

Checklist

8.4 – Toegang tot broncode

Thema: Technisch | ISO 27002: 8.4 | Gerelateerd: 8.3, 8.31

Doelstelling

Aantonen dat toegang tot broncode van applicaties en systemen strikt wordt beheerd om ongeautoriseerde wijzigingen, diefstal en sabotage te voorkomen.

Toegangsbeheer voor broncode

- Is toegang tot broncode beperkt tot geautoriseerde ontwikkelaars en beheerders?
- Worden toegangsrechten tot broncode-repositories beheerd via rolgebaseerde toegangscontrole?
- Is leestoegang gescheiden van schrijftoegang tot broncode?
- Worden externe partijen (contractors) met broncode-toegang beperkt via aparte accounts met minimale rechten?
- Worden toegangsrechten tot broncode periodiek gereviewed?

Versiebeheersysteem en beveiliging

- Wordt alle broncode beheerd in een versiebeheersysteem (Git, SVN)?
- Is het versiebeheersysteem beveiligd met authenticatie en autorisatie?
- Worden alle wijzigingen in broncode gelogd met auteur, tijdstip en omschrijving?
- Is MFA verplicht voor toegang tot het versiebeheersysteem?
- Worden branches en merge-rechten beheerd om ongecontroleerde wijzigingen te voorkomen?

Beveiliging van de ontwikkelomgeving

- Is broncode alleen toegankelijk vanuit beveiligde ontwikkelomgevingen?
- Worden productie-omgevingsvariabelen en secrets niet opgeslagen in broncode?
- Is er een secrets management oplossing ingericht (Vault, AWS Secrets Manager)?
- Worden dependency-scans uitgevoerd op gebruikte open-source bibliotheken?

Controle en monitoring

- Worden grote of ongebruikelijke downloads van broncode gedetecteerd en gealarmeerd?
- Wordt broncode gescand op gevoelige informatie (wachtwoorden, API-keys) vóór commits?

- ☐ Is er een procedure bij vermoeden van diefstal of lek van broncode?
- ☐ Worden broncodewijzigingen in productie-branches gereviewd via een four-eyes principe?

Verantwoordelijke:	_____	Datum controle:	_____
Afdeling:	_____	Score:	___ / 22
Reviewcyclus:	☐ Jaarlijks ☐ Na wijziging ☐ Na incident		Status: ☐ Voldoet ☐ Actiepunt ☐ N.v.t.