littlebit
TECHNOLOGY

Cyberbeveiliging in de IT-branche: checklist voor besluitvormers

Actiegebied	Maatregel/doel	Verantwoordelijkheid voor de uitvoering	Status van de uitvoering	Technische uitvoering
Governance & verantwoordelijkheid	Cyberbeveiliging verankeren op managementniveau (CISO benoemen en integreren in management)	Directie/raad van bestuur	☐	CISO-rol introduceren; duidelijke verantwoordelijkheden en middelen definiëren
Bescherming van identiteit en toegang	Verplichte multi-factor authenticatie (MFA) invoeren in het gehele bedrijf	Verantwoordelijke voor IT-beveiliging /IT-management	☐	IT: MFA-oplossing implementeren voor alle gebruikersaccounts
Bescherming van identiteit en toegang	Externe toegang en onderhoud op afstand consequent beveiligen (bijv. alleen via VPN/Zero Trust met MFA)	IT-management/netwerkbeheerder	☐	IT: VPN/Zero Trust Network Access opzetten; MFA activeren voor alle externe aanmeldingen
Training en bewustmaking	Regelmatig phishing-tests uitvoeren en Security Awareness-training voor alle medewerkers verzorgen	Afdeling HR/IT-beveiligingsteam	☐	HR/IT: Trainingsprogramma opzetten; phishing-simulatietools gebruiken
Leveranciersbeheer	Betrouwbaarheid en beveiligingsstandaarden van alle leveranciers regelmatig controleren en documenteren	Afdeling Inkoop/Supply Chain Management	☐	Afdeling Inkoop: beveiligingsvragenlijsten en -certificaten verkrijgen en analyseren (bijv. ISO 27001)
Leveranciersbeheer	Beveiligingsvereisten contractueel vastleggen en audits van kritieke leveranciers regelen	Directie/afdeling Compliance	☐	Afdeling Compliance: Minimale beveiligingsstandaarden (bijv. verplichte MFA, patch-deadlines) opnemen in leveringscontracten; IT: audits uitvoeren bij leveranciers

Netwerk- & toegangscontrole	Netwerksegmentatie en toegangscontrole implementeren (alleen bevoegde apparaten/gebruikers krijgen toegang)	IT-afdeling/beheerders	☐	IT: Netwerk segmenteren, Network Access Control (NAC) implementeren (geautoriseerde toegang afdwingen)
Systeembeveiliging & onderhoud	Voor consistent patchbeheer zorgen (beveiligingsupdates tijdig en volledig installeren)	IT-afdeling/team van beheerders	☐	IT: updatebeheer automatiseren; patches onmiddellijk toepassen in overeenstemming met de richtlijnen
Product- en systeemintegriteit	Integriteit van software- en firmware-updates waarborgen (uitsluitend ondertekende updates toestaan)	Productontwikkeling/IT-beveiliging	☐	IT: Code Signing gebruiken en updates op integriteit controleren alvorens deze worden gedistribueerd
Incident- en crisisbeheer	Incidentenbestrijdingsplan opstellen voor cyberaanvallen (inclusief incidenten in de toeleveringsketen) en dit regelmatig oefenen	IT-beveiligingsteam/crisisteam	☐	IT-beveiliging: noodplan documenteren; regelmatig incidentbestrijdingsoefeningen houden (ook met partners)
Incident- en crisisbeheer	Procedures opstellen voor veiligheidswaarschuwingen en het terugroepen van producten (onveilige producten onmiddellijk van de markt halen)	Product-/kwaliteitsbeheer	☐	