IDENTITY GOVERNANCE CHECKLIST: 10 PUNTEN VOOR JOUW ORGANISATIE

Hoe goed heb jij grip op identiteiten en toegang?

Identity is voor veel organisaties het grootste aanvalsoppervlak. Toch ontbreekt vaak het overzicht: wie heeft toegang tot wat en is dat nog steeds terecht?

Met deze checklist krijg je snel inzicht in de belangrijkste onderdelen van identity governance.

HOE GEBRUIK JE DEZE CHECKLIST?

☑ Kun je een stelling met zekerheid met "**JA**" beantwoorden? **Zet een vinkje.**

☐ Twijfel je of is het antwoord "**NEE**"? Laat het vakje leeg, daar zit je risico.

1. GEBRUIKERSPROVISIONING

☐ Toegang wordt automatisch toegekend op basis van rol of functie.

Automatische provisioning voorkomt fouten en versnelt onboarding.

Geen vinkje? Dan is toegang afhankelijk van handmatig werk met kans op verkeerde of te ruime rechten.

2. SLAPENDE IDENTITEITEN

☐ Inactieve accounts worden actief opgespoord en verwijderd.

Oude accounts blijven vaak onopgemerkt bestaan.

Geen vinkje? Dan heb je waarschijnlijk actieve accounts zonder eigenaar, dit is een direct securityrisico.

3. ACCESS REVIEWS

☐ Toegangsrechten worden periodiek gecontroleerd en opgeschoond.

Zonder structurele reviews blijven rechten bestaan.

Geen vinkje? Dan stapelen toegangsrechten zich op zonder dat iemand controleert of ze nog nodig zijn.

4. MFA–DEKKING

☐ Multi-Factor Authentication is verplicht voor alle gebruikers.

MFA is een basismaatregel tegen accountmisbruik.

Geen vinkje? Dan zijn er accounts die met alleen een wachtwoord toegankelijk zijn.

5. CONDITIONAL ACCESS

☐ Toegang wordt bepaald op basis van context (apparaat, locatie, risico).

Niet elke login is betrouwbaar.

Geen vinkje? Dan maak je geen onderscheid tussen veilige en risicovolle toegangspogingen.

6. MODERN AUTHENTICATION (PASSKEYS)

☐ Phishing-resistente authenticatie wordt toegepast waar nodig.

Moderne aanvallen omzeilen traditionele MFA.

Geen vinkje? Dan zijn met name kritieke accounts kwetsbaar voor phishing.

7. PRIVILEGED ACCESS (PAM/PIM)

- [ ] Beheeraccounts zijn gescheiden en rechten zijn tijdelijk.

Adminrechten geven maximale toegang.

Geen vinkje? Dan bestaat de kans dat permanente adminrechten misbruikt worden.

8. LIFECYCLE MANAGEMENT

- [ ] Toegang wordt automatisch aangepast bij in-, door- en uitstroom.

Toegang verandert mee met de organisatie.

Geen vinkje? Dan behouden medewerkers waarschijnlijk toegang die niet meer past bij hun rol.

9. MONITORING & LOGGING

- [ ] Identiteitsactiviteiten worden actief gemonitord en opgevolgd.

Zonder monitoring mis je signalen.

Geen vinkje? Dan ontdek je incidenten pas nadat schade is ontstaan.

10. COMPLIANCE & NIS2

- [ ] Identity governance is aantoonbaar ingericht en gedocumenteerd.

Compliance vraagt om bewijs.

Geen vinkje? Dan kun je niet aantonen dat je in control bent met risico op audits en sancties.

WAT BETEKENT JOUW UITKOMST?

- **Meerdere vinkjes gemist?** Dan zijn er zichtbare gaten in je identity governance.
- **Meer dan de helft geen vinkje?** Dan werk je grotendeels op basis van aannames.
- **Bijna alles afgevinkt?** Dan heb je een sterke basis, maar controle vraagt om continu onderhoud.

VOLGENDE STAP: VAN INZICHT NAAR REGIE

Deze checklist laat zien waar je risico loopt, maar niet hoe groot dat risico precies is of hoe je het oplost.

KLAAR OM DE VOLGENDE STAP TE ZETTEN?

Identity is de nieuwe perimeter.
De tooling is er al. Het verschil zit in keuzes maken, eigenaarschap organiseren en processen borgen.

Wil je weten hoe jouw IT-situatie ervoor staat?
Begin met inzicht. Van daaruit ontstaat regie. Neem vrijblijvend contact met één van onze experts op en krijg helderheid over risico's, quick wins en het pad naar beheersbare identity governance.