CENTRE FOR
CYBER SECURITY
BELGIUM

CYBER SECURITY
COALITION.be

CYBERSECURITY-
GIDS VOOR DE KMO

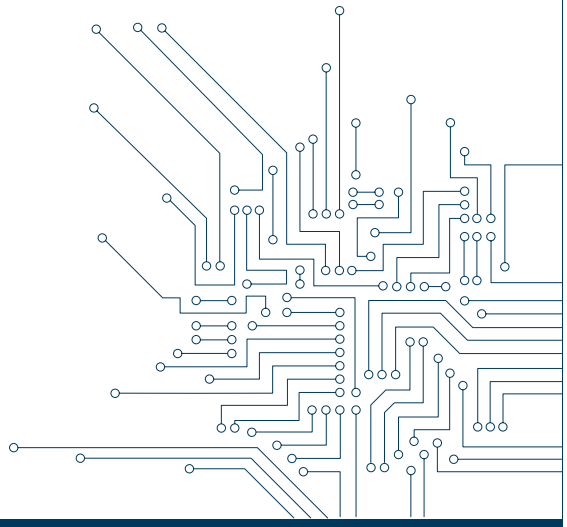
/ BELGIË

OVER DEZE GIDS

DEZE CYBERSECURITY-GIDS WERD OPGESTELD DOOR HET CENTRUM VOOR CYBERSECURITY BELGIË (CCB), IN SAMENWERKING MET DE CYBER SECURITY COALITION BELGIË, EN IS BESTEMD VOOR KLEINE EN MIDDELGROTE ONDERNEMINGEN (KMO'S). HIJ IS GEBASEERD OP DE INPUT EN DE GOEDE PRAKTIJKEN VAN PRIVÉ- EN OVERHEIDSINSTELLINGEN.

Het is de bedoeling de kmo's een overzicht te bezorgen van basis- en meer geavanceerde cyberveiligheidsmaatregelen. Hoewel alle kmo's cybersecurity zouden moeten toepassen op basis van het resultaat van hun eigen risicoassessment, geeft deze gids een quick list van veiligheidscontroles die toegepast kunnen of zouden moeten worden.

Met deze gids zouden kmo's in staat moeten zijn hun cybersecurityniveau te verhogen, cybersecurityrisico's te beperken, kwetsbaarheden te verminderen en hun veerkracht te verbeteren. Hij biedt een eenvoudig kader zodat kleine en middelgrote ondernemingen hun activiteiten op een veilige manier kunnen integreren in een wereldwijd en permanent beschikbare markt.



HET CENTRUM VOOR CYBERSECURITY BELGIE

CENTRE FOR CYBER SECURITY BELGIUM

HET CENTRUM VOOR CYBERSECURITY BELGIË (CCB) IS DE CENTRALE AUTORITEIT VOOR CYBERSECURITY IN BELGIË.

Het CCB is opgericht bij Koninklijk Besluit van 10 oktober 2014. Het Centrum voor Cybersecurity België (CCB) is de centrale autoriteit voor cybersecurity in België. Het zal een nationaal Cybersecuritybeleid opmaken en alle relevante Belgische overheidsdepartementen aanmoedigen om een adequate en geïntegreerde bijdrage te leveren. Het CCB werkt onder het gezag van de eerste minister en maakt voor de uitvoering van zijn taken gebruik van de administratieve en logistieke steun van de Federale Overheidsdienst Kanselarij van de Eerste Minister.
Op www.ccb.belgium.be vindt u een volledig overzicht van de taken van het Centrum terug.

DE CYBERSECURITY COALITION

CYBER SECURITY COALITION.be

DE CYBERSECURITY COALITION IS EEN UNIEK PARTNERSCHAP TUSSEN SPELERS UIT DE ACADEMISCHE WERELD, DE OVERHEDEN EN DE PRIVÉSECTOR DIE OP DIE MANIER HUN KRACHTEN BUNDELEN IN DE STRIJD TEGEN CYBERCRIMINALITEIT.

Op dit ogenblik zijn meer dan 50 belangrijke spelers uit deze drie sectoren actieve leden, die bijdragen aan de opdracht en doelstellingen van de Coalitie. De Coalitie komt tegemoet aan de dringende nood aan een transversale samenwerking om kennis en ervaring te delen, concrete transversale initiatieven in gang te zetten, te organiseren en te coördineren, de bewustwording bij burgers en organisaties te vergroten, de ontwikkeling van expertise te bevorderen en aanbevelingen te schrijven voor een efficiënter beleid en een betere regelgeving.

VOORWOORD

DE KLEINE EN MIDDELGROTE ONDERNEMINGEN (KMO'S) VORMEN EEN BELANGRIJKE MOTOR VOOR INNOVATIE EN GROEI IN BELGIË.

De cybercriminaliteit in kmo-omgevingen vormt een toenemend probleem. In tegenstelling tot grote organisaties hebben de meeste kmo's geen eigen cybersecurityteams (CSIRTs). Cybercriminelen die financieel voordeel willen bekomen of schade willen berokkenen aan bedrijven, zijn geneigd naar gemakkelijke prooien te zoeken. Bovendien heeft het feit dat kmo's afhankelijk zijn geworden van ICT en internet ze kwetsbaarder gemaakt voor cybercriminaliteit. Informatiebeveiliging is dan ook een cruciale zaak geworden voor alle kmo's.

Deze gids met cybersecuritymaatregelen voor kleine en middelgrote ondernemingen werd samengesteld door het Centrum voor Cybersecurity België (CCB), in nauwe samenwerking met de Cybersecurity Coalition. We hebben een lijst van 12 cybersecuritytopics opgemaakt met eenvoudige en geavanceerde aanbevelingen inzake cybersecurity, die kmo's kunnen gebruiken om hun zwakke punten en kwetsbaarheden te beperken en zich te beschermen tegen datalekken en cyberaanvallen.

De basisaanbevelingen in deze gids helpen kmo's om op het vlak van veiligheid een voorsprong te nemen. Ze helpen u de meest voorkomende valkuilen te vermijden en uw waardevolste gegevens te beschermen. De geavanceerde best practices en tips helpen u om nog betere beschermingstechnieken te gebruiken.

MIGUEL DE BRUYCKER
Directeur-generaal Centrum voor Cybersecurity België (CCB)

CHRISTINE DARVILLE
Voorzitster van de Cybersecurity Coalition

INHOUD

01 BETREK HET TOPMANAGEMENT ERBIJ

BASISBESCHERMING

- **Stel** een verantwoordelijke aan voor informatiebeveiliging
- **Identificeer** uw ICT-risico's en beveilig uw onderneming voor de toekomst
- **Streef** ernaar om alle vereisten inzake privacy, gegevensbehandeling en wettelijke en regelgevende veiligheidsvoorschriften te respecteren
- **Wees** u bewust van de cyberdreigingen en kwetsbaarheden in uw netwerken

GEAVANCEERDE BESCHERMING

- **Zorg** ervoor dat de verantwoordelijke voor de informatieveiligheid onafhankelijk is en geen deel uitmaakt van ICT
- **Bepaal** heel duidelijk de doelstellingen van systeem- en netwerkmonitoring
- **Identificeer** de commerciële en wettelijke gevolgen van gegevenslekken, netwerkstoringen ...
- **Voer** regelmatig een risico- en veiligheidsaudit uit; de resultaten en het actieplan worden op C-level gebriefd

02 PUBLICEER EEN EIGEN VEILIGHEIDSBELEID EN GEDRAGSCODE

BASISBESCHERMING

- **Creëer** procedures en pas ze toe bij de aankomst en het vertrek van gebruikers (personeelsleden, stagiairs, etc.)
- **Beschrijf** veiligheidsrollen en –verantwoordelijkheden (voor fysieke veiligheid, veiligheid van het personeel en ICT-veiligheid)
- **Ontwikkel** en verspreid een gedragscode voor het ICT-gebruik
- **Plan** veiligheidsaudits en voer ze uit

GEAVANCEERDE BESCHERMING

- **Maak** een classificatie en markeerschema voor gevoelige informatie
- **Maak** gebruik van de concepten “need to know”, “least privilege” en scheiding van taken in uw beleid en uw businessprocessen
- **Publiceer** een beleid voor responsible disclosure
- **Laat** gevoelige documenten bewaren in afgesloten kasten
- **Laat** gevoelige documenten vernietigen in een papierversnipperaar
- **Laat** op het einde van de werkdag alle documenten die zijn achtergebleven aan de printer versnipperen
- **Stel** de optie “vergrendeld afdrukken” in, als die beschikbaar is
- **Ontwikkel** een concept en een planning voor een cybersecurity-opleiding

03 MAAK UW WERKNEMERS BEWUST VAN DE CYBERRISICO'S

BASISBESCHERMING

- **Laat** de gebruikers uw gedragscode ondertekenen
- **Herinner** de gebruikers regelmatig aan het belang van veilig gedrag
- **Herinner** de gebruikers er regelmatig aan dat de informatie moet worden behandeld als gevoelig & met respect voor de privacyregels
- **Leer** de gebruikers hoe ze phishing (e-mailfraude) kunnen herkennen en hoe ze erop moeten reageren. Een goed hulpmiddel is de volgende test : https://www.safeonweb.be/nl/degrotephishingtest
- **Informeer** de medewerkers van de dienst boekhouding over het fenomeen "CEO-fraude" en voorzie voldoende controle op de uitvoering van betalingen

GEAVANCEERDE BESCHERMING

- **Integreer** de kennis van en het respect voor de gedragscode in de evaluatie van het personeel
- **Evalueer** regelmatig de kennis en reacties van de gebruikers

04 BEHEER UW BELANGRIJKE ICT-ONDERDELEN

BASISBESCHERMING

- **Hou** een inventaris bij van alle ICT-tools en softwarelicenties
- **Zorg** voor een accurate en geactualiseerde kaart van al uw netwerken en interconnecties

GEAVANCEERDE BESCHERMING

- **Gebruik** de configuratiemanagementtool (of ten minste een tool als Microsoft MMC)
- **Leg** een basislijn voor de veiligheidsconfiguratie vast
- **Contracten** en SLA's (Service Level Agreements) bevatten een veiligheidsclausule
- **Implementeer** een change control process
- **Implementeer** een uniform veiligheidsniveau doorheen uw netwerken
- **Voer** regelmatig een audit uit van alle configuraties (met inbegrip van servers, firewalls en netwerkcomponenten)

05 UPDATE ALLE PROGRAMMA'S

BASISBESCHERMING

- **Zorg** voor een interne patch-cultuur (werkposten, mobiele toestellen, servers, netwerkcomponenten, etc.)
- **Voer** zo snel mogelijk securitygerelateerde updates van al uw software uit
- **Automatiseer** het updateproces en controleer de efficiëntie ervan

GEAVANCEERDE BESCHERMING

- **Ontwikkel** een refererentie- en testomgeving voor nieuwe patches
- **Update** alle software van derden zoals browsers en plugins
- **Voor servers**: maak een volledige back-up voor en creëer noodhersteldisks na elke update

06 INSTALLEER ANTIVIRUSBESCHERMING

BASISBESCHERMING

- **Installeer** een antivirussoftware op alle werkposten en servers
- **De updates** van antivirusproducten gebeuren automatisch
- **De gebruikers** weten hoe de antivirussoftware waarschuwt dat er een virusbesmetting is

GEAVANCEERDE BESCHERMING

- **Alle viruswaarschuwingen** worden geanalyseerd door een ICT-expert
- **Installeer** op alle mobiele toestellen een antivirussoftware
- **De antivirussoftware** wordt regelmatig getest met fingerprintoplossingen

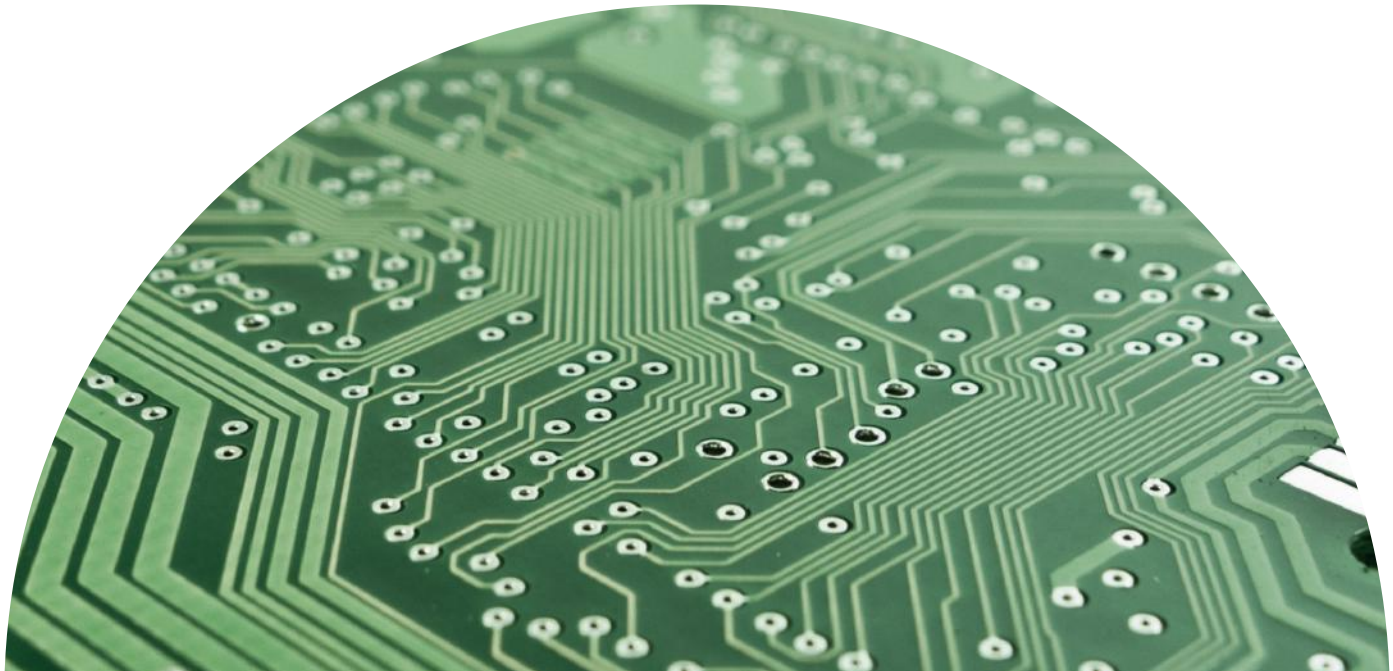
07 MAAK EEN BACKUP VAN ALLE INFORMATIE

BASISBESCHERMING

- **Maak** een dagelijkse back-up van uw belangrijke gegevens
- **Kies** voor eigen of cloud back-upoplossingen
- **Sla** back-ups offline en op een aparte plaats op (indien mogelijk op afstand van hun bron)

GEAVANCEERDE BESCHERMING

- **Back-ups** worden opgeslagen in een veilig of beveiligd gegevenscentrum
- **Regelmatige hersteltests** worden uitgevoerd om de kwaliteit van de back-ups te controleren
- **Geëncrypteerde gegevens** worden opgeslagen in de cloud



08 BEHEER DE TOEGANG TOT UW COMPUTERS EN NETWERKEN

BASISBESCHERMING

- **Verander** alle default paswoorden
- **Niemand** werkt met beheerdersvoorrechten voor dagelijkse opdrachten
- **Hou** de lijst van systeembeheerderaccounts beperkt en geüpdatet
- **Paswoorden** moeten langer zijn dan 10 karakters; een combinatie van karaktertypes; ze moeten op regelmatige tijdstippen of wanneer er een vermoeden van inbreuk is, gewijzigd worden
- **Gebruik** uitsluitend individuele accounts en deel nooit paswoorden
- **Schakel** ongebruikte accounts onmiddellijk uit
- **Leg** paswoord- en authenticatieregels op
- **De rechten** en voorrechten worden beheerd door gebruikersgroepen

GEAVANCEERDE BESCHERMING

- **Gebruikers** krijgen enkel toegang tot informatie die ze nodig hebben om hun opdrachten uit te voeren
- **Zoek** ongebruikte accounts en sluit ze af
- **Gebruik** multifactorauthenticaties
- **Blokkeer** de toegang tot het internet op accounts met beheerdersrechten
- **Zoek** naar abnormale toegangen tot informatie en systemen (tijdsbestekken, toepassingen, gegevens, etc.)
- **Controleer** regelmatig de centrale bestanden (Active Directory of LDAP directory)
- **Beperk** de gebruikstoegang met een badgesysteem en creëer veelvuldige veiligheidszones
- **Registreer** alle bezoeken
- **Laat** de kantoren schoonmaken tijdens de werkuren of onder permanent toezicht

09 BEVEILIG WERKPOSTEN EN MOBIELE TOESTELLEN

BASISBESCHERMING

- **Sluit** werkposten en mobiele toestellen automatisch af wanneer ze niet gebruikt worden
- **Laptops**, smartphones of tablets worden nooit onbewaakt achtergelaten
- **Deactiveer** de autorun-functies van externe media
- **Bewaar** of kopieer alle gegevens op een server of een NAS (Network Area Storage)

GEAVANCEERDE BESCHERMING

- **Harde schijven** en media- en printeropslag die buiten gebruik zijn, worden fysiek vernietigd
- **Verbied** het verbinden van persoonlijke toestellen met het informatiesysteem van de organisatie
- **Encrypteer** harde schijven van laptops
- **Gevoelige of vertrouwelijke gegevens** worden enkel geëncrypteerd verstuurd
- **Zorg** er technisch voor dat niet-geregistreerde draagbare media niet kunnen worden geconnecteerd
- **De gegevens** opgeslagen in de cloud worden geëncrypteerd (bv. BoxCryptor)
- **De garanties** geboden door de cloud provider stemmen overeen met het gevoeligheidsniveau van de opgeslagen informatie
- **Externe media** zoals USB-sticks worden gecontroleerd op virussen voor ze op een computer worden aangesloten

10 BEVEILIG SERVERS EN NETWERKCOMPONENTEN

BASISBESCHERMING

- **Verander** alle default paswoorden en maak niet-gebruikte accounts onbruikbaar
- **Bescherm** de wifi met WPA2-encryptie
- **Sluit** ongebruikte diensten en poorten
- **Vermijd** verbindingen met servers vanop afstand
- **Gebruik** veilige applicaties en protocollen
- **De veiligheidslogs** op de servers en firewalls worden voor een periode van minstens 1 maand bijgehouden
- **Het gastwifinetwerk** wordt apart gehouden van het bedrijfsnetwerk

GEAVANCEERDE BESCHERMING

- **De veiligheidslogs** worden minstens 6 maanden bijgehouden
- **De bedrijfswifi** wordt beschermd met WPA2 Enterprise met toestelregistratie
- **Versterk** alle systemen op basis van de aanbevelingen van de verkoper
- **Gebruik** voor het beheer van de servers een (logisch) van het gebruikersnetwerk afgescheiden netwerk
- **Beoordeel** alle gebeurtenissen/alarmen op server, firewall en netwerkcomponenten
- **Een analyse- en waarschuwingssysteem** gebruikt de logs om elk kwaadwillig gedrag te detecteren (SIEM)
- **Een IDS/IPS** (Intrusion Detection/Prevention System) controleert alle communicatie
- **Fysieke toegang** tot servers en netwerkcomponenten moet beperkt blijven tot een minimum aantal mensen
- **Elke fysieke toegang** tot servers en netwerkcomponenten wordt geregistreerd
- **Voer** penetratietests en kwetsbaarheidsscans uit

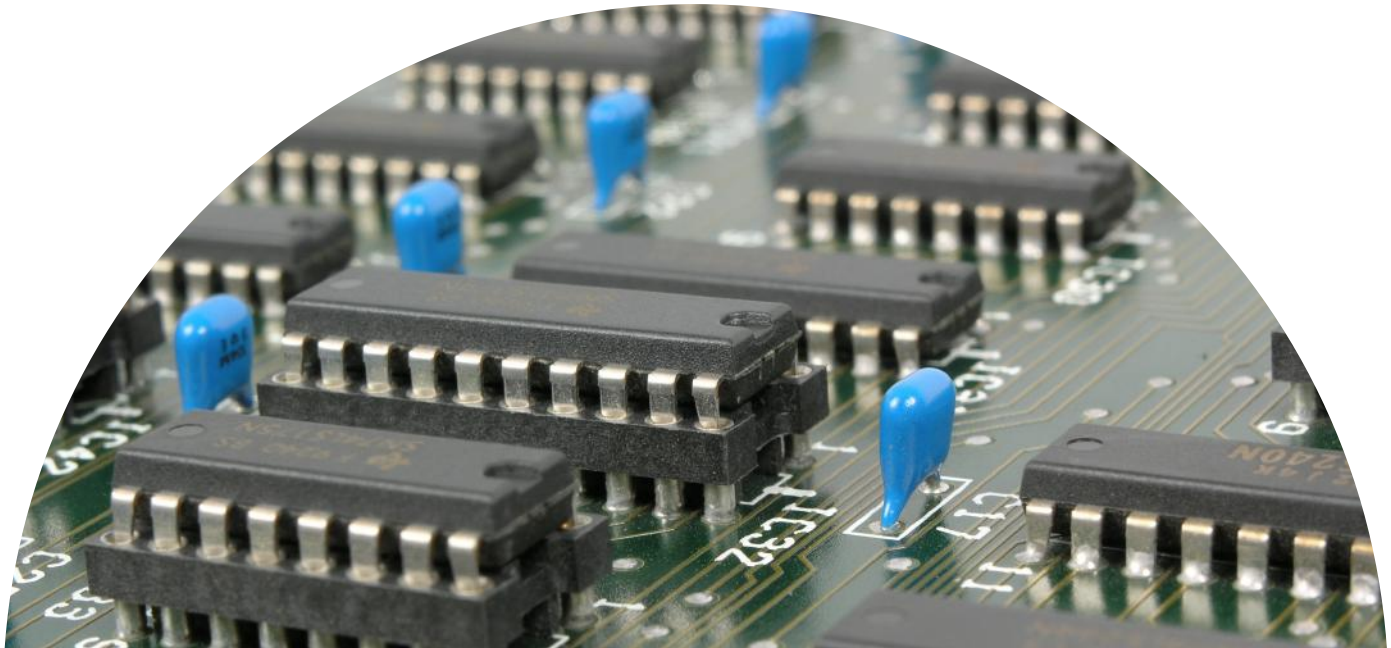
11 BEVEILIG TOEGANG OP AFSTAND

BASISBESCHERMING

- **De toegang** op afstand moet automatisch worden afgesloten wanneer die gedurende een bepaalde periode inactief is
- **Beperk** de toegang op afstand tot het strikt noodzakelijke
- **Alle verbindingen** met het bedrijfsnetwerk zijn beveiligd en geëncrypteerd

GEAVANCEERDE BESCHERMING

- **Werk** enkel met Virtual Private Network (VPN) verbindingen voor eindpunten
- **Hanteer** een strikte authenticatie voor connecties vanuit externe openbare netwerken
- **De toegang** op afstand wordt beperkt tot de IP-adressen van de benodigde providers en regio's



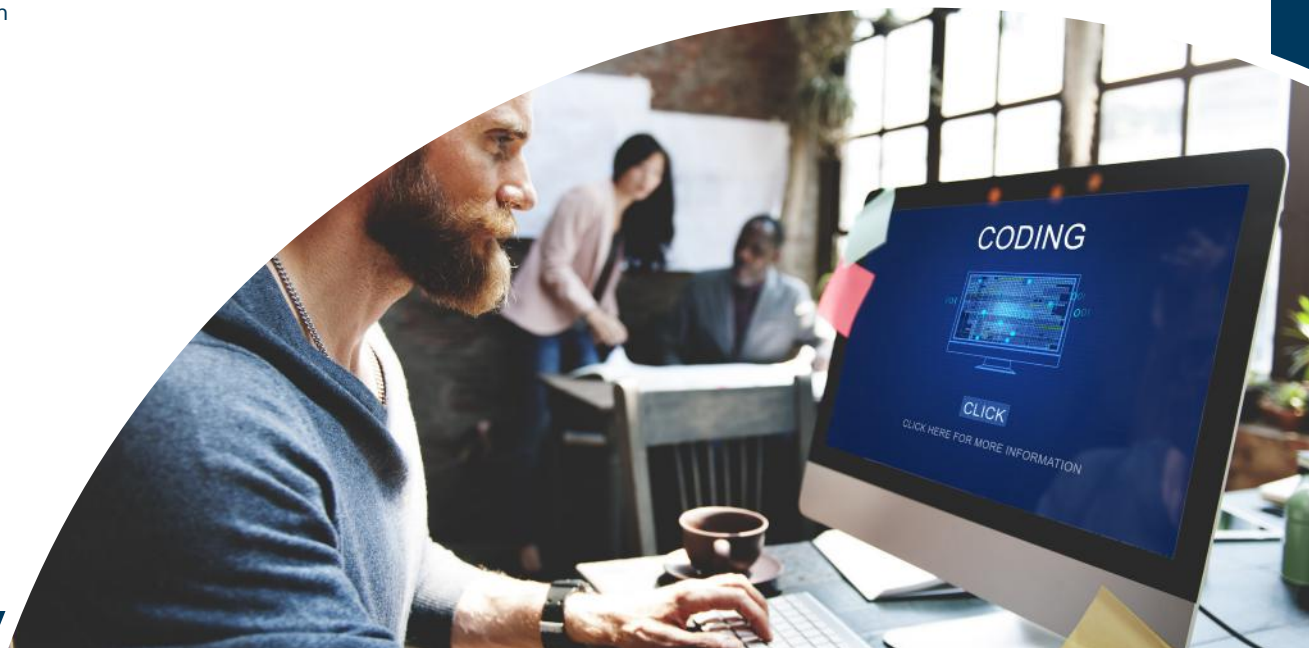
12 ZORG VOOR EEN BUSINESS CONTINUITY EN EEN INCIDENT HANDLING PLAN

BASISBESCHERMING

- **Zorg** voor een Incident Handling Plan om op incidenten te reageren
- **Zorg** voor een Business Continuity Plan om de continuïteit van het werk te vrijwaren
- **Alle werknemers** moeten het contactpunt kennen waar ze een incident moeten melden
- **Verspreid** en update de informatie over het contactpunt (interne en externe contacten, management en technische contacten …)
- **Rapporteer** alle incidenten aan het C-level

GEAVANCEERDE BESCHERMING

- **Evalueer** en test deze plannen jaarlijks
- **Evalueer** de opportuniteit van een verzekering tegen cybersecurity incidenten
- **Installeer** terugvalmogelijkheden voor nutsvoorzieningen (elektriciteit, telefoon, internet, …)



DISCLAIMER

DEZE GIDS EN DE BIJBEHORENDE DOCUMENTEN WERDEN OPGESTELD DOOR HET CENTRUM VOOR CYBERSECURITY BELGIË. ALLE TEKSTEN, LAY-OUT, ONTWERPEN EN ELEMENTEN VAN WELKE AARD OOK IN DEZE GIDS ZIJN AUTEURSRECHTELIJK BESCHERMD. UITTREKSELS UIT DEZE GIDS MOGEN ALLEEN VOOR NIET-COMMERCIËLE DOELEINDEN WORDEN GEPUBLICEERD OP VOORWAARDE DAT DE BRON WORDT VERMELD. HET CENTRUM VOOR CYBERSECURITY BELGIË WIJST ALLE AANSPRAKELIJKHEID VOOR DE INHOUD VAN DEZE GIDS AF.

De geleverde informatie :

- Is uitsluitend van algemene aard en is niet gericht op de specifieke situatie van een particulier of rechtspersoon.
- Is niet noodzakelijk volledig, nauwkeurig of up-to-date.
- Vormt geen professioneel of juridisch advies.
- Is geen vervanging voor deskundig advies.
- Biedt geen garantie voor een veilige bescherming.

SPONSORS

KBC

BNP PARIBAS FORTIS

VBO Verbond van Belgische Ondernemingen | FEB Fédération des Entreprises de Belgique

Deloitte.

Solvay Brussels School Economics & Management

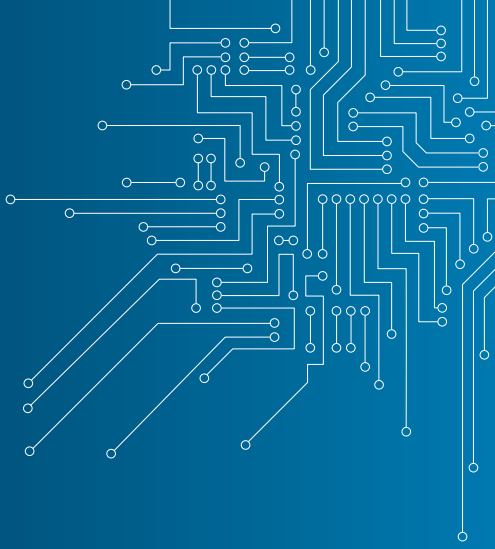
proximus

ICT CONTROL
Your Trusted Advisor

CYBER SECURITY COALITION.be

CENTRE FOR
CYBER SECURITY
BELGIUM

CYBER SECURITY
COALITION.be



HET CENTRUM VOOR
CYBERSECURITY BELGIË
Wetstraat, 16 - 1000 Brussel

T. : +32 2 501 05 63
info@ccb.belgium.be
www.ccb.belgium.be

.be