

## Checklist

## 8.15 – Logging

Thema: Technisch | ISO 27002: 8.15 | Gerelateerd: 8.16, 8.17

### Doelstelling

Aantonen dat activiteiten, uitzonderingen en beveiligingsgebeurtenissen worden gelogd en dat logbestanden worden beschermd en bewaard voor analyse en onderzoek.

#### Logbeleid en -strategie

- ☐ Is er beleid voor logging dat vastlegt welke systemen en activiteiten gelogd moeten worden?
- ☐ Zijn de te loggen gebeurtenissen per systeem gedefinieerd (inlogpogingen, wijzigingen, fouten)?
- ☐ Is de minimale retentietermijn voor logbestanden vastgelegd (conform wet- en regelgeving)?
- ☐ Is het logbeleid afgestemd op beveiligings- en compliancevereisten?

#### Wat wordt gelogd

- ☐ Worden succesvolle en mislukte inlogpogingen gelogd?
- ☐ Worden wijzigingen in gebruikersrechten en systeemconfiguraties gelogd?
- ☐ Worden toegang tot en wijzigingen van gevoelige data gelogd?
- ☐ Worden systeemfouten en uitzonderingen gelogd?
- ☐ Worden beheerdershandelingen (admin-acties) volledig gelogd?

#### Bescherming van logbestanden

- ☐ Worden logbestanden beschermd tegen ongeautoriseerde wijziging of verwijdering?
- ☐ Worden logbestanden opgeslagen op een centrale, beveiligde locatie (SIEM of log-server)?
- ☐ Hebben beheerders van de gelogde systemen geen schrijfrechten op de logbestanden?
- ☐ Worden logbestanden versleuteld opgeslagen of verstuurd?

#### Bewaring en toegang

- ☐ Worden logbestanden bewaard conform de vastgestelde retentietermijn?
- ☐ Is toegang tot logbestanden beperkt tot geautoriseerde functionarissen?
- ☐ Kunnen logbestanden snel worden doorzocht en geanalyseerd bij een incident?



Is er een procedure voor het beschikbaar stellen van logs bij forensisch onderzoek?

|                    |                                          |                 |                                        |
|--------------------|------------------------------------------|-----------------|----------------------------------------|
| Verantwoordelijke: | _____                                    | Datum controle: | _____                                  |
| Afdeling:          | _____                                    | Score:          | ___ / 21                               |
| Reviewcyclus:      | ■ Jaarlijks ■ Na wijziging ■ Na incident |                 | Status: ■ Voldoet ■ Actiepunt ■ N.v.t. |