/// Autorisatiebeleid

1 INTRODUCTIE

Lokale besturen en gemeenten werken elke dag met verschillende soorten informatiesystemen of vertrouwelijke informatie.

Om onbevoegden (binnen uw organisatie) minder gemakkelijk toegang te laten krijgen tot gemeentelijke informatiesystemen en vertrouwelijke informatie is het belangrijk om een logisch autorisatiebeheer te hanteren. Autorisatiebeheer heeft als doel om toegangsrechten (autorisaties) binnen een organisatie te beheren - binnen het wettelijk kader en met in achtneming van doelbinding en proportionaliteit.

Hierdoor kan u als organisatie binnen uw lokaal bestuur zicht houden op de gebruikers en hun autorisaties en bent u beter bestand tegen (potentiële) cyberaanvallen.

2 WET- EN REGELGEVING

Zoals eerder aangegeven moet er bij de uitvoering van een autorisatiebeheer rekening gehouden worden met nationale of Europese regelgeving.
Voor lokale besturen is met name de Algemene Verordening Gegevensbescherming (AVG) of GDPR (General Data Protection Regulation)[1] van belang. 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 schrijven voor dat gegevens volgens een afdoend veiligheidsniveau moeten worden verwerkt binnen een organisatie. Met andere woorden, persoonlijke gegevens mogen enkel gedeeld worden met medewerkers die deze ook daadwerkelijk nodig hebben voor hun werkzaamheden, en dit hangt af van een gedegen autorisatiebeheer.

3 BELEID

Organisatorische maatregelen

Organisatorische maatregelen verwijzen naar het hebben van duidelijke processen, procedures en verantwoordelijkheden met betrekking tot autorisatiebeheer. Bij het inrichten van het autorisatiebeheer is het belangrijk om niet alleen voorwaarden te definiëren voor account- of autorisatiemanagement, maar ook voor authenticatiemanagement. Authenticatie is een belangrijk onderdeel van een autorisatiebeleid omdat men toegang krijgt tot accounts, die bepaalde autorisaties hebben, door middel van authenticatiemiddelen. Bijkomend is het belangrijk om de juistheid en continuïteit van gedefinieerde voorwaarden op te volgen en te rapporteren naar het management.

Technische maatregelen

Technische maatregelen verwijzen naar het hebben van documentatie waarin de werking, voorwaarden, verantwoordelijkheden en onderhoud met betrekking tot de verschillende autorisatieprocessen en -software beschreven staan. Het is belangrijk om vast te leggen hoe, wanneer en aan wie autorisaties uitgereikt mogen worden. Wetgeving kan er bijvoorbeeld voor zorgen dat niet elke medewerker dezelfde autorisaties mag krijgen binnen uw lokaal bestuur.
De Vlaamse overheid biedt een centrale oplossing aan om gebruikers en hun gebruikersrechten te beheren. Via de deze link kan u de documentatie over het Gebruikersbeheer van de Vlaamse overheid raadplegen.

Mensgerichte maatregelen

Mensgerichte maatregelen verwijzen naar het hebben van bewustmakingscampagnes die het belang van een gedegen autorisatiebeheer benadrukken bij gebruikers en bij beheerders van autorisatieprocessen. Dergelijke campagnes zullen ervoor zorgen dat de beleidsprocedures en processen daadwerkelijk gedragen zullen worden door al uw medewerkers en partners.

Fysieke maatregelen

Fysieke maatregelen verwijzen naar het hebben van duidelijke processen, procedures en verantwoordelijkheden met betrekking tot fysiek autorisatiebeheer. Een fysiek autorisatiebeheer is belangrijk aangezien het uw lokaal bestuur controle geeft over de toegangsrechten binnen uw gebouw(en). Hierdoor kan bijvoorbeeld niet elke medewerker toegang krijgen tot het gemeentelijk archief, welke afgeschermde informatie kan bevatten.

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 autorisatiebeheer.

Organisatorische maatregelen

- Zorg ervoor dat de verantwoordelijkheden rond het implementeren en onderhouden van autorisatieprocessen en procedures goed gedefinieerd en bekend zijn.
- Zorg ervoor dat de processen, procedures en verantwoordelijkheden rondom de verschillende soorten accounts (bijvoorbeeld gebruikeraccounts, gedeelde accounts en service-accounts) goed gedefinieerd en bekend zijn.
- Zorg ervoor dat de processen, procedures en verantwoordelijkheden rondom geprivilegieerde gebruikers afzonderlijk gedefinieerd en bekend zijn.

- Definieer autorisatie KPI's, en monitor en review deze op geplande tijdstippen.
- Voer regelmatig een audit uit die uw autorisatiebeheer controleert.

Technische maatregelen

- Gebruik een autorisatieschema, denk hierbij aan een role-based access control (RBAC) of attribute-based access control (ABAC). Het is belangrijk om zo gedetailleerd mogelijk te zijn in het uitgeven van autorisaties.
- Zorg dat de volgende controles worden uitgevoerd bij het toekennen van nieuwe autorisaties:

  De administratieve en technische verantwoordelijke checken op:
  - het minst geprivilegieerde principe;
  - Functiescheiding;
  - het autoriseren van gedeelde accounts op basis van de autorisatierechten van de minst geprivilegieerde gebruiker.

  De data verantwoordelijke checkt op:
  - de noodzaak om toegang te krijgen tot vertrouwelijke data.

  De systeem/applicatie verantwoordelijke checkt op:
  - de noodzaak om toegang te krijgen tot (vertrouwelijke) systemen of applicaties.

- Autoriseer gebruikers alleen voor de periode dat dit noodzakelijk is. Dit is vooral belangrijk bij geprivilegieerde gebruikers.
- Documenteer alle autorisatie aanvragen, inclusief de aard van het verzoek, de termijn van de toekenning en de bijbehorende goedkeuringen van de verantwoordelijke entiteiten.
- Het wordt aangeraden om gebruik te maken van tooling om autorisatieprocessen uit te voeren, zoals provisioning van accounts.

Mensgerichte maatregelen

- Sensibiliseer medewerkers en beheerders over het belang van een autorisatiebeheer door middel van bestaande documentatie.
- Zorg ervoor dat in de onboarding van nieuwe medewerkers, het belang van autorisatie benadrukt wordt.

Fysieke maatregelen

- Maak gebruik van autorisatiebeheer voor tenminste de delen van uw gebouw(en) die gevoelige informatie bevatten.

5 VERKLARENDE WOORDENLIJST

Term	Verduidelijking	Link naar meer informatie
RBAC	RBAC staat voor Role Based Access Control en is een methode om het autorisatiebeheer binnen een organisatie in te richten. Volgens deze methode worden autorisaties niet op individuele basis toegekend, maar op basis van de verschillende rollen binnen een organisatie.	https://www.tools4ever.nl/glossary/role-based-access-control2/
ABAC	ABAC staat voor Attribute Based Access Control en is een methode om het autorisatiebeheer binnen een organisatie in te richten. Volgens deze methode worden autorisaties niet op basis van rollen toegekend, maar op basis van de verschillende attributen van een gebruiker binnen een organisatie.	https://www.nist.gov/publications/guide-attribute-based-access-control-abac-definition-and-considerations-1

REFERENTIES

- Toegangsbeheer van de Vlaamse overheid:
Toegangsbeheer | Vlaanderen Intern
- Toegangs- en gebruikersbeheer VVSG:
Toegangs- en gebruikersbeheer (vvsg.be)
- Minimale IAM-maatregelen Vlaamse Overheid:
Vo_Informatieclassificatie_-_Minimale_maatregelen_-_IAM_xle0xg.pdf (vlaanderen.be)
- Minimale PAM-maatregelen Vlaamse Overheid:
Vo_Informatieclassificatie_-_Minimale_maatregelen_-_PAM_srn1jd.pdf (vlaanderen.be)