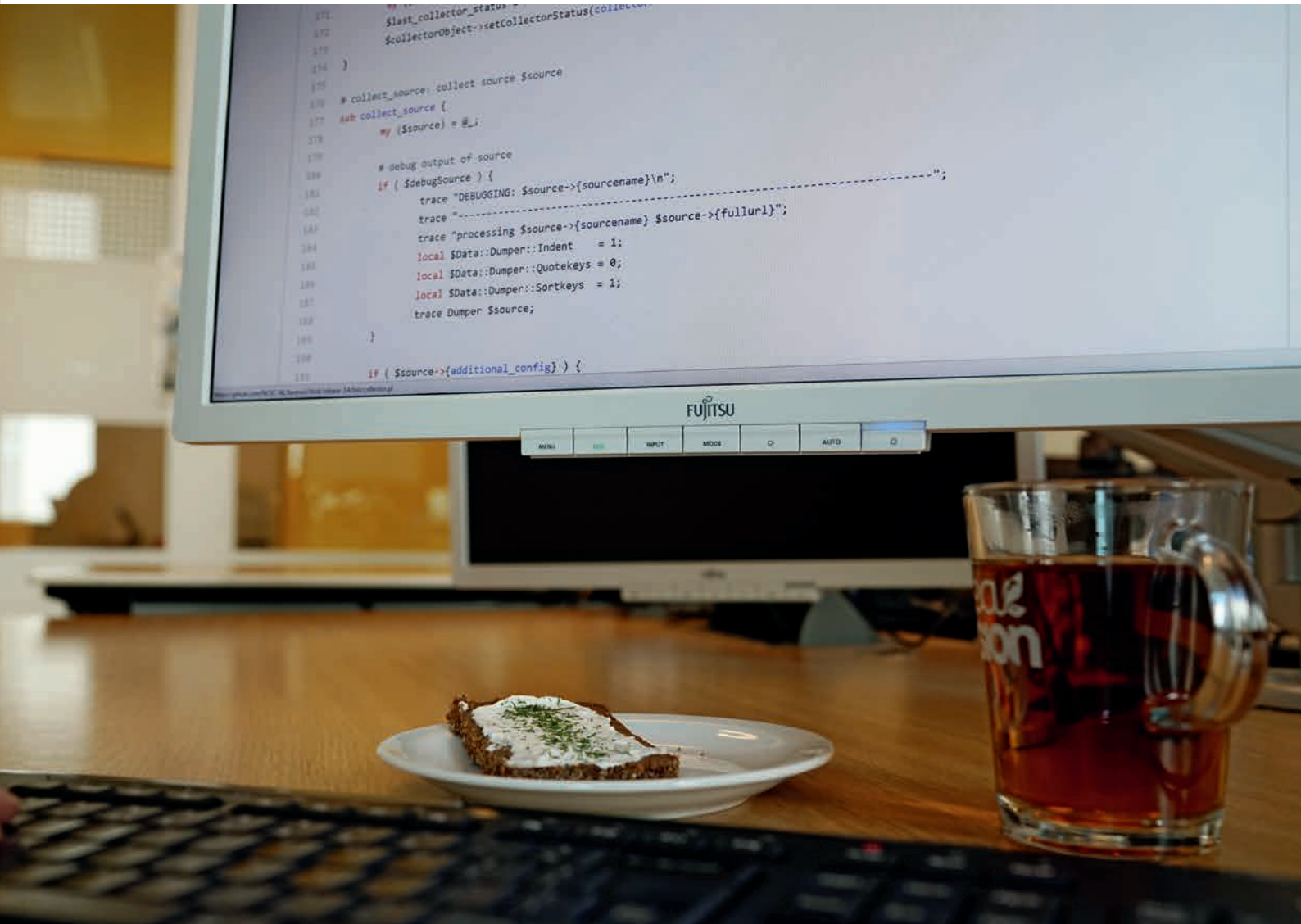
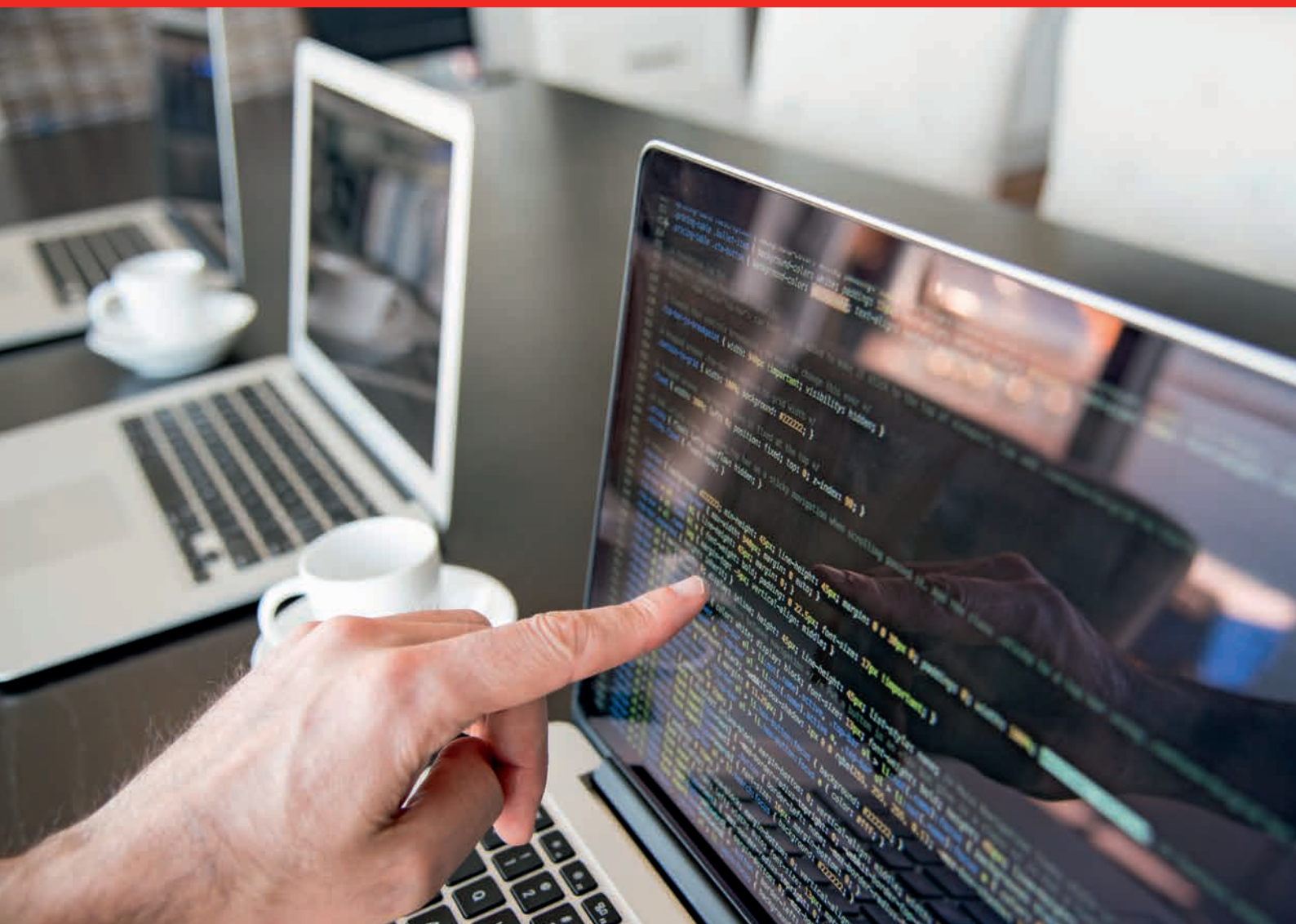
Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Beleids- en beheersings-richtlijnen voor de ontwikkeling van veilige software



Beleids- en beheersings-richtlijnen voor de ontwikkeling van veilige software



Inhoud

Inleiding

Doelgroep

Dit document heeft drie primaire doelgroepen.

- De eerste doelgroep bestaat uit partijen die verantwoordelijk zijn voor het stellen van beveiligingskaders en de controle op naleving hiervan. Hierbij kan worden gedacht aan security-managers en systeemeigenaren (de opdrachtgevers) van de te leveren ICT-diensten.
- De tweede doelgroep bestaat uit diegenen die betrokken zijn bij het ontwerp- en ontwikkelproces, de implementatie en het beheer van applicaties. Deze doelgroep moet de beveiligingsrichtlijnen toepassen.
- De derde doelgroep bestaat uit de controlerende instanties (IT-auditors) die op basis van deze richtlijnen een objectief ICT-beveiligingsassessment uitvoeren.

Reikwijdte en context

Deze richtlijnen zijn niet alomvattend en kunnen naast beveiligingsvoorschriften en baselines met een bredere scope (zoals BIR en BIG) worden gebruikt. Waar dergelijke baselines uit een deelverzameling van de maatregelen uit ISO-standaard 27002 bestaan, kennen deze richtlijnen wel een gedeeltelijke overlap met ISO27002 en baselines, maar zijn ze op bepaalde onderdelen gedetailleerder uitgewerkt.

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

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

Toepassing

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

Prioriteit

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

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

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

Leeswijzer

Dit document is ingedeeld volgens het SIVA-raamwerk. [4] De structuur van de richtlijnen bestaat uit drie domeinen die hieronder kort worden behandeld. Zie bijlage B voor een uitgebreidere toelichting van de SIVA-methode.

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 applicatie uiteengezet.

Beheersingsdomein (control)

Evaluatieaspecten en meetaspecten zijn in dit domein opgenomen. Daarnaast staan hier ook de beheerprocessen beschreven, 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 mobiele apps, 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.

Relatie met andere documenten

De ICT-beveiligingsrichtlijnen voor webapplicaties [1] en de ICT-beveiligingsrichtlijnen voor mobiele apps [3] staan met deze richtlijnen in verbinding. Zij putten uit een gezamenlijk beleids- en beheersingsdomein; de uitvoeringsdomeinen spitsen zicht toe op de verschillende architecturele onderdelen van een applicatieomgeving.

Beleidsdomein

B.01 Informatiebeveiligingsbeleid

Informatiebeveiliging start bij een door het management ondersteund informatiebeveiligingsbeleid, waarover helder wordt gecommuniceerd met medewerkers en, indien relevant, externe partners.

Organisaties die niet voldoen aan ISO 27002 of een daarop gebaseerde baseline, worden geadviseerd de ISO 27002 hanteren om tot een deugdelijk algemeen informatiebeveiligingsbeleid, zowel qua proces als inhoud, te komen. Het informatiebeveiligingsbeleid legt onder meer vast hoe de organisatie ten aanzien van informatiebeveiliging is ingericht en wie welke taken en verantwoordelijkheden heeft.

Voor de beveiliging van software zijn er enkele specifieke aandachtspunten ten aanzien van de inhoud van het informatiebeveiligingsbeleid.

B.01 Informatiebeveiligingsbeleid

Criterium *(wat)*	De organisatie formuleert een **informatiebeveiligingsbeleid** en besteedt hierin specifiek aandacht aan **dataclassificatie**, **toegangsvoorziening** en **kwetsbaarhedenbeheer**.
Doelstelling *(waarom)*	Hiermee wordt ervoor gezorgd dat in het beveiligingsproces specifiek aandacht is voor de softwaretoepassingen van de organisatie.
Risico	Onvoldoende sturing van inspanningen op het gebied van informatiebeveiliging ten aanzien van applicaties, waardoor deze niet of onvoldoende bijdragen aan de doelstellingen van de organisatie.
Classificatie	Hoog

Maatregelen

Informatiebeveiligingsbeleid

01 Het informatiebeveiligingsbeleid voldoet aan de eisen die in ISO-standaard 27002 of een voor de organisatie geldende baseline worden gesteld.

Denk hierbij voor gemeentes aan de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).
Voor de Rijksoverheid gelden het Voorschrift Informatiebeveiliging Rijksdienst (VIR) en de Baseline Informatiebeveiliging Rijksdienst (BIR).

02 Laat het informatiebeveiligingsbeleid vaststellen door verantwoordelijk hoger management (CxO–niveau).

Dataclassificatie

03 Stel een dataclassificatieschema op.

Met behulp van het schema kan bepaald worden welke mate van beveiliging vereist is.

Toegangsvoorziening

04 Formuleer specifiek beleid voor het verlenen van toegang tot functies en gegevens aan personen en systemen.

Kwetsbaarhedenbeheer

05 Formuleer voorschriften om de risico's van kwetsbaarheden te verminderen.

Denk hierbij bijvoorbeeld aan voorschriften voor hardening en voorschriften voor het tijdig doorvoeren van patches en security-updates van softwarecomponenten.

06 Voer een beleid voor coordinated vulnerability disclosure in.

Beveiligingsonderzoekers kunnen zo gevonden kwetsbaarheden in de software op een vertrouwelijke manier melden. Deze kunnen dan worden verholpen voordat anderen er misbruik van kunnen maken.

B.02 Toegangsvoorzieningsbeleid

Het toegangsvoorzieningsbeleid maakt deel uit van het informatiebeveiligingsbeleid en geeft regels en voorschriften voor de organisatorische en technische inrichting van de toegang tot ICT-voorzieningen, bijvoorbeeld applicatie (gebruikers) en ICT-componenten (beheerders). Het toegangsvoorzieningsbeleid beschrijft onder andere de manier waarop de organisatie omgaat met identiteits- en toegangsbeheer.

B.02 Toegangsvoorzieningsbeleid

Criterium *(wat)*	Het toegangsvoorzieningsbeleid formuleert, op basis van **eisen en wensen** van de organisatie, richtlijnen voor de **organisatorische** en **technische inrichting** (ontwerp) van de processen en middelen, waarmee de toegang en het gebruik van ICT-diensten gereguleerd wordt.
Doelstelling *(waarom)*	De effectieve toegang tot informatiesystemen voor bevoegde gebruikers bewerkstelligen en de integriteit, vertrouwelijkheid en controleerbaarheid van de gegevens binnen informatiesystemen garanderen.
Risico	Door het ontbreken van toegangsvoorzieningsbeleid kan er onduidelijkheid ontstaan bij het toekennen van rechten aan gebruikers. Hierdoor kunnen niet-geautoriseerde gebruikers mogelijk toegang krijgen tot informatie waarop zij geen recht horen te hebben.
Classificatie	Hoog

Maatregelen

Eisen en wensen

01 Documenteer zakelijke behoeften en beveiligingseisen voor de toegangsvoorzieningen en stel deze vast.

Eisen en wensen bepalen functionele (zakelijke) en niet-functionele (beveiligings)eisen 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.

Organisatorische inrichting

02 Identificeer gebruikersgroepen, -profielen en/of –rollen.

De organisatie legt gebruikersgroepen, -profielen en/of -rollen vast. Hiermee wordt beschreven welke soorten gebruikers zijn onderscheiden.

03 Leg alleen de hoogst noodzakelijke gegevens van gebruikers vast.

Digitale identiteiten zijn gevoelige persoonsgegevens, waarvan de beveiliging de hoogste aandacht moet hebben. Publiceer het privacybeleid waarin is vastgelegd hoe de organisatie met digitale identiteiten en persoonsgegevens omgaat.

04 Leg de relatie vast tussen gebruikersgroepen, -profielen en/of -rollen en het dataclassificatie-schema.

Hier wordt het dataclassificatieschema van B.01/03 bedoeld.

05 Leg vast welke combinaties van functies, taken en/of rollen ongewenst zijn (functiescheiding).

Het proces van aanvraag, toekenning, schorsing en intrekking kent een zodanige functiescheiding, dat het niet mogelijk is voor één enkele functionaris om volledige controle over alle middelen toe te wijzen aan één gebruiker.
Het beheerproces van de technische middelen voor identificatie, authenticatie en autorisatie kent een zodanige functiescheiding, dat het niet mogelijk is voor één enkele beheerder om volledige controle over alle middelen te verwerven.

06 Stel eisen aan de toegestane authenticators.

Denk hierbij aan regels voor wachtwoorden (lengte, complexiteit, hergebruik), maar ook aan de toepassing van biometrie, crypto-keys, en dergelijke. Ook indien er geen expliciete eisen aan een authenticator worden gesteld, dient dit als zodanig gedocumenteerd te zijn.

Technische inrichting

07 Stel eisen aan de inzet van technische middelen voor identificatie, authenticatie en autorisatie.

08 Stel richtlijnen en procedures op voor de technische inrichting van toegangsvoorzieningen (identificatie, authenticatie en autorisatie) in applicaties.

09 Stel eisen aan:
- de uniformiteit en flexibiliteit van authenticatiemechanismen;
- de rechten voor accounts;
- het automatisch verbreken van de sessie;
- de identificatie- en authenticatie(mechanismen) om voldoende sterke wachtwoorden af te dwingen.

10 Baseer de inrichting van het identiteit- en toegangsbeheer op een vastgesteld ontwerp.

In dit document is vastgelegd welke functies (identiteit-, authenticator-, profiel- en toegangsbeheer) waar (centraal/decentraal) worden uitgevoerd.

B.03 Risicomanagement

De impact van een kwetsbaarheid is zeer afhankelijk van de applicatie en het platform waarop deze draait. De impact wordt ook mede bepaald door de functionaliteit, de aard van de verwerkte gegevens en het gebruik van de applicatie. Het is dan ook belangrijk dat de beveiligingsbehoeften aan de hand van een risicoanalyse worden bepaald. Een risicoanalyse is het systematisch beoordelen van:

- de schade die waarschijnlijk zal ontstaan door een beveiligingsincident als de vertrouwelijkheid, integriteit en beschikbaarheid van de gegevens en andere bedrijfsmiddelen worden geschonden;
- de waarschijnlijkheid dat een beveiligingsincident optreedt rekening houdend met de aanwezige bedreigingen, kwetsbaarheden en de getroffen maatregelen.

De resultaten van deze risicoanalyse worden gebruikt om te bepalen welke prioriteiten moeten worden gesteld ten aanzien van het beheer van beveiligingsrisico's en het implementeren van maatregelen ter bescherming tegen deze risico's. Deze resultaten worden vastgelegd in een informatiebeveiligingsplan. Dit informatiebeveiligingsplan maakt de noodzakelijke stappen voor het implementeren van maatregelen concreet en beschrijft wie wanneer en waarvoor verantwoordelijk is. Hierin wordt ook beschreven dat de maatregelen regelmatig, door middel van onderzoek, worden gecontroleerd op werking en naleving van de richtlijnen. Het is belangrijk om de beveiligingsrisico's en geïmplementeerde maatregelen periodiek te evalueren, om:

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

B.03 Risicomanagement

Criterium *(wat)*	Voor de omgeving van de applicatie wordt risicomanagement uitgevoerd waarbij applicaties zowel tijdens ontwikkeling als tijdens operationeel gebruik periodiek worden onderworpen aan een (informatie) **risicoanalyse**.
Doelstelling *(waarom)*	Bepalen of de risico's (nog) binnen de voor de organisatie acceptabele grenzen liggen en verantwoordelijken informatie verschaffen voor het treffen van eventuele (aanvullende) maatregelen.
Risico	Tekortkomingen in de applicaties en hun ondersteunende infrastructuur worden niet of niet tijdig gesignaleerd. Hierdoor kan de uitvoering van de bedrijfsprocessen die door de applicatie worden ondersteund, worden verstoord.
Classificatie	Hoog

Maatregelen

Risicoanalyse

01 Maak gebruik van een breed toegepaste risicoanalyse-methode.
Voorbeelden van bestaande risicoanalyse-methodes:
ISF:
- *Information Risk Analysis Methodology (IRAM)*

National Institute of Standards and Technology (NIST):
- *SP 800-30 Rev. 1 – Guide for Conducting Risk Assessments*

ISO:
- *NEN-ISO/IEC 27005:2011 'Information security risk management'*

Software Engineering Institute (SEI):
- *Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)*

Microsoft:
- *The Security Risk Management Guide*

BIG-OP:
- *Baselinetoets v1.0*
- *Diepgaande Risicoanalysemethode Gemeenten v1.0*

02 Voer voor (nieuwe) applicaties een risicoanalyse uit en herhaal deze risicoanalyses periodiek.
Dit kan ook door voor clusters van applicaties een generieke risicoanalyse uit te voeren en bij geconstateerde kwetsbare functionaliteiten of hogere risico's voor een specifieke applicatie een diepgaande analyse uit te voeren.

03 Houd van elke uitgevoerde risicoanalyse de rapportage beschikbaar en stel er een informatiebeveiligingsplan bij op.
Registreer van elke applicatie waarop een risicoanalyse wordt uitgevoerd wanneer dit gebeurd is en wanneer deze hernieuwd moet worden.

04 Volg aantoonbaar de aanbevelingen en verbetervoorstellen uit de risicoanalyses op.
Bij elk rapport is een besluitenlijst, in alle aanbevelingen/verbetervoorstellen uit het rapport van een besluit worden voorzien.
Bij elk besluit tot actie is een registratie van de afwikkeling. Hiervoor kan ook een issue-trackersysteem gebruikt worden, met verwijzing naar de risicoanalyse.

B.04 Cryptografiebeleid

Het cryptografiebeleid beschrijft de manier waarop de organisatie omgaat met cryptografisch materiaal en procedures. Cryptografie ligt aan de basis van een reeks belangrijke maatregelen voor informatiebeveiliging. Een solide cryptografiebeleid is daarom een randvoorwaarde om aan deze maatregelen het gewenste vertrouwen te ontlenen.

B.04 Cryptografiebeleid	
Criterium *(wat)*	Het cryptografiebeleid formuleert eisen die worden gesteld aan **processen en procedures** rond het beheer van cryptografisch materiaal en de **opslag en distributie** van dit materiaal.
Doelstelling *(waarom)*	Beschermen van cryptografische sleutels op een manier die past bij de aard van de cryptografisch beschermde gegevens (dataclassificatie B.01/03).
Risico	Het beheer van de cryptografische sleutels sluit niet aan bij het beschermingsbelang van de beschermde gegevens, waardoor het beheer van de cryptografische sleutels niet doelmatig is.
Classificatie	Hoog

Maatregelen

Processen en procedures

01 Stel eisen aan processen en procedures voor aanvraag, creatie, hernieuwing, intrekken en beheer van sleutelmateriaal en certificaten.

Zie NIST SP 800-57 (deel 2) en NIST SP 800-133 voor standaarden voor cryptografische processen en procedures.
Certificaten hebben een maximale geldigheid. Borg dat certificaten tijdig worden vernieuwd. Door het certificaat tijdig te vernieuwen blijft de organisatie in staat aan te sluiten bij het vertrouwelijkheidsniveau binnen het public key infrastructure (PKI)-stelsel.

02 Stel eisen aan procedures voor beheer om te zorgen voor een 'soepele' migratie wanneer een patch een certificaat van de lijst met vertrouwde certificaten verwijdert.

Dit geldt ook als leveranciers een deel van de eerder door hen uitgegeven certificaten intrekken.
De maatregelen dienen (langdurige) verstoring van de dienstverlening te voorkomen. Dit kan betekenen dat deze patches worden uitgesteld als nog niet alle certificaten van de systemen vervangen zijn.

Opslag en distributie

03 Stel eisen aan opslag van sleutelmateriaal.

Besteed expliciet ook aandacht aan back-ups met sleutelmateriaal erin.
Zie NIST SP 800-57 (deel 1 en 3) voor standaards voor het werken met cryptografische technieken en sleutels.

04 Stel eisen aan distributie van sleutelmateriaal.

Het distribueren van sleutelmateriaal zal minstens zo goed beveiligd moeten zijn als de bescherming die de sleutels moeten leveren.

B.05 Contractmanagement

Wanneer de ontwikkeling of het beheer over de dienstverlening met betrekking tot applicaties wordt uitbesteed, moeten de beveiligingseisen in een overeenkomst (bijvoorbeeld een contract of Service Level Agreement (SLA)) tussen beide partijen worden vastgelegd. Deze overeenkomst moet garanderen dat er geen misverstanden bestaan tussen beide partijen.

B.05 Contractmanagement	
Criterium *(wat)*	In een contract met een derde partij voor de uitbestede levering of beheer van een applicatie (als dienst) zijn de **beveiligingseisen en -wensen** vastgelegd en op het juiste organisatorische niveau vastgesteld.
Doelstelling *(waarom)*	Het handhaven van het beveiligingsniveau, wanneer de verantwoordelijkheid voor de ontwikkeling en/of het beheer van de applicatie is uitbesteed aan een andere organisatie.
Risico	Een dienst waarvan de eigenschappen onduidelijk of onberekenbaar zijn, waardoor het gewenste beveiligingsniveau niet gehaald wordt of gebruikers onvoldoende vertrouwen in de dienstverlening hebben.
Classificatie	Hoog

Maatregelen

Beveiligingseisen en –wensen

01 Laat het (beveiligings)beleid onderdeel zijn van het pakket beveiligingseisen en -wensen dat is opgesteld bij de verwerving van diensten en middelen.

Documenteer van de eisen die voortkomen uit het beveiligingsbeleid of deze door de leverancier ingevuld zijn in de offerte, in het contract en in de uitvoering of levering.

02 Laat de eisen en specificaties voor de dienstverlening onderdeel zijn van het eisenpakket dat is opgesteld bij de verwerving van diensten en middelen.

Let er op dat hierbij niet alleen de primaire functionele aspecten als eis worden opgenomen, maar ook beheeraspecten, (management)rapportages en dergelijke.
Deze eisen kunnen ontstaan als uitkomst van onderhandelingen, maar dienen zeker onderdeel van het contract te zijn.

Verdieping

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

Beschrijving van de dienst
Verwijzing per geleverde dienst naar de betreffende service-level-specificaties. Denk hierbij aan concrete beschrijving van diensten, servicetijden (normale servicetijden, weekenden, feestdagen en vakantiedagen), servicebeschikbaarheid, responsetijden, oplostijden etc.

Overlegstructuren, contactpersonen en correspondentie
Vastleggen wanneer gestructureerd overleg plaatsvindt, wie aan dit overleg deelnemen. Ook zal een overzicht opgenomen moeten worden van alle contactpersonen en verantwoordelijken bij escalatie of calamiteiten (escalatiematrix).

Geschillen
Beschrijving wat de procedure is bij het optreden van onderlinge conflicten of geschillen tussen gebruikersorganisatie en dienstverlener.

Prestatie-indicatoren, meten en rapportages
Beschrijving van de prestatie-indicatoren (key performance indicators), hoe deze worden gemeten en hoe hierover wordt gerapporteerd.

Rapportages
Om zicht te hebben, te krijgen en te houden op alles wat te maken heeft met de dienstverlening. Denk hierbij aan afspraken over de inhoud, de frequentie en de verspreiding (distributie) van de rapportage.

Beveiliging
Denk hierbij aan afspraken over procedures voor de beveiliging van systemen, services en data, maatregelen bij het schenden van beveiligingsprocedures en hoe met beveiligingsincidenten wordt omgegaan.

De noodzakelijke beveiligingseisen, zodat aan de beveiligingseisen en -wensen wordt voldaan

- *afspraken over het uitvoeren van audits bij de externe partij;*
- *afspraken over de toegang tot de ICT-omgeving door derden;*
- *afspraken over externe certificering van de (extern) ontwikkelde software. Denk hierbij aan standaardsoftware, software-as-a-service (SaaS) of de ontwikkeling van (maatwerk) software is uitbesteed;*
- *afspraken om de (extern) ontwikkelde software te mogen auditen, bijvoorbeeld het uitvoeren van codereviews;*
- *afspraken over het uitvoeren van andere tests, bijvoorbeeld penetratietest (zie maatregel C.04) om mogelijke kwetsbaarheden op te sporen.*

B.06 ICT-landschap

In het ICT-landschap legt de organisatie vast welke ICT-componenten er zijn en hoe deze aan elkaar gerelateerd zijn. Het verschaft inzicht en overzicht over de ICT-componenten en hun onderlinge samenhang. Bovendien wordt uit het ICT-landschap duidelijk hoe de componenten de bedrijfsprocessen van de organisatie ondersteunen. Dit is een belangrijk hulpmiddel bij het uitvoeren van de risicoanalyse.

Belangrijke onderdelen van het ICT-landschap zijn:
- beveiligingsintegratie-aspecten;
- documentatie.

B.06 ICT-landschap

Richtlijn (wie en wat)	De organisatie heeft de actuele documentatie van het ICT-landschap vastgelegd, met daarin de **bedrijfsprocessen**, de **technische componenten**, hun **onderlinge samenhang** en de **ICT-beveiligingsarchitectuur**.
Doelstelling (waarom)	Het geven van inzicht geven in de relatie tussen techniek en bedrijfsprocessen en de manier waarop en mate waarin deze op elkaar aansluiten. Hiernaast geeft het ICT-landschap inzicht in de interactie en relaties tussen applicaties en andere componenten in de ICT-infrastructuur.
Risico	Dagelijkse operatie is niet in lijn met het geformuleerde beleid en de impact van toekomstige innovaties kan niet in volle omvang en geïntegreerd in beeld worden gebracht.
Classificatie	Midden

Maatregelen

Bedrijfsprocessen

01 Inventariseer en karakteriseer de bedrijfsprocessen, functies, rollen, et cetera die bij het aanbieden, gebruiken en onderhouden van een applicatie betrokken zijn.

Het gaat hier om zowel primaire processen, functies, rollen et cetera als secundaire. Dus ook technisch beheer van de infrastructuur, identiteitenbeheer.

Technische componenten

02 Benoem en beschrijf de technische componenten (waaronder infrastructuur en software) die bij het aanbieden, gebruiken en onderhouden van een applicatie betrokken zijn.

Dit is inclusief de technische componenten die voor de beveiliging gebruikt worden.

03 Benoem en beschrijf de koppelingen met externe netwerken die bij het aanbieden, gebruiken en onderhouden van een applicatie betrokken zijn.

Naast de functionele eigenschappen dient ook de beveiliging van de externe koppelingen opgenomen te worden.

04 Benoem en beschrijf de beveiligingsmaatregelen die hun weerslag hebben (in componenten) in het ICT-landschap.

Deze beschrijving bevat alle (configuratie)elementen die bepalend zijn voor het correct functioneren van de getroffen beveiligingsmaatregel.

Onderlinge samenhang

05 Benoem en beschrijf de onderlinge samenhang tussen technische componenten (waaronder infrastructuur en software) die bij het aanbieden, gebruiken en onderhouden van een applicatie betrokken zijn.

Hieronder valt nadrukkelijk ook de relatie tussen de diverse technische componenten en de aanwezige beveiligingsservices, waaronder:
- *de toegangsvoorzieningen (zie U/TV.01);*
- *de (applicatie-)firewall, loadbalancers, et cetera ;*
- *back-up- en restorefaciliteiten.*

Merk op dat technische componenten elkaar onderling ook beveiligingsservices kunnen en zullen leveren. Gezamenlijk vormen zij een (geïntegreerde) dienst. In het geval van virtualisatie verdienen de regels die op de hypervisor zijn ingesteld extra aandacht. Deze zijn belangrijk om de scheiding van virtuele omgevingen te waarborgen.

06 Benoem en beschrijf de functionele relaties tussen de applicaties die bij het aanbieden, gebruiken en onderhouden van een applicatie betrokken zijn.

Bij de beschrijving van de functionele relaties hoort ook onder welke voorwaarden welke gegevens worden uitgewisseld.

07 Benoem en beschrijf de onderlinge samenhang tussen bedrijfsprocessen die bij het aanbieden, gebruiken en onderhouden van een applicatie betrokken zijn.

08 Benoem en beschrijf de samenhang tussen bedrijfsprocessen en technische componenten die bij het aanbieden, gebruiken en onderhouden van een applicatie betrokken zijn.

ICT-beveiligingsarchitectuur

09 Geef met behulp van de ICT-beveiligingsarchitectuur inzicht in de relatie tussen de toegangsvoorzieningen en het gehele ICT-landschap (inclusief beveiligingsservices).

De inrichting van het identiteit- en toegangsbeheer is gebaseerd op een vastgesteld inrichtingsdocument/ontwerp waarin is vastgelegd welke functies (identiteit-, authenticator-, profiel- en toegangsbeheer) waar (centraal/decentraal) worden uitgevoerd.

Het architectuurdocument geeft aan op welke wijze de toegangsvoorzieningen onderdeel uit maken van de beveiligingsarchitectuur.

Verdieping

Beveiligingsintegratie
Beveiligingsintegratie houdt in dat een applicatie de beschikking krijgt over informatie die aanwezig is binnen de beveiligingscomponenten. Hierdoor kan een beveiligingsoplossing binnen een applicatie worden hergebruikt en hoeven ontwikkelaars de betreffende functionaliteit niet in elke applicatie afzonderlijk in te bouwen.

Hieronder een overzicht van de verschillende manieren waarop een beveiligingscomponent informatie beschikbaar kan stellen aan de achterliggende systemen:

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

Met de invoer van elk nieuw beveiligingscomponent dient men zich af te vragen: hoe wordt deze component binnen de omgeving geïntegreerd?

Belangrijk is vast te stellen:
- welke services de omgeving van de beveiligingscomponent zal afnemen;
- op welke manier de omgeving deze services zal afnemen (actief of passief, welke protocollen).

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

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

Voor elke maatregel wordt documentatie onderhouden. Daarnaast wordt afhankelijk van de gevoeligheid van de applicatie regelmatig het bestaan van maatregelen gecontroleerd en gedocumenteerd. De mate van compliance wordt aan de verantwoordelijke voor de applicatie en de beveiligingsfunctionaris gerapporteerd.

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. Er moeten procedures en verantwoordelijkheden worden vastgesteld en bijgehouden voor het opstellen en aanpassen van documentatie. Documentatie kan gevoelige informatie bevatten en er moeten dan ook maatregelen zijn getroffen om de documentatie te beveiligen tegen ongeautoriseerde toegang (inzien en wijzigen).

De set aan documentatie beschrijft onder andere:
- Hoe wordt omgegaan met risicomanagement, de benodigde bedrijfsmiddelen, de geïmplementeerde maatregelen en noodzakelijke mate van zekerheid; kortom de vastgelegde en vastgestelde procedures en processen.
- De plaatsing van servers en aansluiting van interne netwerkcomponenten en netwerkkoppelingen met externe netwerken zijn duidelijk en schematisch gedocumenteerd, zodat de werking van de ICT-infrastructuur begrijpelijk is en de impact van wijzigingen goed kunnen worden bepaald.
- De beveiligingsinstellingen van de ICT-componenten zijn zodanig gedocumenteerd dat duidelijk is waarom voor bepaalde instellingen gekozen is (verantwoording en onderbouwing). Hierbij wordt speciale aandacht besteed aan de standaardwaarden voor systeeminstellingen.

Beheersingsdomein (control)

C.01 Servicemanagementbeleid

Het servicemanagementbeleid geeft richting aan de wijze waarop de beheersingsorganisatie moet zijn ingericht en de wijze waarop deze moet functioneren. Hiernaast bestaan procedures en instructies voor de ondersteuning van de specifieke beheerprocessen. De beheerorganisatiestructuur geeft de samenhang van de ingerichte processen weer.

C.01 Servicemanagementbeleid

Criterium *(wie en wat)*	Het servicemanagementbeleid formuleert **richtlijnen voor beheerprocessen**, **controleactiviteiten en rapportages** ten behoeve van het beheer van ICT-diensten.
Doelstelling *(waarom)*	Effectieve beheersing, door samenhangende inrichting van processen en controle hierover door middel van registratie, statusmeting, monitoring, analyse, rapportage en evaluatie.
Risico	Onvoldoende mogelijkheden om vast te stellen of de getroffen maatregelen in voldoende mate invulling geven aan beleidsdoelstellingen en onvoldoende mogelijkheden om de beheerorganisatie op de juiste wijze in te richten en bij te sturen.
Classificatie	Midden

Maatregelen

Richtlijnen voor beheerprocessen

01 Stel richtlijnen op voor de inrichting van de servicemanagementorganisatie.

02 Stel een beschrijving op van de relevante beheerprocessen.

03 Richt de processen in conform een vastgestelde cyclus.
Bijvoorbeeld: registratie, statusmeting, monitoring, analyse, rapportage en evaluatie.

04 Gebruik geautomatiseerde middelen voor effectieve ondersteuning van beheerprocessen.

Richtlijnen voor controleactiviteiten en rapportages

05 Stel richtlijnen op voor het uitvoeren van registratie, statusmeting, monitoring, analyse, rapportage en evaluatie.

06 Stel richtlijnen op voor het uitvoeren van controle-activiteiten.
Hieronder vallen ook penetratietests.

07 Stel richtlijnen op voor het evalueren van de organisatie, kwaliteit, effectiviteit, borging en informatievoorziening van de beheerprocessen.

08 Leg de taken, verantwoordelijkheden en bevoegdheden (tvb's) van beheerders vast.

09 Leg de relaties met ketenpartijen vast.

C.02 Compliancemanagement

Compliancemanagement richt zich op het naleven van de verplichtingen die voortkomen uit wet- en regelgeving, en door de organisatie zelf gekozen standaarden en richtlijnen.

Vanuit beveiligingsoptiek is het van belang dat via policycompliancechecks wordt gecontroleerd of de ICT-omgeving na verloop van tijd nog steeds voldoet aan het vastgestelde en geïmplementeerde beveiligingsbeleid, die voortvloeien uit deze verplichtingen (naleving).

De resultaten van de policycompliancechecks worden vastgelegd in de vorm van een rapportage. Wanneer duidelijk wordt dat geïmplementeerde maatregelen niet voldoen aan de gestelde eisen en/of verwachtingen, is opvolging met corrigerende acties noodzakelijk. De literatuur kent dit samenstel als een PDCA-cyclus.

De frequentie voor het uitvoeren van policycompliancechecks dient voort te komen uit het risicoprofiel. Er zijn meerdere momenten waarop een policycompliancecheck zinvol is. Enerzijds als onderdeel van een regulier, periodiek controleproces, anderzijds gekoppeld aan ontwikkelen in verdedigings- en aanvalstechnieken (dreigingen), veranderingen in beleid en techniek en optreden van incidenten.

Periodieke controles (maandelijks, per kwartaal, halfjaarlijks of jaarlijks) dienen om bestaande systemen te testen op naleving van de security policy en/of als onderdeel van de PDCA-cyclus.

In de loop van de tijd veranderen technieken en inzichten. Ook zal het ICT-landschap gaandeweg veranderen. Deze ontwikkelingen kunnen aanleiding zijn het beleid bij te stellen en de controles aan te passen. Elke (groep van) verandering(en) is aanleiding om een policycompliancecheck uit te voeren.

Tot slot zullen er (vermoedens van) incidenten zijn, die aanleiding geven tot het uitvoeren van ad hoc policycompliancechecks.

C.02 Compliancemanagement

Criterium *(wie en wat)*	De inrichting en de beveiliging van de applicaties (**scope**) wordt **procesmatig en procedureel** gecontroleerd (compliancechecks) op basis van vastgestelde beveiligingsrichtlijnen en een vastgestelde applicatie-architectuur.
Doelstelling *(waarom)*	Vaststellen in hoeverre de implementatie van de applicatie voldoet aan de vooraf vastgestelde beveiligingsrichtlijnen en geldende wet- en regelgeving.
Risico	Aansprakelijkheid in geval van beveiligingsincidenten en niet halen van bedrijfs- en beveiligingsdoelstellingen.
Classificatie	Midden

Maatregelen

Scope

01 Zorg voor een beschrijving van de applicatie-omgeving, waarin de configuratie-elementen genoemd worden.

De scope beperkt zich tot dat deel van de totale keten, dat onder de formele verantwoordelijkheid van de organisatie valt.
Indien er sprake is van uitbesteding, valt ook het uitbestede deel van de keten onder de formele verantwoordelijkheid van de uitbestedende organisatie. Met de dienstverlener dienen sluitende procedurele en technische afspraken gemaakt te worden om de vereiste waarborgen tot stand te brengen. In die zin mag er geen verschil zijn met de situatie waarbij alles in eigen huis gerealiseerd is. De scope dient aantoonbaar gebaseerd te zijn op het actuele ICT-landschap.

Procesmatig en procedureel

02 Stel een planning op voor de reguliere policycompliancechecks ten aanzien van de applicatie-omgeving.

De planning toont de activiteiten die zullen worden uitgevoerd (wie, wat en wanneer).
Policycompliancechecks betreffen zowel de procedurele als de technische compliance.

03 Registreer de uitvoering van en rapporteer over de resultaten van de periodieke policycompliancechecks.

De registratie bevat in ieder geval:
- *het controlemoment;*
- *de aanleiding voor de controle;*
- *wie de controle heeft uitgevoerd;*
- *de omgeving waarop de controle is uitgevoerd;*
- *de middelen waarmee de controle is uitgevoerd.*

Indien voor het laatste gebruikgemaakt is van programmatuur: naam, versie en parameters.

04 Communiceer de rapportages met verbetervoorstellen met verantwoordelijken over de afwijkingen.

Afwijkingen worden toegelicht, waarbij de ernst van de afwijking wordt uitgedrukt in een risico voor de organisatie en haar partners.
Verbetervoorstellen worden geprioriteerd op basis van dit risico.

05 Beleg implementatieacties en stel uitvoerings- of systeemdocumenten beschikbaar waaruit blijkt dat de verbetervoorstellen zijn geïmplementeerd.

Het gaat om de daadwerkelijke uitvoering. Dit vereist een registratie van verbeteringen die al zijn uitgevoerd en een planning (wie, wat en wanneer) van nog uit te voeren verbeteringen.

C.03 Vulnerability-assessments

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

Vragen die hierbij een rol spelen:
- Hoe is de ICT-omgeving opgebouwd en geconfigureerd?
- Wat zijn bekende kwetsbaarheden en zwakheden?

Vulnerability-assessments zijn noodzakelijk om zwakheden van in ICT-componenten op verschillende lagen van de ICT-infrastructuur vast te stellen.

Bij een vulnerability-assessment (VA) wordt met behulp van een scanner een (geautomatiseerde) scan uitgevoerd op een van te voren bepaald aantal ip-adressen. Hierbij worden de servers en services onderzocht op alle bekende kwetsbaarheden en zwakheden en worden de gevonden kwetsbaarheden en zwakheden gerangschikt naar risico (hoog, midden en laag). De te analyseren ip-adressen worden door de beheerder opgegeven of automatisch bepaald door een netwerkscan. Door een VA uit te voeren over de ICT-componenten (zowel op ICT-systemen als op netwerken), komen aanwezige kwetsbaarheden en zwakheden naar boven en worden deze weergegeven in een rapportage.

Netwerkgebaseerde VA's worden uitgevoerd door netwerkscanners. Netwerkscanners zijn in staat om open poorten te detecteren, services te identificeren die op deze poorten draaien, mogelijke kwetsbaarheden van deze services te detecteren en aanvallen op deze services te simuleren.

Hostgebaseerde VA's worden uitgevoerd door hostscanners. Hostscanners zijn in staat om kwetsbaarheden op systeemniveau te herkennen, waaronder onjuist toegekende rechten en configuratiefouten. In tegenstelling tot de netwerkscanners, is voor hostscanners een account op de betreffende host (computersysteem) nodig met voldoende toegangsrechten.

Op basis van de rapportage kan de organisatie een afweging maken welke kwetsbaarheden relevant zijn en verholpen moeten worden en welke geaccepteerd worden. Het kan voorkomen dat bepaalde kwetsbaarheden niet verholpen kunnen worden omdat dan de applicatie niet meer functioneert.

De frequentie voor het uitvoeren van vulnerability-assessments dient vastgesteld te worden op basis van het risicoprofiel. Er moet actie worden ondernomen indien geïmplementeerde maatregelen niet voldoen aan de gestelde eisen en/of verwachtingen of tekortkomingen opleveren.

C.03 Vulnerability-assessments

Richtlijn *(wie en wat)*	Vulnerability assessments (security scans) worden **procesmatig en procedureel** uitgevoerd op de ICT-componenten van de applicatie (**scope**).
Doelstelling *(waarom)*	Identificeren van de kwetsbaarheden en zwakheden in de ICT-componenten van de applicatie zodat tijdig de juiste beschermende maatregelen kunnen worden getroffen.
Risico	Onvoldoende zicht op aanwezige kwetsbaarheden en zwakheden van ICT-componenten, onvoldoende zicht op de effectiviteit van reeds getroffen maatregelen en onvoldoende mogelijkheden om te kunnen anticiperen op de nieuwe dreigingen.
Classificatie	Hoog

Maatregelen

Procesmatig en procedureel

01 Stel een planning op voor het uitvoeren van reguliere vulnerability-assessments van de applicatie-omgeving.
Vermeld hierin welke soort VA op welk moment (periode) uitgevoerd moet worden.

02 Registreer de uitvoering van de vulnerability-assessments.
De registratie bevat in ieder geval (a) het VA-moment, (b) wie de VA heeft uitgevoerd, (c) de omgeving waarop de VA is uitgevoerd en (d) de middelen (naam, versie en parameters) waarmee de VA is uitgevoerd.

03 Stel rapportages op met de resultaten van de vulnerability-assessments.
Maak gebruik van richtlijnen of een format voor de VA-rapportage. In een dergelijk rapportage-format is duidelijk vastgelegd welke informatie de rapportage moet bevatten.

04 Communiceer de rapportages met verbetervoorstellen met verantwoordelijken of eigenaren van systemen waarin kwetsbaarheden en zwakheden gevonden zijn.
Afwijkingen worden toegelicht, waarbij de ernst van de afwijking wordt uitgedrukt in een risico voor de organisatie en haar partners. Verbetervoorstellen worden geprioriteerd op basis van dit risico en er wordt een actielijst samengesteld.

05 Beleg implementatieacties en stel uitvoerings- of systeemdocumenten beschikbaar waaruit blijkt dat de verbetervoorstellen zijn geïmplementeerd.

Het gaat om de daadwerkelijke uitvoering. Dit vereist een registratie van verbeteringen die al zijn uitgevoerd en een planning (wie, wat en wanneer) van nog uit te voeren verbeteringen.
Er is aantoonbaar opvolging gegeven; verbeteringen zijn doorgevoerd indien geïmplementeerde maatregelen niet voldoen aan de gestelde eisen en verwachtingen.

Scope

06 Zorg voor een actueel overzicht van te onderzoeken componenten, zoals applicaties, webservers, netwerk(componenten) en ip-adressen.

Geef aan welke componenten in deze scope een rol spelen en hoe deze met elkaar samenhangen. Bijvoorbeeld: applicaties, webservers, netwerk-(component) en ip-adressen.

07 Stel een overzicht op van kwaliteitseisen en -criteria waarover gerapporteerd moet worden.

De kwaliteitseisen en -criteria moeten gekoppeld zijn aan de componenten binnen de scope van de VA. Het wel of niet voldoen aan deze kwaliteitseisen en -criteria moet binnen de invloedsfeer van de organisatie liggen.

C.04 Penetratietestproces

Het penetratietestproces richt zich op het geven van inzicht in de mate waarin de applicatie kwetsbaar is voor inbraken.

Het penetratietestproces is een impliciet onderdeel van het wijzigingenbeheer (richtlijn C.08), maar wordt in verband met het belang afzonderlijk geadresseerd. Vanuit beveiligingsoptiek is het van belang dat wordt gecontroleerd of het mogelijk is de applicatie op enigerlei wijze binnen te dringen. Een penetratietest (ook pentest genoemd) is daarom een waardevolle aanvulling op de beveiliging van applicaties. Het uitvoeren van een penetratietest kan echter een uitdaging zijn. De aan de test verbonden risico's moeten minimaal zijn, de kwaliteit van de test optimaal en resultaten moeten bruikbaar zijn om kwetsbaarheden effectief te verhelpen.

Penetratietests kennen verschillende varianten zoals black box tests, grey box, white box of crystal box. Het verschil zit onder meer in de hoeveelheid kennis en achtergrondinformatie die de tester krijgt. Als een tester minimale voorkennis heeft, is er sprake black box; krijgt een tester van tevoren inzicht in alle aspecten van de systeemarchitectuur, dan wordt het een white box genoemd. Een grey box zit tussen een white box en black box in. Met crystal box wordt meestal bedoeld dat de tester ook de broncode van de applicatie heeft en beschikt over alle mogelijke configuratie-informatie.

Ook het testperspectief leidt tot varianten. Wordt er getest vanuit het perspectief van een interne medewerker, dan gaat het om een 'privileged test'. Het perspectief van een aanvaller vanaf internet heet een 'non-privileged test'.

Er kunnen meerdere momenten zijn waarop een penetratietest zinvol is:
- in de acceptatiefase van een nieuwe applicatie;
- bij significante wijzigingen in een applicatie;
- periodiek (jaarlijks/tweejaarlijks), om bestaande applicaties te testen op nieuwe inbraaktechnieken en/of als onderdeel van de PDCA-cyclus;
- als er een andere reden is om te denken dat de beveiliging van een applicatie minder goed is dan gedacht.

De frequentie dient vastgesteld te worden op basis van het risicoprofiel.

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

De kwaliteit van de penetratietest wordt mede bepaald door de methodiek. Denk hierbij aan:
- een stappenplan waarin de activiteiten in volgorde worden beschreven en op welke methodiek de aanpak is gebaseerd;
- een testplan waarbij per test staat vermeld wat de risico's zijn.

C.04 Penetratietestproces

Criterium *(wie en wat)*	Penetratietests worden **procesmatig en procedureel**, ondersteund door richtlijnen, uitgevoerd op de applicatie **(scope)**.
Doelstelling *(waarom)*	Het verkrijgen van inzicht in de weerstand die een applicatie kan bieden aan pogingen om het te compromitteren (binnendringen of misbruiken van applicatie).
Risico	Onbekendheid met bestaande kwetsbaarheden en zwakheden, waardoor hiertegen geen actie ondernomen wordt.
Classificatie	Hoog

Maatregelen

Procesmatig en procedureel

01 Plan het uitvoeren van reguliere penetratietests van de applicatie.

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

- *Zijn er momenten waarop er niet getest mag worden?*
- *Vermijd kritieke periodes, zoals een pentest van een verkoopkanaal ten tijde van verwachte drukte.*
- *Doe geen pentest als een applicatie tijdens de test veranderingen ondergaat.*

02 Registreer de uitvoering van de penetratietest.

03 Rapporteer over de resultaten van de penetratietest.

Het rapportageformat legt duidelijk vast welke informatie de rapportage moet bevatten.

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

- *type penetratietest (white, grey, back of crystal box);*
- *het tijdstip waarop de test is uitgevoerd;*
- *de gebruikte applicaties (inclusief versienummer);*
- *de parameters die zijn gebruikt bij de tests;*
- *een toelichting per gevonden verbeterpunt;*
- *een inschatting van de prioriteit per verbeterpunt.*

04 Communiceer de rapportages met verbetervoorstellen met verantwoordelijken/eigenaren van applicaties waarin kwetsbaarheden en zwakheden gevonden zijn.

05 Beleg implementatie-acties en stel uitvoerings- of systeemdocumenten beschikbaar waaruit blijkt dat de verbetervoorstellen zijn geïmplementeerd.

Plan de activiteiten die worden uitgevoerd (wie, wat en wanneer) indien geïmplementeerde maatregelen niet aan de gestelde eisen en/of verwachtingen hebben voldaan of tekortkomingen hebben opgeleverd.

Scope

06 Definieer het object van onderzoek in een scopedefinitie.

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

Geef goed aan om welke componenten het gaat. Denk hierbij aan applicaties voor verschillende besturingssystemen, third-partybibliotheken etc.

Geef vooraf de diepgang van de penetratietest aan. Valt bijvoorbeeld het gebruiken van exploits binnen scope of niet? Wordt de scope beperkt tot bepaalde Uitvoeringsdomeinen van de NCSC-richtlijnen of worden hier geen beperking aan gesteld?

Voer voorafgaand een risicoanalyse uit waaruit blijkt dat kwetsbaarheden in een applicatie een groot risico zijn en vervolgens wordt dan de penetratietest uitgevoerd om in kaart te brengen welke kwetsbaarheden er zijn en hoe ze opgelost kunnen worden.

07 Stem de opdracht af met en accordeer deze door een voldoende gemandateerde vertegenwoordiger.

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

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

08 Zorg voor een vrijwaringsverklaring voor penetratietesters, met eventuele beperkingen.

C.05 Technische controlefunctie

De technische controlefunctie betreft technische controleactiviteiten aangaande de applicatie. Deze controles kunnen zowel in ontwikkelfase als in de implementatiefase worden uitgevoerd. In de ontwikkelfase worden verschillende technische controles uitgevoerd, zoals:

- een codereview tijdens ontwikkelingstrajecten om in een vroegtijdig stadium potentiële kwetsbaarheden te ontdekken;
- een periodieke (geautomatiseerde) blackboxscan om te testen of er kwetsbaarheden in de applicatie bestaan.

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

C.05 Technische controlefunctie

Criterium (wie en wat)	De functionaris verantwoordelijk voor de technische controlefunctie van de applicatie voert periodiek **(technische) evaluaties** van de beveiligingsfunctionaliteit van de applicatie uit.
Doelstelling (waarom)	Het vaststellen van de juiste werking van de applicatie en het tijdig signaleren van afwijkingen/kwetsbaarheden.
Risico	Geen inzicht in de status van de operationele implementatie en beveiliging van ICT-componenten.
Classificatie	Midden

Maatregelen

(Technische) evaluaties

01 Voer periodiek reviews of geautomatiseerde scans op de volledige broncode uit.

Het scannen is mogelijk voor wie betrokken is bij het ontwikkeltraject en/of beschikt over de broncode van de programmatuur, door het uitvoeren van codereviews.
Als de software door een externe partij is ontwikkeld, dan wordt de broncode door die softwareleverancier beschikbaar gesteld of de softwareleverancier geeft hierover een verklaring van een onafhankelijke derde af.
Er is documentatie beschikbaar met daarin:

- *dat er een codereview is uitgevoerd;*
- *de bevindingen/rapportage van de codereview;*
- *op welke wijze de bevindingen verwerkt zijn.*

02 Voer periodieke (blackbox-)scans uit, waarbij de volledige functionaliteit van de applicatie geraakt wordt.

Er moet aantoonbaar opvolging worden gegeven; verbeteringen worden doorgevoerd indien geïmplementeerde maatregelen niet voldoen aan de gestelde eisen en/of verwachtingen of tekortkomingen opleveren.
Zorg voor afspraken met de leverancier, over het uitvoeren van een blackboxscan.

Verdieping

Codereview
Om een codereview uit te voeren zijn op hoofdlijnen twee mogelijkheden:

- Geautomatiseerd scannen van de broncode
  Met behulp van geautomatiseerde tools wordt de broncode gescand (ook bekend als statische analyse) op zoek naar patronen die mogelijke kwetsbaarheden vormen.
- Handmatige codereview
  Een handmatige codereview bestaat uit het zoeken in en analyseren van de broncode op zoek naar patronen die mogelijke kwetsbaarheden en zwakheden vormen. Bij een handmatige codereview wordt de broncode gescand door een andere persoon dan de ontwikkelaar.

Deze aanpak, ook wel een whiteboxscan of statische analyse genoemd, kan problemen aan het licht brengen die men via een blackboxscan niet zal ontdekken. Beter nog is het om de codereview in verschillende stadia van het ontwikkelproces uit te voeren om op die manier fouten in een vroeg stadium en dus vaak gemakkelijker te kunnen verhelpen. Een codereview vergt over het algemeen meer inspanning dan een blackboxscan.

Tools voor het uitvoeren van geautomatiseerde codereviews bestaan er in vele soorten en maten. Onderstaande, niet uitputtende lijst geeft enkele punten weer waarop een geautomatiseerde tool kan controleren:

- het afvangen van excepties;
- de mogelijkheid tot het genereren van bufferoverflows;
- de aanwezigheid van type mismatches;
- gebruik van potentieel gevaarlijke functies;
- juiste toepassing van invoervalidatie;
- datastromen door een applicatie.

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

Identificeren en verwijderen van dode code
In de broncode verwijst dode code of onbereikbare code naar stukken code die nooit uitgevoerd (kunnen) worden maar wel in de broncode aanwezig zijn. Deze code kan worden verwijderd zonder dat daarbij semantische eigenschappen van de applicatie veranderen, denk hierbij aan code die uitsluitend gebruikt is voor debuggen. Deze code kan door een kwaadwillende mogelijk worden misbruikt en zou verwijderd moeten worden.

Het verwijderen van dode code heeft zowel voordelen tijdens het compileren als het uitvoeren van de applicatie en verbetert bovendien de onderhoudbaarheid van de applicatie.

Voor het opsporen van dode code is het nodig om de broncode te analyseren. Dit kan met behulp van statische of dynamische codeanalyse en een analyse van de control flow om te kijken welke stukken code niet uitgevoerd (kunnen) worden.

Als de broncode niet beschikbaar is
Als het gaat om closed-source codebibliotheken, software-as-a-service (SaaS) of de ontwikkeling van de software is uitbesteed en er geen handmatige codereview uitgevoerd kan of mag worden, kan worden gedacht aan de volgende aandachtspunten:
- externe certificering van de extern ontwikkelde software;
- afspraken in een overeenkomst vastleggen om de software te auditen;
- afspraken over het dynamisch scannen, bij het dynamisch scannen wordt met behulp van geautomatiseerde tools via de interface van de applicatie, terwijl de applicatie draait, gezocht naar kwetsbaarheden en zwakheden in de applicatie;
- afspraken over het uitvoeren van andere tests, bijvoorbeeld penetratietest (richtlijn C.04) of blackboxscan (zie hierna), om mogelijke kwetsbaarheden op te sporen.

Blackboxscan
Een blackboxscan benadert de aanpak van een kwaadwillende het best, aangezien een tester zonder voorkennis gaat kijken of er kwetsbaarheden in de applicatie bestaan. Tools om blackboxscans uit te voeren zijn bekend onder de noemer applicatiescanner. Een applicatiescanner voert een groot aantal tests uit op een applicatie zoals het uitproberen van verschillende varianten van SQL-injectie en cross-site scripting.

Een applicatiescanner kent enkele beperkingen die belangrijk zijn om in het achterhoofd te houden. Zo is het voor een applicatiescanner vaak moeilijk om ingelogd te blijven in de applicatie als die authenticatie vereist. Door de grote verscheidenheid aan tests die een applicatiescanner uitvoert, bestaat de mogelijkheid dat de applicatie na een aantal tests de sessie beëindigt. Het is voor een applicatiescanner vaak moeilijk om te bepalen dat deze sessie is beëindigd en bijvoorbeeld een cookie niet meer geldig is. Gevolg is dat het testen van applicaties die authenticatie vereisen problematisch en onbetrouwbaar kan zijn.

Tot slot kunnen de scans die een applicatiescanner uitvoert, leiden tot een groot aantal false positives. Het is dus belangrijk dat een persoon met kennis van zaken beoordeelt in hoeverre een gemelde vermeende kwetsbaarheid ook daadwerkelijk een kwetsbaarheid is, hoe eenvoudig deze uit te buiten is en wat de schade zou zijn als gevolg van misbruik.

Wanneer blackboxscans?
Er kunnen meerdere momenten zijn waarop een blackboxscan zinvol is:
- in de acceptatiefase van een nieuwe applicatie;
- bij significante wijzigingen in een applicatie;
- periodiek (jaarlijks/tweejaarlijks), om bestaande applicaties te testen op nieuwe inbraaktechnieken en/of als onderdeel van de PDCA-cyclus;
- als er een andere reden is om te denken dat de beveiliging van een applicatie minder goed is dan gedacht.

De frequentie dient vastgesteld te worden op basis van het risicoprofiel.

C.06 Logging

Logging is een proces voor het registreren van activiteiten en gebeurtenissen in systemen om achteraf de rechtmatigheid van de resourcebenaderingen, evenals vroegtijdig ongeautoriseerde toegangspogingen van systemen en netwerken te kunnen signaleren. Omdat systemen uitgebreide loggingsfunctionaliteit kennen moet vooraf een beperkte maar wel representatieve selectie van de te loggen systeemgegevens worden gemaakt, om de controlewerkzaamheden zo doelmatig mogelijk te laten verlopen. Hierbij moet met een aantal organisatorische en technische aspecten rekening worden houden.

Relevante organisatorische en technische aspecten bij logging zijn:
- detecteren – het signaleren van aanvallen;
- centraliseren – op één punt samenbrengen van loggingsgegevens;
- correlaties (analyse) – het leggen van correlaties tussen de geregistreerde gegevens;
- synchroniseren – het synchroniseren van systeemklokken;
- alternatieven – het beschikken over alternatieven bij uitval van loggingmechanismen;
- bewaartermijnen – het vaststellen van bewaartermijnen van logging;
- integriteit – het beveiligen van loggingsgegevens tegen achteraf wijzigen;
- (pro)actieve controles – het actief uitvoeren van controles op logging.

C.06 Logging

Richtlijn *(wie en wat)*	In de applicatieomgeving zijn signaleringsfuncties (**registratie en detectie**) actief en **efficiënt, effectief** en **beveiligd** ingericht.
Doelstelling *(waarom)*	Het maakt mogelijk eventuele schendingen van functionele en beveiligingseisen te kunnen detecteren en achteraf de juistheid van de uitgevoerde acties, zowel op strategisch als operationeel niveau te kunnen vaststellen.
Risico	Tekortkomingen en zwakheden in de geleverde producten/diensten kunnen niet gesignaleerd worden en herstel acties kunnen niet tijdig worden genomen.
Classificatie	Hoog

Maatregelen

Registratie en detectie

01 Bepaal welke gebeurtenissen en/of beheeractiviteiten aan de applicatie vastgelegd moeten worden.

Stel regelgeving op over vast te leggen gebeurtenissen en handelingen. De regels hierover worden onderhouden. Voorbeelden van vast te leggen gegevens zijn:

- *verdachte gebeurtenissen en wijzigingen aan de webapplicatie;*
- *succesvolle en geweigerde toegangspogingen;*
- *(on)geoorloofde activiteiten door functionarissen.*

Eventueel worden ten behoeve van leesbaarheid en efficiëntie filters gebruikt.

02 *Detecteer aanvallen met detectiesystemen in de webapplicatie-infrastructuur.*

In de ontwerp- of configuratiedocumentatie is vastgelegd waar en hoe IDS'en worden ingezet. Dit is gebaseerd op een risicoanalyse.

Efficiënt en effectief

03 Leg in de ontwerp- of configuratiedocumentatie vast waar en hoe centralisering van logging is ingericht (inclusief configuratie-instellingen).

De inrichting is gebaseerd op een vastgesteld inrichtingsdocument/ontwerp waarin is vastgelegd welke uitgangspunten gelden voor logging. Zorg dat dit inrichtingsdocument/ontwerp onderdeel is van het proces wijzigingenbeheer (zie richtlijn C.08). De ontwerp- en inrichtingskeuzes moeten zijn onderbouwd en op het juiste (organisatie)niveau zijn verantwoord.

Er is een plan met daarin 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.

04 Configureer de systemen zodanig dat interne systeemklokken automatisch gesynchroniseerd worden.

Systemen gebruiken interne systeemklokken voor "time stamps" bij het vastleggen van loggegevens. In de ontwerp- of configuratiedocumentatie is vastgelegd hoe het synchroniseren van de systeemklokken is geconfigureerd.

Beveiligd

05 Bepaal vooraf wat te doen bij het uitvallen van loggingmechanismen (alternatieve paden).

Er wordt aangegeven welke actie een component moet nemen op het moment dat het centrale loggingmechanisme niet meer beschikbaar is.

Er is een procedurebeschrijving van het loggingmechanisme en getest dat het mechanisme van alternatieve actie bij uitvallen loggingmechanismen ook daadwerkelijk werkt.

06 Stel de (online of offline) bewaartermijn voor logging vast en laat dit tot uitdrukking komen in de configuratie-instellingen van de systemen.

Er zijn bewaartermijnen vastgesteld voor de loginformatie. Dit zal moeten blijken uit de configuratie instellingen.

07 Bescherm de loggegevens tegen toegang door onbevoegden beveilig deze tegen achteraf wijzigen/verwijderen.

Ontwerpdocumentatie, configuratie-instellingen en autorisatieprofielen geven aan hoe logfiles beschermd zijn tegen achteraf of ongeautoriseerd wijzigen/verwijderen.

Verdieping

Centraliseren van loggingsgegevens

Logging en ICT-landschap

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

Door de logging op een centraal punt bijeen te brengen en deze intelligent te combineren en te filteren ontstaat een heldere blik op alle informatie vanuit de verschillende componenten uit de infrastructuur.

In een centrale loggingdatabase komt de loginformatie uit verschillende onderdelen van het ICT-landschap samen. Denk hierbij aan de volgende typen informatie:

- logging op het niveau van netwerk-, platform- en applicatiebeveiliging;
- logging op het niveau van identiteit- en autorisatiebeheer;
- logging op het niveau van vertrouwelijkheid en onweerlegbaarheid.

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

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

Aandachtspunten loggingsinformatie

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

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

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

Alternatieven voor beschikbaarheid van registraties (logbestanden)
Het gebruik van centrale loggingmechanismen brengt een belangrijk vraagstuk met zich mee: wat te doen op het moment dat dit centrale loggingmechanisme uitvalt? Op het moment dat een component zijn logging niet meer kwijt kan, bestaat de kans dat deze logging verloren gaat. Dit zou kunnen betekenen dat componenten aanvallen van kwaadwillenden niet meer registreren, of dat transacties niet meer onweerlegbaar zijn. Bepaal daarom op voorhand welke actie een component moet nemen op het moment dat het centrale loggingmechanisme niet meer beschikbaar is. Er bestaan op dit gebied grofweg de volgende mogelijke acties:

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

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

Integriteit van registraties
Om te voorkomen dat kwaadwillende sporen uitwissen moeten logfiles zo zijn ingesteld dat deze achteraf niet kunnen worden aangepast. Deze beveiligingseis is essentieel bij reconstructievraagstukken in relatie tot opgetreden incidenten.

Bewaartermijnen van registraties
Er moet worden bepaald hoe lang logging online en offline beschikbaar moet en mag zijn. Online beschikbaarheid van logging kan essentieel zijn voor het efficiënt verhelpen van beveiligingsincidenten. De duur van offline beschikbaarheid kan beperkt worden door wet- en regelgeving. Voordat wordt besloten om gebeurtenissen in een omgeving te loggen, moet zijn vastgesteld hoe lang en op welke manier logging beschikbaar moet blijven. Dit bepaalt welke media nodig zijn en hoeveel capaciteit voor de logging wordt gereserveerd. Het systeem, waarmee gegevens opgeslagen en behandeld worden, dient dusdanig te zijn dat de gegevens duidelijk geïdentificeerd kunnen worden gedurende hun wettelijke of reglementaire bewaartermijn. De gegevens dienen op een passende wijze vernietigd te kunnen worden na afloop van die termijn voor zover ze niet meer nodig zijn voor de organisatie.

In sommige gevallen is de bewaartermijn voor informatie en het type informatie dat bewaard moet worden geregeld in de nationale wetgeving of voorschriften. Deze beveiligingseis is tevens essentieel bij reconstructie vraagstukken in relatie tot opgetreden incidenten.

C.07 Monitoring

Het monitoren (ofwel bewaken of controleren) van systemen heeft tot doel ongeautoriseerde toegangspogingen tot systeem- en netwerkbronnen en ongeautoriseerd gebruik van deze bronnen tijdig te signaleren en op basis van de ernst van de signalering acties te ondernemen. De monitoringfunctie moet voorbehouden zijn aan een daartoe verantwoordelijke functionaris. Monitoring vindt mede plaats op basis van geregistreerde gegevens (logging). De geregistreerde gegevens dienen te worden geanalyseerd (auditing) en te worden gerapporteerd (alerting). Rapporteren kan ook automatisch door een systeem zelf worden gegevens op basis van vastgestelde overschrijding van drempelwaarden.

C.07 Monitoring

Richtlijn *(wie en wat)*	De loggings- en detectie-informatie (**registraties** en **alarmeringen**) en de condities van de beveiliging van ICT-systemen worden regelmatig gemonitord (**bewaakt**, **geanalyseerd**) en de bevindingen **gerapporteerd**.
Doelstelling *(waarom)*	Tijdig inzetten van correctieve maatregelen en informatie verschaffen over activiteiten van gebruikers en beheerders van de ICT-diensten en de status van de componenten waarmee deze worden voortgebracht.
Risico	Onvoldoende mogelijkheden om tijdig bij te sturen om organisatorisch en technisch te (blijven) voldoen aan de doelstellingen.
Classificatie	Hoog

Maatregelen

Registraties

01 Breng de door verschillende beheerdisciplines gelogde informatie samen voor analysedoeleinden.

Afhankelijk van de typologie van de organisatie is het raadzaam om gelogde gegevens te centraliseren.

Alarmeringen

02 Laat de signaleringssystemen (detectie) tijdig melding maken van ongewenste gebeurtenissen.

In de ontwerp- of configuratiedocumentatie is vastgelegd welke drempelwaarden gelden voor alarmeringen.

Bij alarmeringen gaat het om automatische rapportages gegenereerd door het systeem.

Bewaken

03 Voer periodiek actief controles uit op:

- wijzigingen aan de configuratie van applicaties;
- optreden van verdachte gebeurtenissen en eventuele schendingen van de beveiligingseisen;
- ongeautoriseerde toegang tot en wijzigingen/verwijderen van logbestanden.

Er is een procedurebeschrijving met daarin beschreven hoe en wanneer controles op logging moeten plaatsvinden en hoe taken op dit gebied belegd zijn.

Er is een plan met daarin de activiteiten die worden uitgevoerd (wie, wat en wanneer) indien logrecords op misbruik duiden, geïmplementeerde maatregelen niet aan de gestelde eisen en verwachtingen hebben voldaan of tekortkomingen hebben opgeleverd.

04 Voer periodiek reviews uit van toegangslogs.

Analyseren

05 Analyseer de verzamelde loggingsinformatie in samenhang.

In de ontwerp- of configuratiedocumentatie is vastgelegd waar en hoe correlaties worden aangebracht.

Er is een plan met daarin de activiteiten die worden uitgevoerd (wie, wat en wanneer) indien logrecords op misbruik duiden, geïmplementeerde maatregelen niet aan de gestelde eisen en verwachtingen hebben voldaan of tekortkomingen hebben opgeleverd.

06 Analyseer periodiek de geregistreerde menselijke en systeemacties.

De menselijke acties zijn herleidbaar naar individuele personen.

07 Analyseer periodiek op ongebruikelijke situaties (incidenten) die de werking van applicaties kunnen beïnvloeden.

Rapporteren

08 Rapporteer periodiek de geanalyseerde en beoordeelde gelogde gegevens aan de systeemeigenaren of aan het management.

09 Analyseer en evalueer de rapportages uit de beheerdisciplines compliancemanagement, vulnerability assessment, penetratietest en logging en monitoring op aanwezigheid van structurele risico's.

De resultaten uit deze evaluatie worden geconsolideerd en gerapporteerd naar het hoogste management.

10 Geef aantoonbaar opvolging en voer verbeteringen door indien logrecords op misbruik duiden, geïmplementeerde maatregelen niet voldoen aan de gestelde eisen en verwachtingen of tekortkomingen opleveren.

11 Actualiseer beveiligingsplannen en wijs verantwoordelijken toe voor het realiseren van het beveiligingsplan op basis van de geconsolideerde rapportages.

Verdieping

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

Uit efficiëntie- en beheeroverwegingen moet de monitoringsfunctie zoveel mogelijk vanuit een centrale locatie plaatsvinden. De toegang tot de centrale monitoring, die in een afgeschermde omgeving staat, moet voldoen aan de toegangsbeveiligingscriteria. Inbreuken, zoals onjuiste inlogpogingen, worden direct gedetecteerd, en doorgegeven aan de daartoe verantwoordelijke (onder andere de securitymanager). Verslaglegging vanuit monitoring maakt deel uit van de periodieke rapportage.

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

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

Correlaties tussen gelogde gegevens
Nadat alle loggingsinformatie over applicaties bijeen gebracht is (zie richtlijn C.06/01), is de volgende stap het aanbrengen van correlaties tussen de verschillende gebeurtenissen. De uitdaging hierbij is om alle gebeurtenissen op de verschillende niveaus aan elkaar te correleren en aan een specifieke applicatie te koppelen. Op deze manier kan het pad dat een kwaadwillende heeft doorlopen worden achterhaald en tevens inzicht worden gekregen in de aanvallen die gedurende een bepaalde periode op een applicatie zijn uitgevoerd.

Een goed ingerichte Configuration Management Database (CMDB), zie richtlijn C.11, waarin componenten en de afhankelijkheden daartussen zijn gedefinieerd, kan het leggen van correlaties voor een belangrijk gedeelte vereenvoudigen.

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

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

C.08 Wijzigingenbeheer

Wijzigingenbeheer richt zich op het effectief doorvoeren van wijzigingen in ICT-middelen en ICT-diensten zodanig dat de kans op verstoring van de dienstverlening wordt geminimaliseerd en blijvend voldoet aan de functionele en beveiligingseisen van belanghebbenden.

Wijzigingenbeheer zorgt ervoor dat alle instellingen van de applicatie gecontroleerd en geautoriseerd gewijzigd worden, dit geldt dus ook voor de hardeningsmaatregelen.

Wijzigingen moeten eerst worden getest in een test- of acceptatie-omgeving om de impact van de maatregelen vast te stellen. Dit zorgt ervoor dat de ICT-infrastructuur aan de gestelde maatregelen blijft voldoen.

Het proces configuratiebeheer (richtlijn C.11) is voorwaardenscheppend voor wijzigingsbeheerproces en heeft een beveiligingsbelang in het kader van de integriteits-handhaving, doordat het kan ondersteunen dat updates van ICT-componenten overal worden aangebracht waar ze worden gebruikt.

Voordat een applicatie in productie wordt genomen, is het van belang dat eerst een uitgebreide test wordt uitgevoerd op de applicatie en de omliggende infrastructuur.

Het uitvoeren van tests is niet alleen belangrijk bij de initiële ingebruikname van de applicatie, maar ook na het doorvoeren van belangrijke wijzigingen in de applicatie of de infrastructuur.

Ook voor alle maatregelen die in deze richtlijnen worden beschreven geldt dat deze altijd eerst in een representatieve testomgeving moeten worden uitgeprobeerd voordat ze in een productieomgeving toegepast kunnen worden. Systemen moeten opnieuw worden beoordeeld en getest wanneer wijzigingen plaatsvinden.

Wijzigingen kunnen een onvoorziene negatieve impact hebben op de werking van de ICT-infrastructuur en daarom is het belangrijk te verifiëren of een systeem, ook na het effectueren van wijziging, goed blijft functioneren.

Ontwikkel- en testactiviteiten kunnen verstoringen veroorzaken, bijvoorbeeld onbedoelde wijzigingen in bestanden of systeemomgeving, of storingen in het systeem. Ontwikkel- en testactiviteiten kunnen ook onbedoelde wijzigingen in software en informatie veroorzaken als dezelfde ICT-omgeving wordt gedeeld.

Als ontwikkel- en testmedewerkers toegang hebben tot de productieomgeving en - informatie, zouden zij ongeoorloofde en niet geteste software kunnen invoeren of bedrijfsgegevens kunnen wijzigen. Voorzieningen voor ontwikkeling, testen en productie moeten zijn gescheiden om het risico van onbedoeld wijzigingen of ongeautoriseerde toegang tot productiesystemen en bedrijfsgegevens te verkleinen.

C.08 Wijzigingenbeheer

Criterium *(wie en wat)*	Wijzigingenbeheer is **procesmatig en procedureel** zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van applicaties **tijdig, geautoriseerd** en **getest** worden doorgevoerd.
Doelstelling *(waarom)*	Zekerstellen dat wijzigingen op een correcte en gecontroleerde wijze worden doorgevoerd waardoor de veilige werking van ICT-voorziening wordt gegarandeerd.
Risico	Er kunnen ongeautoriseerde acties worden doorgevoerd of acties zijn onvoldoende op elkaar afgestemd, waardoor de betrouwbaarheid van de ICT-voorziening in het geding kan komen.
Classificatie	Hoog

Maatregelen

Procesmatig en procedureel

01 Laat wijzigingen systematische processtappen doorlopen, zoals intake, acceptatie, impactanalyse, prioritering en planning, uitvoering, bewaking en afsluiting.

In het document wijzigingsbeheerproces zijn onder andere de volgende aspecten vermeld:
- *eigenaar;*
- *afgiftedatum en versienummer;*
- *documenthistorie (wat is wanneer en door wie aangepast);*
- *vastgesteld/geaccordeerd op het juiste organisatorische niveau;*
- *de changekalender.*

Er is een overzicht met alle wijzigingsverzoeken inclusief autorisatie en impactanalyse met betrekking tot informatiebeveiliging.
Er zijn wijzigingsprocessen beschreven die de gehele sequentie van wijzigingen, vanaf initiatie tot afsluiting, weergeven, zoals:
- *impactanalyse van een wijzigingsverzoek;*
- *acceptatie van wijzigingsverzoeken;*
- *categoriseren en prioriteren van wijzigingen;*
- *planning van wijzigingen;*
- *ontwikkelen, inclusief testen, van wijzigingen;*
- *doorvoeren, inclusief validatie, van wijzigingen;*
- *bewaking van wijzigingen;*
- *afsluiten van wijzigingen.*

Er is vastgelegd wie de prioriteit van wijzigingen bepaalt en wie toestemming verleent, bijvoorbeeld een beslissingsforum (Change Advisory Board).
Realisatie en implementatie van wijzigingen worden gepland en deze planningsgegevens worden gepubliceerd (changekalender).
Wijzigingen worden geëvalueerd, waarbij in elk geval vastgesteld wordt of de wijziging niet tot incidenten heeft geleid.

02 Laat alle wijzigingsverzoeken verlopen volgens een formele wijzigingsprocedure (voorkomen van ongeautoriseerde wijzigingen) en OTAP-procedures.

Er zijn procedures gedocumenteerd en vastgesteld voor het overdragen van de ene naar de andere omgeving (van ontwikkel naar test, van test naar acceptatie en van acceptatie naar productie).

03 Sluit functioneel beheer aan op het generiek proces van wijzigingenbeheer.

04 Lever (beheer)documentatie van wijzigingen op conform vastgestelde eisen.

05 Stel wijzigingsprocedures op voor hardware, software en parameterinstellingen (configuratie).

06 Richt configuratiebeheer in en geef daarmee inzicht in gegevens van de kritieke systemen en applicaties.

Tijdig, geautoriseerd

07 Registreer en neem wijzigingen binnen een afgesproken tijdslimiet in behandeling op een gestructureerde wijze.

08 Neem alleen geautoriseerde wijzigingsverzoeken (request for change) in behandeling.

Vanuit efficiëntie- en integriteitsoogpunt is vastgesteld welke functionarissen wijzigingen mogen aanvragen.

09 Neem autorisatie van doorvoeren van wijzigingen in de verschillende OTAP-omgevingen op in het proces van wijzigingenbeheer.

Voor de overgangen van ontwikkel, test, acceptatie en productieomgeving (OTAP) zijn regels en procedures voor het overdragen van systemen van de ene naar de andere omgeving (van ontwikkel naar test, van test naar acceptatie en van acceptatie naar productie).

Testen

10 Test alle wijzigingen altijd eerst voordat deze in productie worden genomen en neem ze via vastgestelde wijzigings- en releaseprocedures in productie.

Bij de testactiviteit zijn onder andere volgende aandachtpunten van belang:

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

Applicaties worden getest voordat deze in de productie worden genomen:

- *Voor nieuwe systemen, upgrades en nieuwe versies moeten acceptatie-criteria zijn vastgesteld.*
- *Er zijn procedures opgesteld voor de omvang en diepgang van de tests. Als de wijziging impact heeft op de informatiebeveiliging, is bepaald of er specifieke beveiligingstests uitgevoerd moeten worden (bijvoorbeeld penetratietests (richtlijn C.04), codereviews etc.).*
- *Penetratietesten maken onderdeel uit van de testen (richtlijn C.04).*
- *Als het gaat om standaardsoftware of software-as-a-service (SaaS) kan worden gedacht aan de volgende aandachtspunten:*
  - ***e**xterne certificering van de extern ontwikkelde software;*
  - *afspraken in het contract vastleggen om de software te mogen auditen;*
  - *uitvoeren van andere tests, bijvoorbeeld penetratietest (richtlijn C.04) of blackboxscan (richtlijn C.05), om mogelijke kwetsbaarheden op te sporen.*

11 Scheid ontwikkel, test en acceptatievoorzieningen van productievoorzieningen (OTAP).

In bepaalde situaties kan een OTP-omgeving een afdoende maatregel zijn.

12 Audit de productieomgeving op ongeautoriseerde wijzigingen.

C.09 Patchmanagement

Patchmanagement is een proces dat zorgt voor het verwerven, testen en installeren van patches (wijzigingen in de code) op verschillende softwarecomponenten van een systeem.

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

Grofweg bestaat een ingericht patchmanagementproces uit de volgende stappen:
- stel vast dat een patch beschikbaar is;
- beoordeel de impact van de uitgebrachte patch en de bijbehorende kwetsbaarheid;
- verkrijg de patch via de leverancier;
- test de patch in een test- en/of acceptatieomgeving;
- rol de patch uit in de productieomgeving;
- volg berichtgeving rondom de patch;
- evalueer het gehele proces.

Het proces configuratiebeheer (zie richtlijn C.11) is voorwaardenscheppend voor het patchmanagementproces en heeft een beveiligingsbelang in het kader van de integriteitshandhaving, doordat het kan ondersteunen dat updates van ICT-componenten overal worden aangebracht waar ze worden gebruikt.

C.09 Patchmanagement

Richtlijn (wie en wat)	Patchmanagement is **procesmatig en procedureel**, ondersteund door **richtlijnen**, zodanig uitgevoerd dat laatste (beveiligings-) patches tijdig zijn geïnstalleerd in de ICT-voorzieningen.
Doelstelling (waarom)	Zekerstellen dat technische en software kwetsbaarheden tijdig en effectief worden aangepakt en zo een stabiele omgeving wordt gecreëerd.
Risico	Technische en softwarekwetsbaarheden brengen de stabiliteit en betrouwbaarheid van systemen in gevaar.
Classificatie	Hoog

Maatregelen

Procesmatig en procedureel

01 Beschrijf het patchmanagementproces en laat het goedkeuren door het management en toekennen aan een verantwoordelijke functionaris.

Het beschreven patchmanagementproces geeft aan hoe de organisatie omgaat met updates: hoe snel implementeert de organisatie een kritieke patch, welke stadia moet de patch doorlopen, wie draagt de verantwoordelijkheid.
Zorg voor een actueel overzicht van systemen die in productie draaien maar niet meer worden onderhouden.

02 Voorzie alle ICT-componenten van de meest recente, relevante patches.

03 Stel de rollen en verantwoordelijkheden voor patchmanagement vast.

04 Voer registratie over de verworven patches, hun relevantie, besluit tot wel/niet uitvoeren, datum patchtest, resultaat patchtest, datum uitvoeren patch en patchresultaat.

Richtlijnen

05 Stel een patchrichtlijn op voor de ondersteuning van patchactiviteiten die op het juiste organisatorische niveau is vastgesteld en is geaccordeerd.

Er is een document beschikbaar waarin het patchrichtlijn is beschreven. Er wordt hierbij ook aangegeven dat patchactiviteiten verband houden met de activiteiten van het configuratiebeheer.
De patchrichtlijn heeft betrekking op het vaststellen van de wenselijkheid van het installeren van patches, het correct installeren van de patches en het testen van de geïnstalleerde patches.

C.10 Beschikbaarheidsbeheer

Beschikbaarheidsbeheer is een proces dat ervoor zorgt dat de aangeboden ICT-diensten beschikbaar zijn voor de klant.

Er moeten hersteltijden worden vastgesteld op basis van de gevoeligheid van de applicaties.

Herstelmaatregelen moeten zijn geborgd, bijvoorbeeld back-up en restore en een calamiteitenplan.

Er moeten regelmatig back-ups (reservekopieën) worden gemaakt van essentiële informatie en systemen of applicaties om de integriteit en beschikbaarheid van systemen of applicaties te waarborgen. Hiervoor moeten goede voorzieningen beschikbaar zijn, zodat alle essentiële gegevens en systemen tijdig hersteld kunnen worden na een incident.

Dagelijkse back-ups zijn vaak voldoende maar voor sommige dynamische componenten (zoals databases) is dit wellicht niet afdoende. Bij dergelijke componenten kan worden overwogen om de transactielog van de database beschikbaar te stellen op een uitwijklocatie (remote journaling). In het geval dat een component crasht, kan een up-to-date versie van de component worden gecreëerd door de laatste back-up hiervan terug te zetten en hierop het transactielog toe te passen.

Het is aan te raden om back-ups te versleutelen. Valt een back-up onverhoopt in handen van een kwaadwillende, dan kan deze in dit geval geen toegang krijgen tot de informatie in de back-up.

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

Het kan voorkomen dat voor een gecompromitteerde server, gecompromitteerde bestanden worden hersteld. Om de integriteit van systemen of applicaties te garanderen moet in sommige gevallen een schone installatie van het systeem of applicatie worden uitgevoerd en dat alleen de data vanuit een back-up wordt teruggehaald.

Als de informatieverwerking, en de bijbehorende verantwoordelijkheid, is uitbesteed aan een andere organisatie moeten hierover afspraken worden vastgelegd in een overeenkomst (contract of SLA) tussen beide partijen. Dit geldt ook op het moment dat software-as-a-servicediensten worden ingekocht, denk dan bijvoorbeeld aan cloud escrow.

C.10 Beschikbaarheidsbeheer

Richtlijn *(wie en wat)*	Beschikbaarheidsbeheer is **procesmatig** ingericht, zodat bij calamiteiten de applicatie binnen de gestelde termijn wordt **hersteld en voortgezet**.
Doelstelling *(waarom)*	Waarborgen van de beschikbaarheid van informatieverwerkende systemen of applicaties.
Risico	Onnodig lange uitval van businessactiviteiten na calamiteiten, waardoor bedrijfsdoelstellingen niet worden gehaald.
Classificatie	Hoog

Maatregelen

Procesmatig

01 Beschrijf het beschikbaarheidsbeheerproces en laat het goedkeuren door het management en toekennen aan een verantwoordelijke functionaris.

02 Documenteer de back-up- en herstelprocessen en -procedures voor de hele applicatie-omgeving.
Er is goede en recente back-up van de bestanden aanwezig op een beveiligde locatie. In het geval van een calamiteit moeten deze gegevens eenvoudig toegankelijk gemaakt kunnen worden.

03 Stel een beschikbaarheidsplan op, met daarin beschikbaarheidseisen per systeem, activiteiten, rollen en verantwoordelijkheden, uit te voeren validaties en escalatiepaden.

04 Test en evalueer het beschikbaarheidsplan periodiek.
De back-up- en restoreprocedures worden regelmatig getest op doelmatigheid.

Hersteld en voortgezet

05 Stel hersteltijden van applicaties vast.
Er zijn recoveryprocedures vastgesteld en geïmplementeerd, en back-up en restore maken hier onderdeel vanuit.
De restoreprocedure wordt periodiek getest.
Er worden aantoonbaar opvolging gegeven; verbeteringen doorgevoerd indien geïmplementeerde maatregelen niet voldoen aan de gestelde eisen en verwachtingen of tekortkomingen opleveren.

C.11 Configuratiebeheer

Configuratiebeheer draagt zorg voor de vastlegging van gegevens over de ICT-middelen en ICT-diensten mede voor het beschikbaar stellen van deze gegevens aan andere ICT-beheerprocessen. Deze richtlijnen beperken zich specifiek tot het configuratie-item applicatie. Organisaties kunnen er voor kiezen om applicaties als configuratie-item gedetailleerder op te delen in meerdere componenten.

Applicaties die niet meer worden gebruikt, dienen niet meer online te staan en te worden verwijderd. Ook de informatie die op de 'oude' website(s) is gepubliceerd en koppelingen met backofficesystemen moeten worden verwijderd.

C.11 Configuratiebeheer

Richtlijn *(wie en wat)*	Het configuratiebeheer is **procesmatig** ingericht en zorgt ervoor dat slechts **operationele applicaties** in gebruik zijn.
Doelstelling *(waarom)*	Het voorkomen van misbruik van 'oude' en niet meer gebruikte applicaties en/of informatie.
Risico	Oude applicaties kunnen enerzijds de dienstverlening aan de klanten negatief beïnvloeden en kunnen anderzijds misbruikt worden.
Classificatie	Hoog

Maatregelen

Procesmatig

01 Neem applicaties conform wijzigingsbeheerprocessen in productie.

Operationele applicaties

02 Voer periodiek controles uit of de operationele applicaties nog worden gebruikt of informatie bevatten die kan worden verwijderd.

03 Houd een overzichtslijst bij van de applicaties die operationeel zijn inclusief de daarbij vermelde eigenaren.

Bijlage A **Referenties**

[1] NCSC: ICT-beveiligingsrichtlijnen voor webapplicaties.
https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html

[2] NCSC: Beveiligingsrichtlijnen voor mobiele apparaten.
https://www.ncsc.nl/actueel/whitepapers/beveiligingsrichtlijnen-voor-mobiele-apparaten.html

[3] NCSC: ICT-beveiligingsrichtlijnen voor mobiele apps.
https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-mobiele-apps.html

[4] W. Tewarie: SIVA – Methodiek voor de ontwikkeling van auditreferentiekaders.

[5] CIP: Grip op SSD, de Normen voor Mobiele Apps.
https://www.cip-overheid.nl/downloads/grip-op-ssd/

[6] NCSC: ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS).
https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls.html

Bijlage B **De SIVA-methode**

In deze bijlage wordt de indeling van deze richtlijnen toegelicht.

Indeling van de applicatieomgeving op basis van domeinen (Structuur)

De richtlijnen zijn, naar de gelijknamige domeinen, georganiseerd in de hoofdstukken Beleidsdomein, Uitvoeringsdomein en Beheersingsdomein (of control). Deze indeling komt voort uit het SIVA-raamwerk. [4]

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 applicatie uiteengezet. Per type applicatie is een andere uitvoering nodig. In de ICT-beveiligingsrichtlijnen voor webapplicaties [1] en de ICT-beveiligingsrichtlijnen voor mobiele apps [3] zijn de daarvoor relevante uitvoeringsdomeinen opgenomen.

Beheersingsdomein (control)

Evaluatieaspecten en meetaspecten zijn in dit domein opgenomen. Daarnaast staan hier ook de beheerprocessen beschreven, 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 mobiele apps, 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.

Maatregelen per domein (Inhoud)

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

Beschrijving van de richtlijnen (Vorm)

De richtlijnen kennen een doelstelling en een risico. Hiermee is vastgelegd wat de richtlijn inhoudt en waarom deze gesteld wordt. Vervolgens wordt per conformiteitsindicator uit de richtlijn (de gearceerde trefwoorden) een aantal maatregelen gegeven, waarmee kan worden bereikt (of vastgesteld) dat invulling is gegeven aan de richtlijn.
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.

Analysevolgorde

In deze richtlijnen komt het aspect analysevolgorde uit het SIVA-raamwerk niet aan bod.

Uitgave
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
richtlijnen@ncsc.nl
@ncsc_nl

Juni 2018