de andere webapplicaties die de organisatie via de DMZ ontsluit.

Bepaal in een risicoanalyse welke zoneringen waar in het netwerk nodig zijn.

Slaagt een kwaadwillende erin een server binnen een compartiment aan te vallen, dan heeft de kwaadwillende vanaf deze server alleen toegang tot andere systemen in datzelfde compartiment. De impact van een succesvolle aanval op een systeem wordt hierdoor verkleind. De impact is afhankelijk van de verkeersstromen die zijn toegestaan tussen de verschillende compartimenten. Zo bestaat de kans dat een kwaadwillende via een succesvol aangevallen webserver alsnog een databaseserver in een ander compartiment kan benaderen omdat de firewall bepaalde databaseverbindingen vanaf de webserver richting de databaseserver toestaat.

Hieronder een indicatie van systemen die niet in een DMZ mogen worden geplaatst:
- databaseserver;
- e-mailserver;
- directory-services zoals LDAP en Active Directory.

Hieronder een indicatie van systemen die wel in een DMZ kunnen worden geplaatst:
- webservers;
- mailgateway (MTA);
- (reverse) proxy.

Hanteer als uitgangspunt om alleen de systemen in de DMZ te plaatsen die noodzakelijk zijn om de gewenste functionaliteit te bieden. Ga voor het ontwerp van de DMZ uit van de volgende stappen.

Stel vast welke webapplicaties ontsloten worden

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

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

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

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

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

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

Stel de verkeersstromen tussen de compartimenten vast
Bepaal welke verkeersstromen (dit bevat zowel bron- en bestemmings-ip-adressen als netwerkprotocollen) noodzakelijk zijn voor het ontsluiten van webapplicaties via de DMZ en de ondersteunende applicaties. Deze verkeerstromen bepalen mede het ontwerp van de DMZ.

Volstaat http-verkeer vanaf het internet richting de webapplicatie of zijn ook koppelingen nodig vanuit de DMZ naar het interne netwerk? Op het koppelvlak tussen compartimenten zijn filterfuncties gepositioneerd voor het gecontroleerd doorlaten van gegevens; niet-toegestane gegevens worden tegengehouden.

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

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

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

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

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

U/NW.04 Protectie- en detectiefunctie

Implementeer protectie- en detectiefuncties. De inrichting van ICT-componenten, het netwerkverkeer en de gehanteerde protocollen dienen een robuuste eenheid vormen om bescherming te kunnen bieden tegen aanvallen en aanvallen te kunnen detecteren. Dit verbetert de beschikbaarheid van de te leveren diensten.

U/NW.04 Protectie- en detectiefunctie toepassen	
Richtlijn (wie en wat)	De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van protectie- en detectiemechanismen.
Doelstelling (waarom)	Het detecteren van aanvallen (onder andere (D)DoS) om te voorkomen dat de vertrouwelijkheid, integriteit en/of beschikbaarheid van geleverde services negatief wordt beïnvloed.
Risico	Via netwerkcomponenten of netwerkverkeer wordt vertrouwelijkheid, integriteit en/of beschikbaarheid aangetast, zonder dat dit (tijdig) gedetecteerd wordt en zonder dat hier adequaat op geacteerd kan worden.
Classificatie	Hoog
Verwijzingen	CRE 132-146 (Bescherming tegen, detectie van en respons op netwerkaanvallen) CRE 058-083 (Monitoring) CRE 623-550 (Bescherming tegen denial of service) CRE 842-876 (Logging en foutafhandeling) CRE 463-577 (Incidentrespons)

Maatregelen

protectiemechanismen

01 Zorg voor een actueel DMZ-inrichtingsdocument dat inzicht geeft welke protectiemechanismen zijn betrokken.
Het DMZ-inrichtingsdocument (zie richtlijn U/NW.03/05) geeft onder andere inzicht in: gehanteerde uitgangspunten, inrichtingskeuzes, geïmplementeerde maatregelen tegen (D)DoS-aanvallen, vaststelling van het document op het juiste (organisatie)niveau.

02 Pas anti-spoofingmechanismen toe in het netwerk.
Unicast Reverse-Path Forwarding (URPF) controleert op een interface of een ip-pakket afkomstig is van een bron ip-adres dat volgens de routeringstabel bereikbaar is via datzelfde interface.
Ip-adressen die nog niet door IANA zijn uitgegeven worden geblokkeerd (bogon lists).

03 Reguleer dataverkeer met access control lists (ACL's) op basis van bijvoorbeeld ip-adres of poortnummer.

Maatregelen

04 Stel de firewall-regels op, configureer deze via een proces en review dit periodiek.
De regels zijn opgesteld door aangewezen functionaris, rekening houdend met informatiebeveiligingsbeleid en gebaseerd op 'least privilege'.

detectiemechanismen

05 Monitor inkomend en uitgaand verkeer in het netwerk.

06 Monitor de infrastructuur zodat detectie van (DDoS-)aanvallen mogelijk is.
Gebruik hiervoor standaarden zoals sFlow of Jflow.

07 Implementeer Intrusion Detection Systemen (IDS) en Intrusion Prevention Systemen (IPS).
Leg in de ontwerp- of configuratiedocumentatie vast waar en hoe IDS'en en IPS'en worden ingezet en beschrijf daarbij:
De zakelijke behoeften en maatregelen. Rapportage van de risicoanalyse (B.03/01 [1]) waarop de beslissing is gebaseerd.
Een plan met daarin de activiteiten die worden uitgevoerd (wie, wat en wanneer) indien logrecords op kwaadwillend misbruik duiden, geïmplementeerde maatregelen niet aan de gestelde eisen en/of verwachtingen hebben voldaan of tekortkomingen hebben opgeleverd.
Welke acties op basis van welke bevindingen automatisch worden uitgevoerd door de IPS.

08 Richt de IDS'en en IPS'en in op basis van een geaccordeerd inrichtingsdocument/ontwerp.
Zorg dat het inrichtingsdocument of -ontwerp onderdeel is van het proces wijzigingsbeheer (zie richtlijn C.08 [1]).

09 Houd rapportage(tool)s beschikbaar voor analyses van de door detectiemechanismen vastgelegde gegevens.

Verdieping

Bescherm tegen (D)DoS-aanvallen

Het NCSC geeft een actueel advies over bescherming tegen (D)DoS-aanvallen in de publicatie Technische maatregelen voor continuïteit voor online diensten.[18] Bepaal in een risicoanalyse welke maatregelen nodig zijn in relatie tot de beschikbaarheids-behoefte van de dienstverlening. De factsheet Continuïteit van online diensten beschrijft de doelwitten en gevolgen van (D)DoS-aanvallen.[19]

Detecteer aanvallen

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

18 Zie: https://www.ncsc.nl/ddos/technische-maatregelen-voor-de-continuiteit-van-online-diensten
19 Zie: https://www.ncsc.nl/ddos/continuiteit-van-online-diensten

- Network-based Intrusion Detection System (NIDS). Een NIDS wordt als losstaand component in het netwerk geplaatst waarna deze component netwerkverkeer opvangt.
- Host-based Intrusion Detection System (HIDS). Een HIDS wordt op een server geïnstalleerd waarna het HIDS continu de activiteiten op deze server monitort. Het HIDS kijkt hierbij niet alleen naar het netwerkverkeer (zoals het NIDS) maar ook naar logging en veranderingen op het systeem zelf.
- Application-based IDS (APIDS). Een application-based IDS wordt specifiek ingezet voor het monitoren van misbruik van een specifieke webapplicatie of een specifiek protocol.
- Een Intrusion Prevention System (IPS). Dit is een toepassing die naast detectie ook automatisch beschermende acties kan ondernemen bij gedetecteerd misbruik. Denk hierbij bijvoorbeeld aan het droppen van ip-pakketten en het blokkeren van ip-adressen.

Het detecteren van aanvallen gebeurt veelal op basis van bekende aanvalspatronen. Deze manier van detectie, op basis van 'handtekeningen' van bekende aanvallen, wordt ook wel signature-based genoemd. Tegenover de signature-based IDS'en staan de anomaly-based systemen. Deze systemen werken niet op basis van handtekeningen, maar op basis van afwijkingen van normaal gedrag.

Bij het inrichten van een NIDS is het belangrijk goed te bekijken welke meetpunten interessant zijn voor het NIDS om op die manier een zo compleet mogelijk beeld te krijgen van aanvallen op de omgeving. Bekijk daarbij aan de hand van de DMZ-opbouw en de compartimentering (zie richtlijn U/NW.03) in het algemeen wat interessante meetpunten zijn.Om kwalitatief hoogwaardige informatie te verzamelen en deze effectief te verwerken, is het belangrijk om aandacht te schenken aan de volgende zaken.

- Voorzie signature-based systemen regelmatig van de nieuwste aanvalspatronen (bij voorkeur automatisch).
- Zorg ervoor dat databases voldoende ruimte bieden om de grote hoeveelheid gegevens die een NIDS produceert onder te kunnen onderbrengen.
- Beslis hoe lang logging moet worden opgeslagen en hoe deze moet worden gearchiveerd.
- Stel de alarmering van het NIDS doorlopend bij. Beheerders zullen een NIDS dat continu alarmen uitzendt, niet meer serieus nemen. Onderschat daarbij de hoeveelheid mankracht die nodig is voor het monitoren en onderzoeken van anomalieën en false positives niet.

IDS'en en IPS'en worden ook als clouddienstverlening aangeboden, waarbij een aantal van deze taken door de dienstverlener worden verzorgd.

Stel eisen aan loginformatie

Regel een goede beheerprocedure in voor het IDS. Leg bijvoorbeeld vast wie regelmatig de logging van het IDS bekijkt. Daarnaast is het, ter verbetering van de leesbaarheid van de logging, aan te raden filters op de logging te plaatsen (zie ook richtlijn C.06 [1]).

Zorg voor de opvolging van meldingen

Er moet actie worden ondernomen indien logrecords op kwaadwillend misbruik duiden, geïmplementeerde maatregelen niet voldoen aan de gestelde eisen en/of verwachtingen of tekortkomingen opleveren (zie ook richtlijn C.07 [1]).

U/NW.05 Beheer- en productieomgeving

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

Er zijn verschillende vormen van beheer met ieder hun eigen maatregelen:

- **Contentbeheer**
  Contentbeheer wordt over het algemeen door de organisatie zelf, vanaf hun eigen werkplek, uitgevoerd en hiervoor gelden dan de aandachtspunten zoals die zijn benoemd in richtlijn U/NW.03. De contentbeheerders moeten op een veilige en gecontroleerde wijze toegang krijgen tot de systemen waar de content is opgeslagen. Denk hierbij aan webservers, databases en contentmanagementsystemen.
  Afhankelijk van de mogelijkheden die de contentbeheerders hebben, bijvoorbeeld het ontwikkelen van formulieren en dynamische content, moet rekening worden gehouden met andere relevante maatregelen zoals die in deze richtlijnen zijn beschreven.
- **Applicatiebeheer**
  Voor applicatiebeheer gelden in hoofdlijnen de richtlijnen zoals die zijn beschreven in het domein U/WA.
- **Technisch beheer**
  Deze beheerders benaderen de systemen die zij beheren veelal via terminal-emulatie of soortgelijke applicaties. Vaak hebben ze de mogelijkheid om commando's uit te laten voeren en configuraties naar eigen inzicht aan te passen.

Scheid beheer- en productieverkeer. Onderbouw de gemaakte beslissingen en stel ze op het juiste (organisatie)niveau vast, documenteer en onderhoud ze zodat altijd over een actueel ontwerp van het netwerk wordt beschikt. Gebruik steeds als uitgangspunt wat minimaal noodzakelijk is om de gewenste functionaliteit te kunnen bieden.

U/NW.05 Beheer- en productieomgeving afschermen	
Richtlijn (wie en wat)	Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd.
Doelstelling (waarom)	Het voorkomen van misbruik van de beheervoorzieningen vanaf het internet.
Risico	Door het ontbreken van afdoende afscherming kunnen eindgebruikers beheerdersautorisaties verwerven.

U/NW.05 Beheer- en productieomgeving afschermen	
Classificatie	Hoog
Verwijzingen	CRE 273-600 (Scheid onderdelen met verschillende vertrouwensniveaus)

Maatregelen

beheer- en productieverkeer	
01	Geef in een inrichtingsdocument aan op welke wijze contentbeheer (web- en database-content), applicatiebeheer en technisch beheer worden uitgeoefend. *Zorg dat dit document onderdeel is van het proces wijzigingsbeheer (zie richtlijn C.08 [1]). De ontwerp- en inrichtingskeuzes moeten zijn onderbouwd en op het juiste (organisatie)niveau zijn verantwoord.*
02	Stel een overzicht op van de ontsluiting van storage en de aansluiting op een back-upinfrastructuur.
03	Stel een overzicht op van ondersteunende communicatieprotocollen voor beheer. *Gebruik SSH, SFTP (niet FTP), https (niet http).*
04	Stel een overzicht op van ondersteunende applicaties voor beheer.
05	Leg vast op welke wijze beheerders toegang krijgen tot de beheeromgeving.

Verdieping

Pas bewezen beheermechanismen toe

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

- Secure Shell (SSH) in plaats van Telnet;
- SSH File Transfer Protocol (SFTP) of FTP over SSL (FTPS) in plaats van File Transfer Protocol (FTP);
- https in plaats van http voor webinterfaces.

Regel beheerderstoegang tot het beheerdomein in

Stel vast hoe beheerders toegang krijgen tot het beheerdomein. Hier zijn verschillende mogelijkheden voor:

- Implementeer beheerclients in het beheerdomein, die alleen te gebruiken zijn in een afgeschermde ruimte. Beheer over de omgeving kan alleen plaatsvinden via deze fysiek afgeschermde beheerclients.
- Implementeer beheerclients in het beheerdomein die op basis van een remote interface te benaderen zijn voor een beperkte groep werkstations in het interne netwerk. Beheerders maken vanaf hun werkstation in het interne netwerk een verbinding

met de beheerclients en kunnen vervolgens via deze beheer-clients het beheer over de omgeving uitvoeren.
- Implementeer een apart beheer-LAN binnen het interne netwerk en sta verbindingen richting het beheerdomein alleen toe vanuit dit beheer-LAN.
- Implementeer een Virtual Private Network (VPN) op het moment dat het beheer remote via het internet wordt uitgevoerd. Een VPN-tunnel kan ook toegepast worden als het beheer vanaf het bedrijfsnetwerk wordt uitgevoerd.

U/NW.06 Hardening van netwerken

De hardening van netwerken is het resultaat van de toepassing van het hardeningsproces (zie richtlijn B.10 [1]).

De meeste systemen voeren een beperkt aantal functies uit. Ontdoe het systeem van software, gebruikersaccounts en diensten die niet gerelateerd of niet strikt noodzakelijk zijn voor het functioneren van het systeem om de aanvalsmogelijkheden te beperken. Wanneer dat niet mogelijk is, moeten alle niet strikt noodzakelijke functionaliteiten zijn uitgeschakeld. Systeemhardening is een leverancierspecifiek proces, aangezien de verschillende leveranciers het systeem op verschillende manieren configureren en voorzien van verschillende diensten tijdens het installatieproces.
- Indien (externe) systemen, zoals webservers en mailservers hun type en versienummer adverteren, wordt het een aanvaller makkelijker gemaakt om bekende zwakke plekken van deze systemen te exploiteren. Het verbergen van het versienummer helpt ten dele, maar met fingerprintingtechnieken kan een aanvaller vaak alsnog achterhalen welke software en versie wordt gebruikt.
- Systemen die onnodige diensten draaien en poorten open hebben die niet open hoeven te staan zijn makkelijker aan te vallen omdat deze diensten en poorten mogelijkheden bieden om het systeem aan te vallen.

Beperk de communicatiemogelijkheden van het systeem tot het strikt noodzakelijke. Eén van de manieren om dit te bereiken is door onnodige services onbereikbaar te maken door ze te verwijderen of uit te schakelen. Door benodigde services in kaart te brengen en vervolgens de afhankelijkheden te bepalen, ontstaat er een lijst van services die minimaal op het systeem moeten staan. Verwijder alle overige services, of schakel ze uit als ze niet verwijderd kunnen worden. Niet-actieve maar wel aanwezige services op een systeem kunnen uiteindelijk toch tot een kwetsbaar systeem leiden aangezien kwetsbare programmacode op het systeem aanwezig is.

U/NW.06 Hardening van netwerken configureren	
Richtlijn (wie en wat)	Voor het configureren van netwerken is een hardeningrichtlijn beschikbaar.
Doelstelling (waarom)	Beperken van het netwerkverkeer tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.
Risico	Bedoeld of onbedoeld negatief beïnvloeden van het netwerkverkeer, waardoor vertrouwelijkheid, integriteit en/of beschikbaarheid van het netwerk-verkeer niet gegarandeerd is.
Classificatie	Hoog
Verwijzingen	CRE 467-784 (Netwerkbeveiliging)

Maatregelen	
hardeningrichtlijn	
01	Houd een actueel overzicht bij van de noodzakelijke netwerkprotocollen, -poorten en -services. *Zorg dat dit document onderdeel is van het proces wijzigingsbeheer (zie richtlijn C.08* [1]*).*
02	Schakel op de netwerkcomponenten alle netwerkprotocollen, -poorten en –services uit, behalve de noodzakelijke. *Bij voorkeur worden uitgeschakelde netwerkprotocollen, -poorten en -services geheel verwijderd.*
03	Pas de (beveiligings)configuraties van netwerkprotocollen, -poorten en -services op de netwerkcomponenten aan conform richtlijnen.
04	Wijs op switches netwerkpoorten toe aan Virtual LANs (VLANs) op basis van het MAC-adres van de aangesloten systemen (port security).

Verdieping

Neem hardeningsmaatregelen op netwerkniveau

Onderstaand enkele voorbeelden van hardeningsmaatregelen op netwerkniveau:

- Sluit beheermogelijkheden zoveel mogelijk af. Bied webinterfaces voor beheerfuncties alleen aan via beheercompartimenten (zie richtlijn U/NW.05).
- Sta beheer alleen toe vanaf vooraf gedefinieerde ip-adressen.
- Maak gebruik van phishingresistente authenticatiemechanismen voor het uitvoeren van beheer op de componenten.
- Maak gebruik van versleutelde verbindingen bij beheerwerkzaamheden (zie richtlijn U/NW.05).
- Harden het onderliggende besturingssysteem.
- Besteed aandacht aan de beveiligingsconfiguratie van netwerkservices en -protocollen: Simple Network Management Protocol (SNMP), Network Time Protocol (NTP), SYSLOG, Trivial FTP (TFTP), finger en routeringsprotocollen zoals Border Gateway Protocol (BGP) en Open Shortest Path First (OSPF).
- Gebruik Resource Public Key Infrastructure (RPKI) om te voorkomen dat routeringen door kwaadwillenden kunnen worden omgeleid.
- Schakel alle ongebruikte protocollen, services en netwerkpoorten uit (en verwijder ze).
- Maak op switches gebruik van Virtual LANs (VLAN) en beperk de toegang tot netwerkpoorten op basis van MAC-adres.

Veel leveranciers leveren netwerkcomponenten in de vorm van appliances waarop weinig extra hardeningsmaatregelen mogelijk zijn. In de gevallen dat een netwerkcomponent echter niet gebaseerd is op een appliance, harden dan het onderliggende systeem (zie ook richtlijn U/PW.07).

Voorbeelden van protocollen die veelal standaard zijn ingeschakeld op netwerkcomponenten maar in veel gevallen niet nodig zijn, zijn Cisco Discovery Protocol (CDP) en Spanning Tree Protocol (STP). Bedenk dat niet-actieve maar wel aanwezige services op een systeem uiteindelijk toch tot een kwetsbaar systeem kunnen leiden aangezien kwetsbare programmacode op het systeem aanwezig is. Veiliger is het daarom om onnodige services volledig van het systeem te verwijderen.

Harden de DNS-infrastructuur

Door de vitale rol die het Domain Name System (DNS) speelt in het bereikbaar houden van webapplicaties, verdient de beveiliging van DNS-services extra aandacht. Door de DNS-infrastructuur te hardenen, wordt DNS-misbruik voorkomen. Aandachtspunten bij het beveiligen van DNS-services zijn:[20]

- Maak gebruik van de meest recente software, zodat het misbruik van bekende beperkingen en kwetsbaarheden zoveel mogelijk wordt voorkomen. Het maskeren van oudere versies door bijvoorbeeld het blokkeren van hostname.bind-query's is niet afdoende, aangezien er andere manieren zijn om de versie van uw software te achterhalen (DNS-fingerprintingtechnieken).
- Maak onderscheid tussen autoritatieve nameservers (waar de domeinnamen/zonefiles op draaien) en recursieve resolvers (waar client-systemen hun DNS-vragen aan stellen). Sommige DNS-software kan beide functies combineren.
- Zorg dat alleen geautoriseerde systemen een zonetransfer kunnen uitvoeren van autoritatieve nameservers. Doorgaans betekent dit dat alleen primaire en secundaire nameservers dit onderling mogen. Dit kan door in de configuratie de betreffende ip-adressen op te geven. Eventueel kan dit extra beveiligd worden via TSIG (RFC2845[21]). Zonetransfers blokkeren door TCP-poort 53 te blokkeren op de firewall, is niet de geëigende methode. TCP-poort 53 is een essentieel onderdeel van het DNS-protocol en dient enkel te worden geblokkeerd in de firewall als daar zwaarwegende redenen voor zijn. Blokkeer het in geen geval als manier om zonetransfers te voorkomen en blokkeer het evenmin wanneer op de autoritatieve nameservers gebruik wordt gemaakt van DNSSEC of wanneer DNS-antwoorden om een andere reden groter (kunnen) zijn dan 512 bytes. Blokkeer TCP-poort 53 ook niet op resolvers.
- Maak gebruik van meerdere autoritatieve nameservers per zone en plaats deze netwerk-topologisch van elkaar gescheiden. Zodoende is de kans groter dat domeinnamen bereikbaar blijven bij gedeeltelijke uitval van uw netwerk of servers. Wanneer de impact van een DDoS-aanval op nameservers groot is en het risico daarop niet ondenkbaar, maak dan de

20 Aanvullende informatie over de manier waarop men DNS kan beveiligen is te vinden in de publicatie 'Secure Domain Name System (DNS) Deployment Guide' van het National Institute of Standards and Technology (NIST): http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-81-2.pdf

21 http://www.ietf.org/rfc/rfc2845.txt

autoritatieve-nameserverinfrastructuur nog robuuster. Maak ook gebruik van minimaal twee resolvers.
- Overweeg maatregelen tegen DNS-rebindingaanvallen, door resolvers dusdanig te configureren dat zij nooit externe domeinnamen zullen resolven naar interne ip-adressen.
- Maak gebruik van DNSSEC[22],[23] (DNS Security Extensions) hiermee kan de authenticiteit van DNS-antwoorden worden gewaarborgd. Hiermee wordt voorkomen dat deze onderweg worden gemanipuleerd. Op autoritatieve nameservers worden DNS-gegevens met DNSSEC voorzien van een digitale handtekening. Deze worden aan de kant van de resolvers gevalideerd. DNS over https (DoH) kan hier aanvullend op worden gebruikt, maar is geen vervanger van DNSSEC.[24]
- Wanneer u beslist geen zonetransfers wilt toestaan, kies dan bij gebruik van DNSSEC voor NSEC3, waarmee zone enumeration, dat kenmerkend is voor NSEC, aanzienlijk wordt bemoeilijkt.[25]
- Zorg dat resolvers alleen ter beschikking staan aan uw (interne) gebruikers en stel ze in geen geval open voor de rest van het internet.
- Beperk de beheerderstoegang tot nameservers en laat alleen de noodzakelijke beheerders toe. Overweeg eventueel gescheiden systemen, waar uitsluitend DNS-beheerders toegang toe krijgen.
- Verwijder onnodige records uit de zone. Dergelijke records (bijvoorbeeld HINFO- en TXT records) leveren een kwaadwillende extra informatie.
- Ruim zones waarvoor u niet meer verantwoordelijk bent op van de autoritative nameservers.
- Houd het (netwerk)verkeer op nameservers nauwlettend in de gaten (zie ook richtlijnen C.06 en C.07 [1]). Wees alert op afwijkende patronen in logging en overweeg het gebruik van een Intrusion Prevention System (IPS). Omdat DNS vaak open staat in firewalls, wordt het bijvoorbeeld door kwaadwillenden misbruikt als manier om interne informatie naar buiten weg te sluizen. Het kan ook zijn dat kwaadwillenden uw name servers misbruiken bij een DDoS aanval gericht aan derden (DNS-amplificatie).

U/NW.07 Netwerktoegang tot webapplicaties

Als webapplicaties ook bereikbaar moeten zijn vanaf het interne netwerk moet hiervoor een koppeling tot stand gebracht worden, wat een extra verkeersstroom introduceert (zie richtlijn U/NW.03). Deze extra verkeersstroom mag geen nieuwe beveiligingsrisico's introduceren.

Voorkom dat beveiligingsbeperkingen die zijn opgelegd door componenten in de DMZ (onbedoeld) door interne medewerkers worden omzeild. Onderwerp gebruikers binnen de organisaties aan dezelfde netwerkmaatregelen als gebruikers van buiten de organisatie. Bekrachtig vastgestelde routepaden (zie richtlijn U/NW.03) ook voor intern netwerkverkeer. Hierdoor zal intern netwerkverkeer in grote lijnen dezelfde weg moeten volgen als internetverkeer, met als gevolg dat intern netwerkverkeer op dezelfde plek de DMZ binnenkomt als regulier internetverkeer. Dit geldt voor productieverkeer en niet voor netwerkverkeer in verband met beheerdoeleinden, zoals in richtlijn U/NW.05 beschreven.

U/NW.07 Netwerktoegang tot webapplicaties garanderen	
Richtlijn (wie en wat)	De opzet van het netwerk garandeert dat alle gebruikers langs dezelfde netwerkpaden toegang krijgen tot webapplicaties, ongeacht hun fysieke locatie.
Doelstelling (waarom)	Voorkom (nieuwe) beveiligingsrisico's omdat de webapplicaties ook bereikbaar moeten zijn vanaf het interne netwerk voor gebruikers binnen de organisatie.
Risico	Een aanvaller krijgt mogelijkheden om de toegangsbeveiliging voor externe gebruikers te omzeilen.
Classificatie	Midden
Verwijzingen	CRE 467-784 (Netwerkbeveiliging)

22 http://www.dnssec.nl/home.html

23 DNSSEC staat op de 'pas-toe-of-leg-uit' lijst https://forumstandaardisatie.nl/open-standaarden/dnssec. Overheden zijn verplicht de open standaarden, die op de lijst met 'pas toe of leg uit'-standaarden staan, bij aanschaf van ICT-systemen en -diensten te eisen.

24 Zie voor meer informative over de toepassing van DNS over https: https://www.sidn.nl/nieuws-en-blogs/dns-over-https-verovert-de-browserwereld

25 Zie voor aanbevelingen voor het instellen van NSEC3: https://www.rfc-editor.org/rfc/rfc9276.html

Maatregelen

netwerkpaden

01 Bied gebruikers slechts één netwerkpad om een webapplicatie te bereiken.
Dit blijkt uit het netwerkontwerp.
Het is toegestaan voor verschillende gebruikersgroepen van verschillende (fysieke) netwerkpaden gebruik te maken, zolang deze qua logische opzet maar identiek zijn. Dit kan bijvoorbeeld een oplossing zijn in geval van (zeer) drukbezochte websites.

U/NW.08 Netwerkarchitectuur

De architectuur van netwerken beschrijft de functionele en beveiligingssamenhang en legt de relatie met het algemene ICT-landschap. Realiseer alle netwerkcomponenten vanuit een eenduidig gemeenschappelijk beeld conform deze architectuur. Pas hiervoor de richtlijnen, instructies en procedures van richtlijn U/NW.01 toe. Op deze manier wordt zeker gesteld dat iedere netwerkcomponent aan de vereiste functionele en beveiligingsdoelen bijdraagt.

De architectuur documenteert gemaakte ontwerp- en inrichtingskeuzen en verantwoordt en onderbouwt deze keuzen.
Het architectuurdocument beperkt zich dus niet tot het vastleggen wat de huidige situatie is, maar ook waarom deze zo is. Neem verwijzingen naar functionele eisen, risicoanalyses, best practices en alternatieven op om dit te onderbouwen. Alle gedocumenteerde ontwerpen en inrichtingskeuzen moeten te herleiden zijn naar functionele eisen. Documentatie speelt ook een rol bij het bepalen van de impact van wijzigingen en het voorkomen van ontwerpfouten. Documentatie moet dan ook na elke wijziging worden bijgewerkt en oude documentatie moet worden gearchiveerd.
Dit geldt zowel voor systeem- als gebruikersdocumentatie.

Documentatie moet goed leesbaar zijn, voorzien zijn van een datum (evenals de revisiedata), een eigenaar hebben, op een ordelijke manier worden onderhouden en gedurende een bepaalde periode worden bewaard. Stel procedures en verantwoordelijkheden voor het opstellen en aanpassen van documentatie vast en houd ze bij.

Documentatie kan gevoelige informatie bevatten en er moeten dan ook maatregelen zijn getroffen om de documentatie te beveiligen tegen ongeautoriseerde toegang.

Beschrijf in de documentatie:
- hoe wordt omgegaan met risicomanagement, de benodigde bedrijfsmiddelen, de geïmplementeerde maatregelen en noodzakelijke mate van zekerheid;
- de plaatsing van servers en aansluiting van interne netwerkcomponenten en netwerkkoppelingen met externe netwerken, zodat de werking van de ICT-infrastructuur begrijpelijk is en de impact van wijzigingen goed kunnen worden bepaald;
- de instellingen van de ICT-componenten, zodanig dat duidelijk is waarom voor bepaalde instellingen gekozen is. Besteed hierbij aandacht aan de standaardwaarden voor systeeminstellingen.

Onderhoud voor elke maatregel documentatie. Controleer en documenteer daarnaast regelmatig het bestaan van maatregelen, afhankelijk van de gevoeligheid van de webapplicatie. De mate van compliance wordt aan de verantwoordelijke voor de webapplicatie en de beveiligingsfunctionaris gerapporteerd.

U/NW.08 Netwerkarchitectuur vastleggen	
Richtlijn (wie en wat)	Voor het implementeren, integreren en onderhouden van netwerken zijn architectuurvoorschriften, beveiligingsvoorschriften en de benodigde documentatie beschikbaar.
Doelstelling (waarom)	Een netwerklandschap bieden dat een betrouwbare verwerking garandeert.
Risico	Onvoldoende beheersing van netwerken, waardoor de stabiliteit van ondersteunde systemen (platformen) niet gegarandeerd is en mogelijkheden voor misbruik ontstaan.
Classificatie	Midden
Verwijzingen	CRE 467-784 (Netwerkbeveiliging) CRE 708-355 (Veilige architectuur) CRE 766-162 (Analyse en documentatie)

Maatregelen

architectuurvoorschriften

01 Onderhoud architectuurvoorschriften actief.
Zorg dat dit document onderdeel is van het proces wijzigingsbeheer (zie richtlijn C.08 [1]*).*

beveiligingsvoorschriften

02 Stel hardeningrichtlijnen op voor netwerken, aantoonbaar afgeleid uit de architectuur.
Het gaat hier om de aantoonbare, navolgbare relatie tussen wat de architectuur beschrijft en de concretisering in richtlijnen. Bij de registratie van de inrichting wordt deze lijn doorgetrokken naar de daadwerkelijke configuratie en getroffen maatregelen.
Zie ook U/NW.06.

03 Stel inrichtingsrichtlijnen op voor registratie van beveiligingsevents (logging) , aantoonbaar afgeleid uit de architectuur.

04 Stel inrichtingsrichtlijnen op voor de restricties van faciliteiten/utilities en de uitschakeling van features en poorten van netwerkcomponenten.

05 Stel richtlijnen op voor periodieke security-updates, herstelbaarheid van netwerkcomponenten en bescherming (van de stroomvoorziening) van kritieke netwerkcomponenten (zoals UPS/no-breaks voor de stroomvoorziening op de core-switches).

documentatie

06 Documenteer de plaatsing van servers en aansluitingen van interne netwerkcomponenten en netwerkkoppelingen met externe netwerken.
De documentatie is begrijpelijk en voorzien van relevante schema's, zodat de werking van de ICT-infrastructuur duidelijk is en de impact van wijzigingen goed kan worden bepaald.

Bijlage A: Conformiteitsindicatoren

aanmelden
Bij het aanmelden verandert het autorisatieniveau van de gebruiker. Op dat ogenblik vervalt de sessie die geldig was voor het oude autorisatieniveau, en wordt die vervangen door een nieuwe sessie (en nieuwe sessie-identifier).

analyseren
Het ontleden en onderzoeken van de vastgelegde loggingsgegevens op bedreigingen en of ongeoorloofde activiteiten.

architectuurvoorschriften
De architectuurvoorschriften zijn een levend document, dat bijdraagt aan een samenhangend en consistent geheel van technieken en maatregelen.

automatiseren van arbeidsintensieve taken (workflow)
Het automatiseren van arbeidsintensieve taken heeft betrekking procesmatige en procedurele inrichting van toegangsvoorzieningsomgeving. De processen die hierbij een rol spelen zijn bijvoorbeeld aanmaken, wijzigen en verwijderen van gebruikersinformatie en bijbehorende autorisaties (de complete levenscyclus). Hiermee is het op- afvoeren van gebruikers eenvoudiger te regelen en te beheren. Het identiteit- en toegangsmanagementsysteem dat hiervoor wordt ingezet zal deze processen moeten ondersteunen.

baseline
Een baseline geeft het afgewogen minimale beveiligingsniveau waaraan een organisatie moet (willen) voldoen.

bedrijfsprocessen
Alle bedrijfsprocessen, functies, rollen, et cetera die bij het aanbieden, gebruiken en onderhouden van een webapplicatie betrokken zijn, zijn geïnventariseerd en gekarakteriseerd.

beheer- en productieverkeer
Binnen de netwerkinfrastructuur zijn compartimenten aangebracht. Binnen deze compartimenten geldt een gelijk beveiligingsniveau voor het netwerkverkeer en de aangesloten systemen. Voor het beheer wordt een apart beheercompartiment gebruikt. Beheerverkeer vanuit het beheercompartiment blijft logisch gescheiden van het normale netwerkverkeer, door toepassing van cryptografische technieken.

beleid
Het beleid beschrijft hoe een organisatie haar missie op en visie richting wil geven. Een beleid is algemeen of specifiek van aard zijn. Een specifiek beleid is bijvoorbeeld een internetbeleid. Dit internetbeleid beschrijft hoe een organisatie op internet aanwezig wil zijn, bijvoorbeeld met een website. Hierin spelen inhoud, presentatie en veiligheid een hoofdrol.

bekende, toegestane communicatiestromen
Alles wat niet noodzakelijk is voor de (web)applicatie is verboden, om problemen met ongebruikte functionaliteit en protocollen te voorkomen. De veronderstelling is dat van de (web)applicatie bekend is wat deze nodig heeft en dat dit gedocumenteerd is. Het gevolg is dat alleen het verkeer dat gedocumenteerd is de lokale firewall mag passeren.

betrouwbare netwerkcomponenten
Netwerkcomponenten zijn alle typen systemen (zoals: router, firewall) die in de netwerk zijn opgenomen voor het verzorgen van juiste en veilige netwerkverbindingen. Deze systemen dienen adequaat op basis van een configuratiebaseline te zijn geconfigureerd. Niet relevante en niet noodzakelijke services zijn binnen deze systemen moeten uit voorzorg worden uitgeschakeld.

beveiligd
Beveiligde inrichting is gerelateerd aan maatregelen met betrekking tot juiste en tijdige werking en beschikbaarheid van de registratie en detectiefunctie, beveiliging van logbestanden tegen manipulaties, alternatieve paden bij uitval, veilig stellen van

loggingbestanden. Juiste en tijdige werking houdt verband met bijtijds activeren van de registratiefunctie. Hiervoor is het van belang dat systeemklokken van systemen gesynchroniseerd zijn.

beveiligingseisen en -wensen
Beveiligingseisen ten aanzien van webapplicaties betreffen de te treffen maatregelen voor het beveiligen van webapplicaties zelf en het beveiligen van systemen, services en data bij het schenden van beveiligingsprocedures en bij het optreden van beveiligingsincidenten.

beveiligingsorganisatie
De beveiligingsorganisatie beschrijft de structuur van een divisie (of een entiteit) die verantwoordelijk is voor het vormgeven en effectief en efficiënt inzet van ICT-middelen. Hierbij dienen de rollen, de uit te voeren activiteiten en de relaties tussen actoren als units te worden beschreven. Tevens is van belang dat binnen de beveiligingsorganisatie de procedurebeschrijving beschikbaar is die aangeven hoe functies en verantwoordelijkheden voor de beveiliging worden ingevuld. Een overzicht van de benoemde functies en daarbij behorende verantwoordelijkheden dient ook beschikbaar te zijn.

beveiligingsvoorschriften
De beveiligingsvoorschriften zijn een specifiek onderdeel van de architectuur, die eventueel in een losstaand document zijn vastgelegd. Zij dragen bij aan een veilige basis voor de realisatie van webapplicaties.

bewaken
Het (controleren) waarnemen en analyseren (proactief beheren) van informatie ten aanzien vastgelegde acties in het systeem (trendanalyse). Hierbij worden ook meetwaarden ten opzichte norm/planwaarden bewaakt bedoeld om uitzonderingen te signaleren (alarmeringen). Alarmeringen zijn automatische mededelingen door het detectie systeem voor een naderend gevaar of ongewenste situatie.

condities
Condities beschrijven de grenzen waarbinnen actoren op verschillende hiërarchische lagen mogen opereren. Zoals schillende beleid soorten (beveiligingsbeleid, PKI-beleid) waarin de beperkingen, richtinggevende adviezen en opties voor toepassingen worden vermeld.

configuratie-baseline
Voorschrift voor de configuratie van de webserver. Dit voorschrift zal in ieder geval enkele basale instellingen beschrijven om onnodig lekken van informatie tegen te gaan.

contract
Een formeel document waarin onder meer de overeengekomen functionele en beveiligingseisen zijn vermeld. De contracten worden slechts door daartoe bevoegde functionaris afgesloten. De contracten die hieruit voortkomen, dienen steeds actueel en geldig te zijn. Het verloop van de levering van diensten en middelen wordt, op basis van het contract, geëvalueerd.

controleerbaar maken van het gebruik
De toegang van gebruikers tot systemen moeten worden door het systeem geregistreerd voor controle doeleinden. Er moet kunnen worden vastgelegd, met name in fraude gevoelige omgevingen, welke gebruiker op basis van zijn/autorisatie welke acties heeft uitgevoerd.

cryptografische technieken
Gegevens worden beschermd tegen ongeautoriseerde kennisname en/of manipulatie door toepassing van cryptografische technieken.

periodiek proces
Het proces bevat een terugkoppel-mechanisme, zodat het beleid kan worden bijgestuurd en gecorrigeerd. Bekende voorbeelden zijn Plan-Do-Check-Act (PDCA) of Observe-Orient-Do-Act (OODA).

dataclassificatie
Informatie dient te worden geclassificeerd, om de behoefte aan, de prioriteit en de mate van beveiliging aan te geven. Het informatiebeveiligingsbeleid definieert gegevensgroepen (of -klassen). Hiervoor kan het teruggrijpen op de eisen uit wet- en regelgeving en de kenmerken van gegevensopslag en -verwerking binnen de organisatie. Binnen een gegevensklasse gelden naar aard en gewicht dezelfde beschermingsmaatregelen.

detectiemechanismen
Detectiemechanismen detecteren problemen of aanvallen in de communicatie. Voorbeelden zijn intrusion detection systeem en monitoringsystemen.

DMZ
In het kader van webapplicatie wordt met fysieke en logische domeinen de fysieke en logische inrichting van een sub-netwerk (een Demilitarised Zone (DMZ)) bedoeld die uit een verzameling hardware en software componenten bestaat en die fysiek en logisch met elkaar zijn verbonden. Door deze connecties is dit sub-netwerk in staat om specifieke (beveiligings)diensten te bieden.

documentatie
Vastleggen van de daadwerkelijk toegepaste inrichting, configuratie, samenhang en afhankelijkheden van (technische) componenten.

efficiënt en effectief
In het webapplicatiedomein worden vaak verschillende logging-mechanismen (registraties) naast elkaar gebruikt. Om de loggings-informatie niet omslachtig, met beperkte inspanning en doeltreffend te kunnen analyseren is van belang deze te centraliseren.

eisen en wensen
Eisen en wensen bepalen zakelijke behoeften (functionele eisen) en niet-functionele eisen (beveiligingseisen) met betrekking tot toegangsvoorziening. De functionele eisen zijn gerelateerd aan de faciliteiten voor de medewerkers om op een efficiënte en effectieve manier zijn/haar taken te kunnen uitvoeren en de juiste resources (data) te kunnen benaderen. De niet-functionele eisen zijn gerelateerd aan de faciliteiten om beveiliging te kunnen realiseren.

functieprofielen
De taken binnen het beheer zijn bekend en verdeeld in verschillende groepen, de functieprofielen. Deze profielen zijn bedoeld om enerzijds tot een effectief takenpakket te komen, anderzijds tot een adequate functiescheiding (zie ook richtlijn U/TV.01en U/TV.01/02). De functieprofielen komen tot uitdrukking in de autorisaties van beheerders.

functionarissen
Binnen de informatiebeveiligingsorganisatie worden verschillende functionarissen, met specifieke beveiligingsrollen, onderscheiden.

fysieke en logische domeinen
De netwerk componenten kunnen, om onder andere beveiligingsredenen of fault tolerance, fysiek of logisch gegroepeerd worden in bepaalde domeinen. Een fysiek domein geeft aan hoe netwerkcomponenten fysiek met elkaar zijn verbonden, terwijl een logisch domein weergeeft hoe netwerkcomponenten door middel van protocollen zijn verbonden. De logische connecties kunnen over de grenzen van de fysieke domeinen heen gaan.

gegevensleveringen en transacties
De organisatie beschrijft welke gegevensleveringen en transacties onderdeel zijn van de reguliere en ad hoc processen, procedures en verwerkingen. De organisatie kan hierin zowel de leverende als de ontvangende partij zijn.

Bij elk van de leveringen en transacties wordt vastgelegd wat de voorwaarden zijn en welke zekerheden gerealiseerd moeten worden.

In plaats van concrete, individuele leveringen en transacties te benoemen kan de organisatie er ook voor kiezen het transactiebeleid te laten verwijzen naar de classificatie van hetgeen wordt uitgewisseld. Voor gegevensuitwisseling kan de dataclassificatie uit B.01/03 gebruikt worden.

hardeningbeleid
Het informatiebeveiligingsbeleid bevat een onderdeel expliciet gericht op hardening. De meeste computer- en netwerkapparatuur en softwarepakketten bevatten meer functionaliteit dan een organisatie nodig heeft voor het doel waarvoor deze is aangeschaft. Het hardeningbeleid beschrijft hoe de organisatie hiermee wil omgaan.

hardeningrichtlijn
Hardeningrichtlijnen geven voorschriften en/of aanwijzingen voor het veilig configureren van netwerken, platformen en webservers.

hersteld en voortgezet
Maatregelen zoals redundante actieve componenten en back-ups, om beschikbaarheidsincidenten te kunnen oplossen, zodat de dienstverlening gecontinueerd kan worden.

ICT-beveiligingsarchitectuur
Een ICT-beveiligingsarchitectuur bestaat uit een gelaagde architectuur. Deze gelaagde architectuur zorgt ervoor dat op elke laag de juiste maatregelen zijn genomen en noodzakelijke procedures beschikbaar zijn om de doelstellingen van de organisatie te realiseren.

instructies
De beschrijving van een reeks met elkaar verbonden activiteiten voor het configureren van infrastructuurcomponenten en periodiek controleren van deze componenten.

internetbeleid
Het internetbeleid beschrijft hoe een organisatie op internet aanwezig wil zijn, bijvoorbeeld met een website. Hierin spelen inhoud, presentatie en veiligheid een hoofdrol.

isolatie
Mechanismen om een proces af te schermen van zijn omgeving. Dit voortkomt dat het proces andere processen beïnvloedt casu quo door ander processen wordt beïnvloedt. Het voorkomt ook ongewenste toegang tot informatie doordat ook bestanden worden afgeschermd.

levensduur
Er dient een limiet gesteld te worden aan de maximale tijd dat een gebruiker inactief is. In voorkomende gevallen kan het ook gewenst zijn de maximale totale sessieduur te beperken. Hiermee worden de mogelijkheden voor een ongeautoriseerde derde om de sessie ‘over te nemen’ van de geautoriseerde gebruiker beperkt.

manipulatie
Manipulatie kan via de inhoud van de invoer tot stand komen, via het systeem waarop de webapplicatie is geïnstalleerd en via de geprogrammeerde controles. Manipulatie via de inhoud wordt door normaliseren en valideren afgevangen. Manipulatie op het niveau van de programmering en het systeem stelt eisen aan de manier waarop de webapplicatie is opgebouwd.

netwerkpaden
Beslissingen om een gebruiker toe te laten tot een webapplicatie zijn aan de toegangsvoorzieningen, niet aan de netwerkroutering. Het netwerk (de netwerkpaden en de routering) dient er voor te zorgen dat er geen manieren zijn om de toegangsvoorzieningen te omzeilen.

noodzakelijke functionaliteit
Functies die niet nodig zijn voor de functionaliteit van een (web) applicatie vormen een onnodig risico en dienen daarom achterwege te blijven.

normaliseren
Door invoer en uitvoer te normaliseren wordt voorkomen dat het ontvangende systeem gemanipuleerd kan worden via de webapplicatie. Normaliseren van inhoud betekent dat de inhoud gaat voldoen aan een aantal beperkende regels. Hierdoor wordt de mogelijkheid weggenomen om de validaties te omzeilen.

onderlinge samenhang
De samenhang tussen technische componenten en bedrijfsprocessen is gedocumenteerd. Dit geldt zowel voor de horizontale samenhang (gelijksoortige elementen) als verticale samenhang (ondersteunende elementen).

onweerlegbaarheid
Een belangrijke zekerheid ten aanzien van transacties is onweerlegbaarheid dat de transacties hebben plaatsgevonden. Er zijn verschillende redenen waarom een organisatie onweerlegbaarheid kan wensen. Denk hierbij aan financiële transacties of de levering van goederen of informatie.

Ook binnen het kader van een werkende keten, audit-trails en (de mogelijkheid voor) forensisch onderzoek kan onweerlegbaarheid een gewenste eigenschap zijn.

operationele websites
Alle websites die actief bijdragen in de dienstverlening van de organisatie.

opslag en distributie
Naast zorgvuldige processen en procedures voor het omgaan met sleutels, dienen de sleutels ook veilig te worden opgeslagen en gedistribueerd.

organisatorische inrichting
De aspecten ten aanzien van de organisatorische inrichting betreffen alle activiteiten van identiteit- en toegangsbeheer die moeten worden uitgevoerd om gebruikers en autorisaties voor webapplicaties te administreren en de naleving van regels hierover af te dwingen.

Gebruikersidentiteiten en autorisaties op webapplicaties zijn continue aan veranderingen onderhevig. Nieuwe gebruikers moeten worden aangemaakt en autorisaties worden uitgedeeld, bestaande gebruikers en autorisaties worden verwijderd of autorisaties van bestaande gebruikers worden ingeperkt. Vandaar dat deze toegangsvoorzieningsomgeving procesmatig en procedureel ingericht moet zijn.

organisatorische positie
De informatiebeveiligingsorganisatie dient zodanig gepositioneerd te zijn binnen de gehele organisatie, dat zij effectief invulling kan geven aan haar rol.

preventieve en detectieve instrumenten
Preventieve en detectieve instrumenten refereren naar intrusion- en detectie systemen die in de infrastructuur zijn opgenomen met als doel deze operationeel te bewaken. In het kader van governance is het van belang dat de informatie uit deze systemen gerelateerd wordt aan informatie uit andere bronnen. Hierdoor kunnen structurele risico's geïdentificeerd worden die om aandacht van het hoger management vragen.

procedure(el)
Het uitvoeren van handelingen volgens vast omschreven stappen.

procesmatig
Het uitvoeren activiteiten op basis van vooraf vastgestelde stappen of fasen die logisch met elkaar samenhangen om een doel te bereiken.

processen en procedures
Processen en procedures nodig zorgen ervoor dat handelingen volgens vast omschreven stappen en in vaste volgorde worden uitgevoerd, zodat de kwaliteit van uitvoering en daarmee de beveiliging van systemen geborgd kan worden.

protectiemechanismen
Protectiemechanismen zijn maatregelen die tot doel hebben te voorkomen dat bedreigingen tot verstoringen in de communicatie leiden. Voorbeelden zijn tunneling, hardening van componenten, anti-spoofingmechanismen en anti-virus.

protocollen
De webserver ondersteunt het http-protocol. Http kent methoden, headers en foutinformatie, die mogelijk misbruikt kunnen worden. Daarom is het gebruik hiervan beperkt tot het minimum dat noodzakelijk is voor de goede werking van de ontsloten webapplicaties.

queries en commando's
Bij het gebruik van geparameteriseerde queries is de syntax van de query statisch en wordt invoer alleen gebruikt om vooraf gedefinieerde variabelen te vullen. Door te voorkomen dat de syntax van de query wijzigt, voorkomt de webapplicatie SQL-injectieaanvallen.

Geparametriseerde queries zijn ook efficiënter: doordat ze voorgedefinieerd zijn, gebruiken ze bekende tabelstructuren optimaal. Toch geven ze de gebruiker geen volledige vrijheid.

Op dezelfde manier voorkomen statisch geprogrammeerde commando's ervoor dat de gebruiker geen mogelijkheid heeft de aard van de commando's te beïnvloeden.

rapportages
Rapportages uit verschillende beheerdisciplines, zoals vulnerability assessment, penetratie testen en compliance assessment moeten aan elkaar gerelateerd en in samenhang geanalyseerd worden. Op basis van geconstateerde structurele risico's kunnen verbeterplannen worden opgesteld dan wel worden bijgesteld.

rapporteren
Het verschaffen van informatie door middel van een uitgebracht verslag over de geanalyseerde situatie.

redundantie
In de ICT-infrastructuur kunnen additionele systemen worden opgenomen die voor alternatieve paden zorg dagen. Zo kan bij falen van een netwerkcomponent de beschikbaarheid van de dienstverlening gegarandeerd worden.

registratie en detectie
De registratiefunctie houdt verband met het vastleggen van menselijke- en systeemgerichte acties en informatie over gebeurtenissen voor controle en analyse doeleinden. De detectiefunctie houdt verband met het (selectief) waarnemen van signalen voor het opsporen en blootleggen van ongewenste gebeurtenissen in de webapplicatie omgeving.

registratie-instrumenten
Registratie-instrumenten refereren naar logging en monitoring systemen. In de praktijk worden gescheiden logging en monitoring systemen per ICT-diensten laag (beveiligingslaag) geïmplementeerd. Voor analyse doeleinden is het effectiever om de geregistreerde informatie te centraliseren.

richtlijnen
Richtlijnen zijn nadere concretisering van diverse beleidstypen, zoals toegangsvoorzieningsbeleid en internetbeleid. Richtlijnen geven voorschriften en/of aanwijzingen voor de uitvoering van taken die leiden tot de invulling van deze beleidstypen.

risicoanalyse
Risicoanalyse levert inzicht in een situatie rondom een object, zoals een webapplicatie en infrastructuur. Het is van belang dat deze risicoanalyses gestructureerd en consequent worden uitgevoerd om op basis van de resultaten de juiste acties te nemen.

scope
De scope beschrijft de afbakening van de webapplicatie-omgeving. Hierin wordt vastgelegd welke onderdelen van het ICT-landschap deel uit maken van de webapplicatie-omgeving.

sessie zelf beëindigen
Wanneer de gebruiker besluit het werken met de (web)applicatie te beëindigen dient hij dit kenbaar te kunnen maken, zodat de sessie afgesloten kan worden. Hiermee wordt voorkomen dat een ongeautoriseerde derde de sessie kan 'overnemen' van de geautoriseerde gebruiker, nadat de laatste is gestopt met zijn werkzaamheden.

specifieke protocolkenmerken
Protocolkenmerken zijn de zogenaamde features van protocollen waarmee bepaalde functionaliteiten of diensten kunnen worden geboden. Zo kent het http-protocol ook een verzameling features. Slechts een beperkte deelverzameling van deze features levert veilige en betrouwbare communicatie. Onjuist gebruik geeft kwaadwillende derden mogelijkheden de communicatie te verstoren of de ontsloten webapplicaties te misbruiken, bijvoorbeeld door sessies van legitieme gebruikers te 'kapen'. Daarom is het noodzakelijk dat de webserver http alleen op een veilige en correcte manier ondersteunt.

taken, verantwoordelijkheden en bevoegdheden
De rol van de informatiebeveiligingsorganisatie worden vertaald naar taken, verantwoordelijkheden en bevoegdheden van de informatiebeveiligingsorganisatie en haar functionarissen.

technische componenten
Technische componenten representeren infrastructuur en software componenten. Elke technische en of applicatie omgeving ken een verzameling componenten die gezamenlijke een dienst leveren. Zo heeft een webapplicatie omgeving een verzameling technische componenten op basis waarvan webapplicatieve diensten worden geleverd. Het is van belang inzicht te hebben in deze verzameling componenten.

(technische) evaluaties
Het uitvoeren van evaluaties van technische aspecten van webapplicatie,
- zoals codereview tijdens ontwikkelingstrajecten en
- het uitvoeren van periodieke (geautomatiseerde) blackbox scan.

technische inrichting
De technische inrichting betreft de technische vormgeving van de toegangsvoorzieningen van de webapplicatie. Een juiste inrichting kan risico's van (systeem)misbruik aanzienlijk verminderen door rechten op een systeem te beperken. De manier waarop rechten op het systeem beperkt kunnen worden, is afhankelijk van het besturingssysteem en de technische richtlijnen met betrekking tot toegangsbeheer.

Zaken die bij de technische inrichting een rol spelen zijn onder meer:
- inrichting van toegangsvoorziening en beheer (identificatie, authenticatie en autorisatie) Hierbij zijn organisatorische aspecten: rollen en profielen van belang,
- centraal of decentraal van opzet,
- inrichting van gebruikers- en beheerdersaccounts,
- beperkte toegang tot accounts met hoge privileges,
- technische configuratie van onderliggende infrastructurele systemen.

testen
Het testen van doorgevoerde wijzigingen in de test omgeving. Hierbij is het van belang te weten wat er getest gaat worden (het testobject), waarmee er vergeleken gaat worden; (de testbasis), wanneer er getest gaat worden en hoe er getest gaat worden.

tijdig en geautoriseerd
Wijzigingen worden bijtijds ingediend en in behandeling genomen anders bestaat het risico dat noodzakelijke verbeteringen of de instandhouding van de beveiliging van de webapplicatie in het gedrang komt. Wijzigingen worden geautoriseerd anders bestaat het risico dat ongewenste (neven)effecten hebben op de webapplicatie. De initiator van de wijziging overziet niet altijd alle wijzigingen. Het is daarom van belang alle wijzigingen gestructureerd in kaart te brengen en de impact af te stemmen met alle belanghebbenden, zoals de eigenaar en de beheerders van de webapplicatie.

toegangsvoorziening
Het toegangsvoorzieningsbeleid als onderdeel van het informatiebeveiligingsbeleid bepaalt welke medewerkers onder wat voor voorwaarden toegang hebben tot welke gegevens en de activiteiten die hiermee kunnen en mogen worden uitgevoerd. Hierbij kan het beleid voortbouwen op de wet- en regelgeving en de dataclassificatie. Naast zaken als authenticatie en algemene autorisatie van een gebruiker, kunnen hierin ook nadere autorisatie regels opgenomen worden, zoals locatie en tijdstip.

toekennen van de rechten
Alle personen met toegang tot zakelijke toepassingen, informatie systemen, netwerken en computerapparatuur moet worden geautoriseerd, op basis van hun rollen en autorisatieprofielen, voordat toegangsrechten worden toegekend.

uitvoer
Uitvoer refereert aan informatie aan gebruiker en/of informatie over de inrichting van de applicatie zelf. Dit laatste houdt in dat bijvoorbeeld een webapplicatie zo is geconfigureerd dat hiervan informatie over de inrichting kan worden verstrekt. Om misbruik te voorkomen moeten webapplicatie zo zijn geconfigureerd dat de webapplicatie geen informatie geeft over de interne werking of configuratie van de webapplicatie zelf of een van de systemen waarmee de webapplicatie samenwerkt.

valideren
Valideren van de inhoud zorgt ervoor dat alleen geldige gegevens verwerkt worden. Validatie vindt zowel op protocol-niveau (meestal http) als op applicatie-niveau plaats. Het doel is te voorkomen dat de software op het betreffende niveau in misbruikt wordt of faalt door de door de gebruiker aangeleverde gegevens.

vaststellen van de identiteit
Gebruikers doorlopen een aanvraagproces voordat ze worden voorzien van toegang tot zakelijke toepassingen, informatie systemen, netwerken en computerapparatuur. Bij het inloggen zal het identiteit- en toegangsmanagementsysteem de identiteit moeten vaststellen. Hiervoor zullen moeten voldoen aan bepaalde wachtwoord- en toegangsvoorzieningsbeleid (B.02) die tevens door het toegangssysteem wordt afgedwongen.

veilige (communicatie)protocollen
Er kan onderscheid gemaakt worden tussen veilige en onveilige (communicatie)protocollen. Onveilige protocollen kunnen worden afgeluisterd, voorbeelden zijn Telnet en http. Door gebruik te maken van versleuteling (encryptie) via SSL of https wordt afluisteren voorkomen.

vertrouwelijkheid van transacties
Bij een deel van de transacties zal het noodzakelijk zijn de vertrouwelijkheid te waarborgen. Dit heeft betrekking op de communicatie die voor de transacties nodig is, maar ook op de opslag van authenticatiegegevens die nodig zijn om een transactie aan te (willen) gaan.

voorschriften
Regels bedoeld voor het beheersen of reguleren van het gedrag van personen en organisaties.

werkinstructies
Zie instructies.

wet- en regelgeving
Het informatiebeveiligingsbeleid vermeldt de relevante wet- en regelgeving die van toepassing is op de (geautomatiseerde) gegevensopslag en -verwerking binnen de organisatie. Van deze wet- en regelgeving worden de relevante eisen op een rijtje gezet.

Colofon

Publicatie
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 55 55

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

mei 2024