Regel Veilige Basisconfiguraties

Een minimale set basisconfiguraties voor veilig gebruik van ICT-middelen

Versie

1.0

Auteur(s)

Lars van Zijl

Regel Veilige Basisconfiguraties

Een minimale set basisconfiguraties voor veilig gebruik van ICT-middelen

Opdrachtgever
Michiel Pellenbarg

Status
Definitief

Verspreiding
Bedrijfsvertrouwelijk

Versiehistorie

Versie	Datum	Auteur	Opmerking
1.0	23 oktober 2024	Lars van Zijl	Scope verduidelijkt

Recensiehistorie

Versie	Datum	Recensent	Opmerking
1.0	28 september 2024	MT BOI	Duidelijkere scoping

Inhoudsopgave

1. Achtergrondinformatie

1.1 Inleiding

Een belangrijk onderdeel van informatiebeveiliging is het voorkomen van beveiligingsincidenten. Een centraal onderdeel hierin is het voorkomen dat kwaadwillende gebruik kunnen maken van technische kwetsbaarheden.

Deze regel gaat specifiek in op de technische kwetsbaarheden die voortvloeien uit onveilige configuraties (configuratiefouten).

1.2 Noodzaak

Informatiesystemen bieden zeeën aan opties om het functioneren van het systeem te beïnvloeden en te laten werken zoals afnemers dat willen. De realiteit is dat niet elke (standaard)configuratie of combinatie veilig is. Sommige instellingen kunnen onbedoelde consequenties hebben, waardoor kwaadwillende de betrouwbaarheid van het systeem kunnen aantasten. Denk hierbij bijvoorbeeld aan zwakke versleuteling of ongewijzigde standaardwachtwoorden.

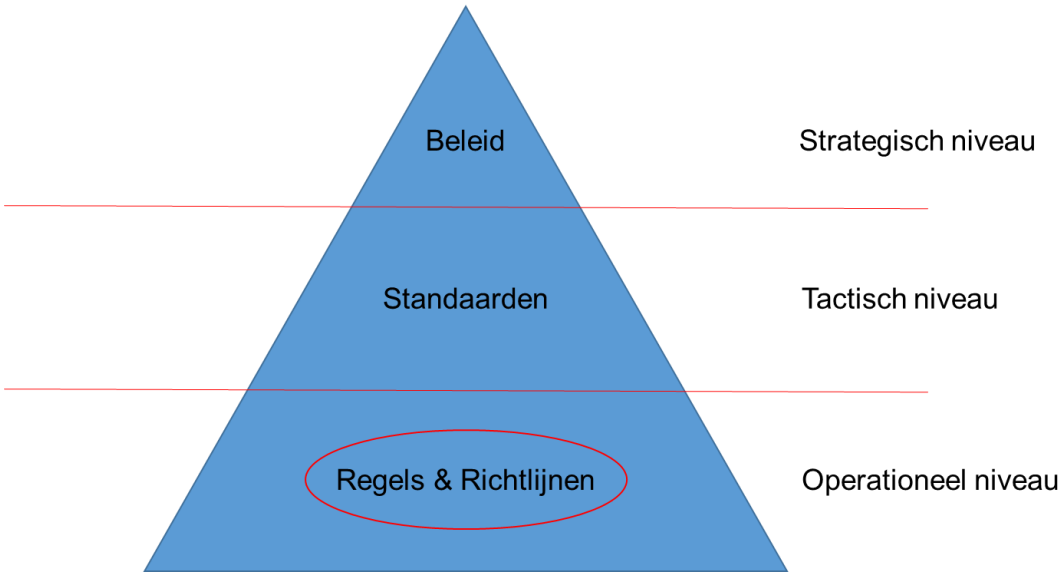
Het kiezen van een veilige set configuraties is hierom van essentieel belang voor het borgen van de betrouwbaarheid van deze informatiesystemen binnen BOI én richting afnemers.

1.3 Doelstelling(en)

Het doel van deze regel is om voor alle ICT-middelen een fundament veilige configuraties voor te schrijven en af te dwingen, zodat de directie BOI in ieder geval een basisniveau beveiliging biedt aan de afnemende diensten elders in de organisatie.

1.4 Reikwijdte

Dit document is van toepassing op de volgende directie(s): BOI. Specifiek de afdeling IT4ALL.



Beleidspiramide Kadaster

1.5 Eigenaarschap

De eigenaar van deze regel is de directeur van de directie BOI. De actiehouder van deze regel is de manager van de afdeling IT4ALL.

1.6 Positionering

Deze regel valt onder de volgende standaard(en): Standaard Beveiligde Bedrijfsvoering.

1.7 Pas-toe-of-leg-uit

Deze regel past de standaard toe.

1.8 Definities

De volgende definities worden in deze regel gehanteerd:

1.8.1 Hardening

Hardenen is het zodanig configureren van een informatiesysteem dat alleen de noodzakelijke functies die benodigd zijn om de taken uit te voeren gebruikt kunnen worden.

1.8.2 External Service Provider (ESP)

Externe dienstenleverancier die een deel van het ICT-landschap van Kadaster faciliteert, verzorgt of onderhoud.

1.8.3 Informatiesysteem

Een informatiesysteem is een georganiseerde set van componenten waarmee informatie over objecten of personen beheerd, verzameld, bewerkt, geanalyseerd, geïntegreerd en gepresenteerd kan worden.

1.8.4 Internal Service Provider (ISP)
Een interne leverancier die (externe) ICT-middelen beschikbaar stelt aan afnemers binnen het Kadaster.

1.9 Randvoorwaarden

- Een bijgewerkte Configuration Management Database (CMDB), met daarin een overzicht van diensten gekoppeld aan interne eigenaren en eventueel externe leveranciers.

2 Scope

Deze regel is van toepassing op de volgende soorten informatiesystemen:

Categorie	**Voorbeelden[1]**
Clouddiensten[2]	▪ Amazon Web Services ▪ Google Cloud ▪ Microsoft 365 ▪ Microsoft Azure
Applicaties	▪ Microsoft Office ▪ Browsers (Firefox / Chrome)
Mobiele telefoons	▪ Apple iOS ▪ Google Android
Printers	▪ Multifunctionals
Netwerkapparatuur	▪ Firewalls ▪ Switches ▪ Routers
Besturingssystemen	▪ Microsoft Windows ▪ Microsoft Windows Server ▪ Linux
Middleware	▪ Webservers (Nginx, Apache) ▪ Database Servers (Oracle, MariaDB)
Virtualisatie	▪ Hypervisors (Vmware ESXI) ▪ Container Orchestration (Kubernetes)

Middleware kan ook aanwezig zijn in de diensten die onderhouden worden buiten BOI IT4ALL. Voor nu zijn deze informatiesystemen buiten scope voor deze regel.

3 CIS Benchmarks

Het Center for Information Security (CIS) onderhoudt configuratievoorschriften (baselines) voor verschillende soorten ICT-middelen en stelt deze gratis ter beschikking. Deze baselines vormen de industriestandaard voor veilige basisconfiguraties voor ICT-middelen.

CIS biedt benchmarks met verschillende niveaus aan diepgang aan (levels), waarbij de niveaus oplopend veiliger zijn. Dit hogere niveau aan beveiliging heeft als keerzijde merkbare impact op de gebruiksvriendelijkheid van het ICT-middel als gevolg.

[1] Slechts voorbeelden. De regel is van toepassing op alle soortgelijke vendoren, producten en/of middelen.
[2] Alleen van toepassing op cloudplatformen die als Infrastructure-as-a-Service (IaaS) of Platforrm-as-a-Service (PaaS) geleverd worden. SaaS-diensten zijn hiermee expliciet uitgezonderd, tenzij uit een risicoanalyse blijkt dat dit toch nodig is.

CIS Niveau	Omschrijving
Level I	Basisvoorschrift om het aanvalsoppervlak te beperken. Weinig tot geen gebruikersimpact.
Level II	Diepgaande voorschriften voor organisaties waar informatiebeveiliging cruciaal is.
STIG	Specifieke voorschriften opgesteld door het Amerikaanse Ministerie van Defensie

4 Regels

De **Product Owners** van diensten die fungeren als Internal Service Provider (ISP) zijn verantwoordelijk voor het implementeren van een CIS Benchmark of soortgelijke industriestandaard op de in scope zijnde ICT-middelen die zij leveren.

Indien een of meerdere **External Service Providers (ESP)** de ICT-middelen van een ISP verzorgen, wordt de implementatie van de CIS Benchmark uitbesteed aan deze partij(en) en contractueel geborgd. De **Product Owner** van de ISP draagt de verantwoordelijkheid voor het laten implementeren van de CIS Benchmark en het contractueel borgen ervan.

Minimaal wordt 'Level I' van de desbetreffende CIS Benchmark of soortgelijke industriestandaard geïmplementeerd, tenzij uit een risicoanalyse blijkt dat een hoger niveau van informatiebeveiliging nodig is.

Het niet bedoeling dat individuele configuraties uit de CIS Benchmark of soortgelijke industriestandaard uitgeschakeld worden. Alleen in uitzonderlijke gevallen kan hier een uitzondering op aangevraagd worden. De **Product Owner** van de ISP is verantwoordelijk voor het aanvragen van een 'Uitzondering op informatiebeveiligingsbeleid' voor een of meerdere configuraties via het 'Uitzondering op informatiebeveiligingsbeleidproces'. Alleen met een goedgekeurde uitzondering mogen de desbetreffende configuraties (deels) uitgeschakeld worden.

External Service Providers rapporteren aan Kadaster over de naleving van de geconfigureerde CIS Benchmark of soortgelijke industriestandaarden op de ICT-middelen die zij leveren.

Het **Cyber Security Team** is verantwoordelijk voor het onafhankelijk monitoren op de naleving van de geconfigureerde CIS Benchmarks of soortgelijke industriestandaarden, via rapportages van de ESP of eigen tooling.

Maandelijks levert het **Cyber Security Team** een rapport over de naleving op aan de Information Security Officer(s) van de directie BOI en de Product Owner(s) van relevante dienst(en) / ISP.

De **Information Security Officer** bespreekt indien nodig de resultaten met de desbetreffende Product Owner(s) van relevante dienst(en) / ISP.