

Checklist

5.29 – Informatiebeveiliging tijdens verstoring

Thema: Organisatorisch | ISO 27002: 5.29 | Gerelateerd: 5.30, 8.13, 8.14

Doelstelling

Aantonen dat de organisatie de informatiebeveiliging op peil houdt tijdens verstoringen, calamiteiten en crises.

Continuïteitsplanning voor beveiliging

- ☐ Is informatiebeveiliging expliciet opgenomen in het bedrijfscontinuïteitsplan (BCP)?
- ☐ Zijn beveiligingseisen vastgelegd voor uitwijkscenario's en noodomgevingen?
- ☐ Is vastgelegd welke beveiligingsmaatregelen minimaal gehandhaafd moeten blijven tijdens verstoring?
- ☐ Wordt bij activering van het BCP ook de CISO of beveiligingsfunctionaris betrokken?

Noodprocedures en toegang

- ☐ Is er een noodtoegangsprocedure (break-glass) voor kritieke systemen bij uitval van normale toegang?
- ☐ Worden noodaccounts en -wachtwoorden veilig beheerd en periodiek geroteerd?
- ☐ Is toegang tot noodprocedures beperkt tot bevoegde functionarissen?
- ☐ Worden noodtoegangsgebruik gelogd en achteraf gecontroleerd?
- ☐ Is vastgelegd hoe noodtoegang wordt ingetrokken na herstel van normale situatie?

Beschikbaarheid van beveiligingsfuncties

- ☐ Zijn beveiligingsmonitoring en -logging beschikbaar tijdens een verstoring?
- ☐ Is de SIEM of logging-infrastructuur redundant uitgevoerd?
- ☐ Zijn beveiligingscontacten (CISO, CSIRT) bereikbaar tijdens een calamiteit?
- ☐ Is vastgelegd hoe communicatie over beveiligingsincidenten verloopt tijdens een crisis?

Testen en oefenen

- ☐ Worden continuïteitsplannen inclusief beveiligingsaspecten periodiek getest?
- ☐ Worden beveiligingsfunctionarissen betrokken bij BCP-oefeningen?
- ☐ Worden lessen over beveiliging uit oefeningen verwerkt in verbeterde plannen?
- ☐ Is er aandacht voor cyberdreigingen als oorzaak van verstoringen in oefenscenario's?

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