Verdel cybersecurity checklist©

Hoe goed ben jij gewapend tegen cybercriminaliteit en op welke vlakken is er nog werk aan de winkel?
Na het invullen van de checklist heb je een duidelijk overzicht hoe de beveiliging er binnen jouw bedrijf voor staat.

Beoordeel onderstaande security-elemenenten met een cijfer: 1 = slecht, 2 = matig of 3 = voldoende.
In totaal zijn er 57 punten te behalen.

Categorie 1: Mens

- ☐  Bewustzijn
- ☐  Organisatie
- ☐  Clean desk policy
- ☐  Bezoekersprogramma

Categorie 2: Techniek

- ☐  Netwerksecurity
- ☐  Device management
- ☐  Applicatie
- ☐  Continue monitoring
- ☐  Toegangscontrole
- ☐  MFA
- ☐  VPN
- ☐  Secure wifi
- ☐  DNS en webfiltering
- ☐  EDR
- ☐  Secure endpoint configuratie

Categorie 3: Proces

- ☐  Organisatorische veerkracht
- ☐  Beheerprocessen
- ☐  Software beheer
- ☐  Vulnerability Management

En nu?

Scoor jij minder dan 40 punten, zeer matig op een categorie of wil je meer weten over deze checklist en jouw score? Neem vrijblijvend contact op met ons securityteam via info@verdel.nl of bel naar (071) 331 01 84.

Verdel cybersecurity checklist©

Categorie 1: Mens

Bewustzijn I Is iedereen binnen het bedrijf op de hoogte van de dagelijkse securityrisico's en weten medewerkers hoe ze adequaat moeten reageren op een phishingmail en andere gevaren?

Organisatie I Het securitybeleid van je organisatie is van groot belang om je goed te weren tegen cybercriminaliteit. Is er voor het bedrijf een securitybeleid opgesteld en in hoeverre zijn alle medewerkers hiervan op de hoogte?

Clean desk policy I In hoeverre zijn de bureaus na een werkdag leeg? En in welke mate voorkom je dat een kwaadwillende toegang heeft tot rondslingerende USB-sticks of documenten?

Bezoekersprogramma I Is het pand voor iedereen vrij toegankelijk? En is het hierdoor mogelijk dat een ongewenste bezoeker gemakkelijk het bedrijf betreedt om data te verzamelen? Denk hierbij aan rondslingerende USB-sticks, laptops of documenten.

Categorie 2: Techniek

Netwerksecurity I In hoeverre is het interne netwerk ingericht om bedrijfsgegevens te beschermen? Is het netwerk bijvoorbeeld opgeknipt in verschillende onderdelen (via VLAN) en is er een gedegen firewall geïnstalleerd?

Device management I In welke mate zijn (derde) devices van medewerkers beveiligd om de data van het bedrijf te beschermen? Worden de laptops en telefoons waarmee medewerkers toegang hebben tot bedrijfsdata regelmatig geüpdatet en is hier controle op?

Applicatie I Niet geüpdatete programma's vormen een bedreiging voor je interne netwerk. In hoeverre stuur je als bedrijf op updates en controleer je wie er toegang hebben tot de applicaties?

Continue monitoring I Hoe snel ontdek je een technische storing of datalek? In welke mate monitort je organisatie dit?

Toegangscontrole I Is er in jouw organisatie sprake van verschillende toegangsrechten tot de bedrijfsdata of kan iedereen overal bij? En in welke mate wordt er gecontroleerd of de rechten nog juist zijn?

MFA I Maakt je bedrijf gebruik van Multi Factor Authenticatie om toegang te krijgen tot het bedrijfsnetwerk en -applicaties?

VPN I Kan je binnen jouw bedrijf overal ter wereld toegang krijgen tot de bedrijfsgegevens? Zo ja, is de toegang tot deze bedrijfsgegevens afgeschermd met een beveiligde verbinding (VPN)?

Secure wifi I In hoeverre is jouw gastenwifi-netwerk afgeschermd van het reguliere wifi-netwerk?

DNS en webfiltering I Is de firewall van het bedrijf zo ingesteld dat websites, waarvan bekend is dat ze een verhoogd risico hebben op malware, afgeschermd zijn en niet bezocht kunnen worden? En staan de DNS-records van jouw e-maildomein goed ingesteld?

EDR I Endpoint Detection en Response is een cyberbeveiligingstechnologie die de gehele dag het bedrijfsnetwerk monitort en automatisch reageert op bedreigingen. Maak je met jouw bedrijf gebruik van deze technologie?

Secure endpoint configuratie I Doe jij er alles aan om de impact van cybercriminaliteit zo klein mogelijk te maken? Maakt jouw bedrijf bijvoorbeeld gebruik van endpoint beveiliging via Intune om de beveiliging op devices in te stellen volgens het bedrijfsprotocol?

Categorie 3: Proces

Organisatorische veerkracht I Ieder bedrijf is vroeg of laat slachtoffer van een cyberaanval. De impact van de aanval heeft alles te maken met de inrichting van jouw beveiliging. Hoe goed heb jij een herstelplan opgesteld en hoe snel is jouw bedrijf weer operationeel na een securityincident?

Beheerprocessen I In welke mate heeft je bedrijf het beheer van het bedrijfsnetwerk geautomatiseerd en ingericht in vaste processen?

Softwarebeheer I Elk programma op een device is een mogelijke ingang voor een hacker. In hoeverre wordt erop toegezien dat ongebruikte software en poorten verwijderd worden van devices?

Vulnerability Management I Aan het bedrijfsnetwerk zijn meer apparaten verbonden dan je denkt. Apparaten die vaak vergeten worden zijn bijvoorbeeld printers en camera's én juist via deze weg komen cybercriminelen graag binnen. Waarom? De apparaten worden sneller vergeten en het aantal securityupdates is heel laag. In welke mate heeft jouw bedrijf deze risico's in kaart gebracht en wordt er met regelmaat gecontroleerd op securitygerelateerde updates?