

Checklist

8.8 – Beheer van technische kwetsbaarheden

Thema: Technisch | ISO 27002: 8.8 | Gerelateerd: 8.19, 12.6

Doelstelling

Aantonen dat technische kwetsbaarheden in informatiesystemen tijdig worden geïdentificeerd, beoordeeld en verholpen om misbruik en schade te voorkomen.

Identificatie van kwetsbaarheden

- ☐ Is er een proces voor het actief monitoren van kwetsbaarheidsmeldingen (NCSC, leveranciers)?
- ☐ Worden beveiligingsadviezen van leveranciers structureel gevolgd en beoordeeld?
- ☐ Wordt minimaal jaarlijks een kwetsbaarhedenscan uitgevoerd op systemen?
- ☐ Zijn alle systemen en softwareversies geregistreerd zodat kwetsbaarheden gekoppeld kunnen worden?
- ☐ Worden ook cloudservices en uitbestede systemen meegenomen in de kwetsbaarhedenbeoordeling?

Prioritering en risicoafweging

- ☐ Wordt per kwetsbaarheid een expliciete risicoafweging uitgevoerd?
- ☐ Worden kwetsbaarheden met hoge kans op misbruik EN hoge schade binnen één week aangepakt?
- ☐ Is er een prioriteringsschaal (bv. kritiek/hoog/midden/laag) die consequent wordt toegepast?
- ☐ Worden uitzonderingen (niet-patchen) onderbouwd en gedocumenteerd?

Patching en mitigatie

- ☐ Is er een patchbeleid met vastgestelde doorlooptijden per risiconiveau?
- ☐ Worden patches getest in een acceptatieomgeving vóór productie-uitrol?
- ☐ Worden systemen die niet gepatcht kunnen worden gecompenseerd met andere maatregelen?
- ☐ Is het patchproces geautomatiseerd waar mogelijk (bv. WSUS, SCCM, Ansible)?
- ☐ Worden patches na uitrol geverifieerd op correcte installatie?

Monitoring en rapportage

- ☐ Worden openstaande kwetsbaarheden en patchstatus gerapporteerd aan het management?
- ☐ Is er een dashboard of overzicht van de actuele kwetsbaarhedenstatus?

- ☐ Worden trends in kwetsbaarheden geanalyseerd om structurele verbeteringen door te voeren?
- ☐ Worden bevindingen uit kwetsbaarhedenscans opgenomen in het risicobeheer?

Penetratietesten en red teaming

- ☐ Wordt minimaal jaarlijks een penetratietest uitgevoerd op kritieke systemen?
- ☐ Worden bevindingen uit penetratietesten aantoonbaar opgevolgd?
- ☐ Is red-teaming overwogen of uitgevoerd voor systemen met hoog risico?

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