

Checklist

8.23 – Webfiltering

Thema: Technisch | ISO 27002: 8.23 | Gerelateerd: 8.20, 8.7

Doelstelling

Aantonen dat toegang tot externe websites en internetdiensten wordt gefilterd om blootstelling aan kwaadaardige inhoud, datalekken en ongepast gebruik te beperken.

Webfilterbeleid

- ☐ Is er beleid voor webfiltering dat vastlegt welke categorieën websites geblokkeerd worden?
- ☐ Is het beleid afgestemd op het aanvaardbaar-gebruikbeleid?
- ☐ Worden risicovolle categorieën standaard geblokkeerd (malware, phishing, illegale content)?
- ☐ Is vastgelegd wie uitzonderingen kan aanvragen en goedkeuren?

Technische implementatie

- ☐ Is een webfilteroplossing (proxy, DNS-filtering, cloud-gebaseerd) ingericht?
- ☐ Worden categoriefilters toegepast op basis van actuele URL-databases?
- ☐ Is SSL/TLS-inspectie ingericht voor versleuteld webverkeer?
- ☐ Worden downloads van uitvoerbare bestanden gescand op malware?
- ☐ Is webfiltering ook van toepassing op mobiele apparaten en thuiswerkers (cloud proxy, DNS)?

Monitoring en rapportage

- ☐ Worden geblokkeerde toegangspogingen gelogd?
- ☐ Worden trends in webfiltergebeurtenissen gerapporteerd aan management of CISO?
- ☐ Worden pogingen tot toegang tot kwaadaardige sites als beveiligingssignaal behandeld?
- ☐ Worden gebruikers geïnformeerd wanneer een website geblokkeerd is en waarom?

Uitzonderingen en handhaving

- ☐ Is er een proces voor het aanvragen en goedkeuren van uitzonderingen op het webfilter?
- ☐ Worden uitzonderingen periodiek gereviewd en verlopen uitzonderingen automatisch geblokkeerd?
- ☐ Is er monitoring op omzeiling van het webfilter (VPN-gebruik, tor, proxy)?



Worden overtredingen van het webfilterbeleid signaleerd en opgevolgd?

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