

/// Asset- en configuratiebeheer

1 INTRODUCTIE

Correct werkende computersystemen en applicaties worden steeds belangrijker in organisaties. Deze groeiende afhankelijkheid kan problemen opleveren als uw website bijvoorbeeld offline is door implementatiefouten of wanneer er geen disaster recovery aanwezig is nadat uw systemen zijn vastgelopen of gehackt.

Om dit soort van situaties te voorkomen, is een sterk asset- en configuratiebeheer van groot belang. Dit is de basis voor het beheren en het up-to-date houden van alle soft- en hardware binnen uw organisatie. Asset- en configuratiebeheer schrijft duidelijke regels en verantwoordelijkheden voor met betrekking tot het garanderen dat alle IT-activa – en hun veranderingen – gekend, gedocumenteerd en gemonitord worden. Het juist uitvoeren van een configuratiebeheerbeleid zorgt er dus voor dat uw organisatie kan terugvallen op een continue en actuele inventaris van uw technologische activa en op de hoogte is van hoe het tot deze specifieke inventaris gekomen is.

Om een succesvol beheer te implementeren is het ook belangrijk dat het toezicht van dit beheer wordt toegewezen aan een beleidsmedewerker. Deze persoon heeft de verantwoordelijkheid en de bevoegdheid om de toepassing en naleving van het beleid op te volgen en eventuele inbreuken te rapporteren.

2 WET- EN REGELGEVING

Er bestaat geen specifieke bindende nationale of Europese regelgeving over asset- en configuratiebeheer. Echter, lokale besturen dienen wel rekening te houden met de Algemene Verordening Gegevensbescherming (AVG) of GDPR (General Data Protection Regulation)¹. Deze regelgeving schrijft voor dat alle bedrijven, overheidsdiensten, organisatie en instellingen die in Europa persoonsgegevens verwerken, gebruiken, registreren of bewaren, moeten voldoen aan bepaalde richtlijnen. Deze richtlijnen stellen dat gegevens volgens een afdoend veiligheidsniveau moeten worden verwerkt binnen een organisatie. Met andere woorden, om te voldoen aan de AVG, wordt er verwacht dat systemen die persoonsgegevens bevatten naar behoren worden bijgehouden, waarvoor asset- en configuratiebeheer essentieel is.

Bijkomend, door een gedegen asset- en configuratiebeheer te hebben, bent u als organisatie altijd op de hoogte van de prestaties van uw IT-activa. Hierdoor kunt u op tijd weten wanneer ze hun vereiste functionaliteitseisen niet halen, en potentiële cyberaanvallen of datalekken voorkomen.

3 BELEID

Organisatorische maatregelen

Organisatorische maatregelen verwijzen naar het hebben van duidelijke processen, procedures en verantwoordelijkheden met betrekking tot asset- en configuratiebeheer. Vanuit een organisatorisch perspectief is het belangrijk om een configuratieplanning en -verificatie te definiëren. De planning kan gebruikt worden als configuratiemanagementstrategie en zo structuur geven aan de invulling en uitvoering van de technische maatregelen. De verificatie kan gebruikt worden om te controleren dat de technische processen in orde zijn en de IT-activa hun vereiste functionaliteitseisen halen.

Technische maatregelen

Technische maatregelen verwijzen naar het hebben van documentatie waarin de werking, voorwaarden, verantwoordelijkheden en onderhoud met betrekking tot de verschillende configuratieprocessen en -software beschreven staan. Vanuit een technisch perspectief is het belangrijk om configuratie-identificatie, -veranderingsmanagement en -status accounting te definiëren. Configuratie-identificatie omschrijft voorwaarden met betrekking tot het systematisch selecteren, organiseren en uiteenzetten van IT-activa. Configuratieveranderingsmanagement omschrijft voorwaarden met betrekking tot het managen van goedgekeurde designs en de implementatie van goedgekeurde mutaties en configuratie-status accounting omschrijft voorwaarden voor het monitoren en rapporteren van configuratiedata.

Mensgerichte maatregelen

Het asset- en configuratiebeheer wordt voornamelijk uitgevoerd door IT-medewerkers en daarom verwijzen mensgerichte maatregelen in de context van configuratiebeheer naar maatregelen voor deze specifieke doelgroep. Belangrijke mensgerichte maatregelen zijn het organiseren van voldoende kennistrainingen voor IT-medewerkers en het asset- en configuratiebeheer gebruiks- en onderhoudsvriendelijk houden.

4 AANBEVELINGEN

Hieronder vindt u een aantal aanbevelingen die het Cyber Response Team voor Lokale Besturen (Vo-CRT) geeft met betrekking tot de inrichting van een authenticatiebeheerbeleid.

Organisatorische maatregelen

- Zorg voor de aanwezigheid van een duidelijke asset- en configuratiemanagementstrategie waarin het bijkomende beleid en verantwoordelijke partijen omschreven staan.
- Zorg ervoor dat processen, procedures en verantwoordelijkheden rondom het communiceren van de asset- en configuratiemanagementstrategie naar IT-medewerkers beschreven staan.
- Definieer de configuratie van KPIs, en monitor en review deze op geplande tijdstippen.
- Voer regelmatig een audit uit die uw asset- en configuratiebeheer controleert.

//

Technische maatregelen

- Zorg ervoor dat processen, procedures en verantwoordelijkheden rond het selecteren, organiseren en uiteenzetten van IT-activa attributen beschreven staan.
- Gebruik configuratie baselines per IT-activa (Functional baseline, Allocated baseline, Product baseline, As-Deployed baseline), dewelke iets zeggen over de fase waarin het product design zich bevindt (zie verklarende woordenlijst).
- Zorg ervoor dat de processen, procedures en verantwoordelijkheden rond het doorvoeren van configuratieveranderingen beschreven staan.
- Documenteer alle veranderingen en verander indien nodig de baseline voor gemuteerde IT-activa.
- Zorg ervoor dat de processen, procedures en verantwoordelijkheden rond het monitoren en rapporten van configuratiedata beschreven staan.
- Zorg dat uw configuratie-status account tenminste de volgende informatie monitort en rapporteert:
 - Complete huidige en historische configuratiedocumentatie en unieke identificeurs.
 - Status van de voorgestelde mutaties, afwijkingen, en vrijstellingen voor IT-activa.
 - Status en bepaling van geïdentificeerde afwijkingen en acties tijdens configuratie-audits.

Mensgerichte maatregelen

- Organiseer voldoende kennistrainingen voor IT-medewerkers.
- Zorg voor een gebruiks- en onderhoudsvriendelijk asset- en configuratiebeheer.

5 VERKLARENDE WOORDENLIJST

Term	Verduidelijking	Link naar meer informatie
Functional baseline	Functional baseline verwijst naar de productfase waarin de eerste specificaties zijn gedefinieerd.	What is a Configuration Baseline? - Definition from Techopedia
Allocated baseline	Allocated baseline verwijst naar de productfase waarin de specificaties zijn goedgekeurd.	What is a Configuration Baseline? - Definition from Techopedia
Product baseline	Product baseline verwijst naar de productfase waarin alle fysieke en functionele specificaties zijn doorgevoerd.	What is a Configuration Baseline? - Definition from Techopedia
As-Deployed baseline	As-Deployed baseline verwijst naar de productfase waarin alle noodzakelijke stappen zijn doorgevoerd en gedocumenteerd. Het product is klaar voor gebruik.	What is a Configuration Baseline? - Definition from Techopedia



REFERENTIES

- Asset- en configuratiebeheer van de Vlaamse overheid:
[Asset en configuratie beheer \(asset & configuration management\) \(vlaanderen.be\)](#)

