# Checklist voor cyberrisico's

## Controleer met de Cyberchecklist uw ICT-beveiliging

### 1. Afhankelijkheid IT-leverancier

☐ **Afspraken met uw leveranciers**
Als u uw IT heeft uitbesteed, maak dan afspraken met uw leveranciers over informatiebeveiliging en privacy. Bijvoorbeeld een verwerkersovereenkomst.

☐ **Communicatie bij problemen**
Zorg dat u met uw leverancier afspraken heeft vastgelegd (in een SLA) over communicatie bij problemen. Zo voorkomt u onduidelijkheid en tijdverlies bij een cyberincident.

☐ **Afspraken over incident response**
Maak goede afspraken met uw IT leverancier over wat te doen bij een cyberincident. Leg dit vast in een contract of SLA. Zo weet u precies wie wat moet doen.

☐ **Communicatieplan**
Maak een communicatie doe-lijst of plan. Zo weet u direct wie u moet bellen en hoe u deze partijen kunt bereiken als er een cyberincident plaatsvindt. En voorkomt u kostbaar tijdsverlies.

### 2. Ransomware

☐ **Goed ingericht patch-management**
U heeft uw patch management goed ingericht. Een patch is een stukje software om fouten op te lossen of updates te doen. Patch management is het proces en de tools om software updates te krijgen, te testen en te installeren op uw computersystemen.

☐ **Update Anti Virus automatisch**
Zorg dat 'automatisch updaten' van uw anti-virus programma's altijd aan staat. Zo bent u steeds voorzien van de laatste scanlijsten van uw leverancier en kan hij bij een nieuwe dreiging, direct updates doorvoeren.

☐ **Update firewall en intrusion prevention en detection automatisch**
Zet 'automatisch updaten' van firewall software en systemen die het binnendringen van uw netwerk monitoren en voorkomen aan. Zo weet u zeker dat op uw systemen de laatste inzichten, kennis en oplossingen verwerkt zijn.



Ga verder op de volgende pagina ›

27763 19.10

## 2. Ransomware (vervolg)

- [ ] **Back-up en recovery**
  Zorg voor een back-up en hersteloplossing die regelmatig uw belangrijkste data veilig opslaat. Bewaar deze back-ups op een aparte locatie die niet aan het internet is gekoppeld. Dus niet op uw netwerk of productiesystemen.

- [ ] **Netwerksegmentatie**
  Deel uw netwerk op in segmenten die niet of op een veilige manier met elkaar zijn verbonden. Hierdoor maakt u de toegang tot kwetsbare onderdelen van uw netwerk klein en zijn de gevolgen minder groot als er toch een cyberincident plaatsvindt.

- [ ] **Altijd bereikbaar**
  Zorg dat u op een andere manier bereikbaar bent als uw systemen niet meer beschikbaar zijn. Dat kan bijvoorbeeld via een andere website of telefoon.

- [ ] **Afspraken met IT-leverancier of een breach response dienstverlener**
  Een goede IT-leverancier of een specialistische breach response dienstverlener (datalek hulpdienst) kan u helpen bij een ransomware aanval. Maak alvast afspraken over: wat doen, wat niet doen en welk noodnummer u kunt bellen bij een incident.

- [ ] **Detectiemechanismen**
  Plaats IDS (een geautomatiseerd systeem dat hackpogingen en andere aanvallen in uw netwerk herkent) in uw netwerk. Hiermee voorkomt u een verdere verspreiding van ransomware. Dat scheelt tijd en geld bij het oplossen van ransomware.

- [ ] **Bekende unlock-codes**
  Kijk bij een infectie met ransomware eerst op nomoreransom.org/nl/. Daar worden bekende unlock-codes gedeeld. Probeer uit of deze unlock-codes werken in uw situatie.

## 3. DDoS-aanval

- [ ] **Gewenste beschikbaarheid**
  Bepaal de gewenste beschikbaarheid van uw website of uw aan internet gekoppelde systemen. Weet welke maatregelen u moet nemen wanneer uw website en systemen niet beschikbaar zijn.

- [ ] **Business continuity plan**
  Zorg voor een operationeel plan waarin u beschrijft wat te doen bij een cyberincident. Hoe u bij uw systemen en netwerk komt.

- [ ] **Afspraken met uw leveranciers van hosting**
  Maak duidelijke afspraken met uw leveranciers over hosting van uw website: over beschikbaarheid, het maken en beheren van back-ups en anti-DDoS-maatregelen.

## 4. Zwakheden in soft- of hardware

- [ ] **Goed ingericht patch-management**
  U heeft uw patch management goed ingericht. Een patch is een stukje software om fouten op te lossen of updates te doen. Patch management is het proces en de tools om software updates te krijgen, te testen en te installeren op uw computersystemen.

- [ ] **Update AV automatisch**
  Zet 'automatisch updaten' van uw anti-virus programma's altijd aan. Zo heeft u steeds de laatste scanlijsten van uw leverancier en kan hij bij een nieuwe dreiging, direct updates doorvoeren.

- [ ] **Gebruik intrusion prevention en detection mechanismen**
  Gebruik zogenaamde 'intrusion prevention' en 'detection' systemen. Hiermee voorkomt u dat hackers binnendringen in uw netwerk en computersystemen. Ook merken deze systemen een poging tot inbraak op.

- [ ] **Update firewall en intrusion prevention en detection automatisch**
  Zet 'automatisch updaten' van firewall software en systemen die het binnendringen van uw netwerk monitoren en voorkomen aan. Zo weet u zeker dat uw op systemen de laatste inzichten, kennis en oplossingen verwerkt zijn.

- [ ] **Regelmatig securitytesten**
  U controleert regelmatig uw netwerk en computersystemen door te testen of ze gehackt kunnen worden. Hiervoor zetten gespecialiseerde bedrijven zogenaamde 'pentesters' en 'redteams' in: dit zijn ethische hackers die zwaktes in uw netwerk proberen te vinden

- [ ] **Pas netwerksegmentatie toe**
  Deel uw netwerk op in segmenten die niet of veilig met elkaar zijn verbonden. Hierdoor beperkt u de toegang tot kwetsbare onderdelen van uw netwerk. Hiermee voorkomt u dat iemand die in een deel van uw netwerk inbreekt, toegang krijgt tot het hele netwerk

- [ ] **Detectiemechanismen in uw netwerk**
  Plaats 'detectie software' in uw netwerk en voorkom verdere verspreiding van de ransomware.
  Dat scheelt tijd en geld bij het oplossen van ransomware.

## 5. Awareness van medewerkers

- [ ] **Wachtwoordbeleid**
  Dit is een plan voor uw medewerkers waarin beschreven staat wat sterke wachtwoorden zijn en hoe men ze veilig gebruikt. Leg daarin ook uit waarom men nooit wachtwoorden mag delen met anderen en hoe men het veilig opslaat.

- [ ] **Gebruik 2 factor authenticatie**
  Gebruik een '2-factor authenticatie'. Dit is een manier van inloggen waar u naast login en wachtwoord, ook gebruik maakt van een code aangemaakt op een ander apparaat. Zoals een app op een smartphone of via sms naar een vooraf gekozen telefoonnummer.

## 5. Awareness van medewerkers (vervolg)

- [ ] **Phishing herkennen**
  Bij phishing worden uw medewerkers verleid om op 'kwaadaardige' links in e-mails te klikken.
  Door training kunt u uw medewerkers leren om phishing e-mails te herkennen. En er alert op te zijn.

- [ ] **Zorg voor een goed accesscontrol programma**
  U heeft een accesscontrol (toegangscontrole) programma. Hierdoor krijgen alleen die gebruikers toegang tot dat deel van het netwerk of tot bepaalde software die daar nodig zijn om hun werk goed te kunnen doen.

- [ ] **Functiescheiding bij gevoelige processtappen**
  U past functiescheiding toe. U verdeelt de verschillende taken en verantwoordelijkheden binnen een taak / opdracht / proces over verschillende personen. Het is duidelijk wat er gebeurt en iedereen doet mee. En zo voorkomt u fouten en fraude.

- [ ] **Detectiemechanismen in uw netwerk**
  Plaats 'detectie software' op uw netwerk en voorkom verdere verspreiding. Dat scheelt tijd en geld bij het oplossen van het cyberincident.

## 6. Malware voorkomen

- [ ] **Goed ingericht patch-management**
  U heeft uw patch management goed ingericht. Een patch is een stukje software om fouten op te lossen of updates te doen. Patch management is het proces en de tools om software updates te krijgen, te testen en te installeren op uw computersystemen.

- [ ] **Update Anti Virus automatisch**
  U heeft 'automatisch updaten' van uw anti-virus programma's aanstaan. Zo heeft u altijd de laatste scanlijsten van uw leverancier. Bij een eventuele nieuwe dreiging kan hij deze opdates direct doorvoeren.

- [ ] **Intrusion prevention en detection mechanismen**
  Gebruik zogenaamde 'intrusion prevention' en 'detection' systemen. Hiermee voorkomt u dat hackers binnendringen in uw netwerk en computersystemen. Ook merken deze systemen een poging tot inbraak op.

- [ ] **Update firewall en intrusion prevention en detection automatisch**
  Zet 'automatisch updaten' van firewall software en systemen die het binnendringen van uw netwerk monitoren en voorkomen aan. Zo weet u zeker dat u op uw op systemen de laatste inzichten, kennis en oplossingen verwerkt heeft.

- [ ] **Pas netwerksegmentatie toe**
  Pas netwerksegmentatie toe. Hiermee voorkomt u dat iemand die in een deel van uw netwerk inbreekt, toegang krijgt tot het hele netwerk.

## 6. Malware voorkomen (vervolg)

- [ ] **Implementeer detectiemechanismen in uw netwerk**
  Plaats detectiemechanismen in uw netwerk waarmee u een verdere verspreiding van malware kunt voorkomen. Dat scheelt tijd en geld bij het oplossen van malware.

- [ ] **Social engineering herkennen**
  Train uw medewerkers om pogingen tot social engineering te herkennen. Deze manier van criminaliteit heeft als doel om medewerkers handelingen te laten doen die niet in het belang van uw bedrijf zijn.

## 7. Misbruik van website voorkomen

- [ ] **Afspraken over beveiliging van uw website**
  Maak vooraf goede afspraken over veiligheidsmaatregelen met het bedrijf dat uw website bouwt en host. Zowel bij ontwikkeling als tijdens de productie.

- [ ] **Gebruik Secure Software Development Life Cycle bij software en website**
  Gebruik de Secure Software Development Lifecycle. Hiermee ontwerpt en bouwt u vanaf de start op een veilige manier aan software en websites. Zo bouwt u aan een veilig eindproduct.

- [ ] **Zorg voor een responsible disclosure procedure**
  Er is een lek gevonden in software of een website. Bij ‘responsible disclosure’ meldt de ontdekker van het lek direct aan de software-ontwikkelaar wat hij/zij gevonden heeft. Zo heeft de producent tijd om het lek te dichten en gebruikers te informeren.

- [ ] **Loggen gebruikersactiviteiten webapplicatie**
  Omdat u alle activiteiten van gebruikers in uw webapplicaties vastlegt en analyseert, ziet u ook mogelijke afwijkingen. En kunt u hier tijdig op reageren.

- [ ] **Web application firewall**
  Een web application firewall houdt het verkeer van en naar uw webapplicatie bijvoorbeeld een website in de gaten. Deze firewall geeft een signaal en grijpt in als het afwijkt van normaal.

## 8. Zwakheden in de website

- [ ] **Beveiliging website**
  De leverancier van uw website (bouwen en hosten) moet de juiste maatregelen nemen om u zekerheid te geven over de veiligheid van uw website. Zowel bij ontwikkeling als tijdens de productie. Maak hier vooraf afspraken over.

- [ ] **Secure Software Development Life Cycle**
  Gebruik de Secure Software Development Lifecycle. Hiermee ontwerpt en bouwt u vanaf de start op een veilige manier aan software en websites. Zo bouwt u aan een veilig eindproduct.

## 8. Zwakheden in de website (vervolg)

- [ ] **Zorg voor een responsible disclosure procedure**
  Er is een lek gevonden in software. Bij 'responsible disclosure' meldt de ontdekker van het lek direct aan de software-ontwikkelaar wat hij/zij gevonden heeft. Zo heeft de producent tijd om het lek te dichten en gebruikers te informeren.

- [ ] **Loggen gebruikersactiviteiten**
  U legt alle activiteiten van gebruikers in uw webapplicaties vast. Zo merkt u direct mogelijke afwijkingen op en kunt u tijdig reageren.

- [ ] **Web application firewall**
  Een web application firewall houdt het verkeer van en naar uw webapplicatie bijvoorbeeld een website in de gaten. Deze firewall geeft een signaal en grijpt in als het afwijkt van normaal.

- [ ] **Goed ingericht patch-management**
  U heeft uw patch management goed ingericht. Een patch is een stukje software om fouten op te lossen of updates te doen. Patch management is het proces en de tools om software updates te krijgen, te testen en te installeren op uw computersystemen.

- [ ] **Automatisch updaten Anti Virus software**
  Zet het automatisch updaten van uw anti-virus programma's altijd aan. Zo heeft u altijd de laatste scanlijsten van uw leverancier. Bij een mogelijke nieuwe dreiging kan de leverancier direct updates doorvoeren.

- [ ] **Intrusion prevention en detection mechanismen**
  Gebruik zogenaamde intrusion prevention en detection systemen. Hiermee voorkomt u dat hackers binnendringen in uw netwerk en computersystemen. Ook ziet dit programma pogingen tot inbraak.

- [ ] **Automatisch updaten firewall en intrusion prevention en detection**
  'Automatisch updaten' van firewall software en systemen die het binnendringen van uw netwerk monitoren en voorkomen staat altijd aan. Zo zijn uw systemen voorzien van de laatste inzichten in bekende zwakheden en de oplossingen die uw leverancier heeft ontwikkeld.

- [ ] **Netwerksegmentatie**
  U past netwerksegmentatie toe. Hiermee voorkomt u dat iemand die in een deel van uw netwerk inbreekt, toegang krijgt tot het hele netwerk.

- [ ] **U heeft een detectieprogramma**
  Plaats detectiemechanismen in uw netwerk waarmee u een verdere verspreiding kunt voorkomen. Dat scheelt tijd en geld bij het oplossen van ransomware.

## 9. Fysieke toegang tot IT en data

- [ ] **Beperk en controleer fysieke toegang tot uw IT-omgeving**
  Zorg dat alleen bevoegde medewerkers bij het netwerk en de computersystemen kunnen komen. Hiermee voorkomt u dat mensen die kwaad willen apparatuur kunnen gebruiken, beschadigen of misbruiken.

- [ ] **Vergrendel computers als ze niet gebruikt worden**
  Elke medewerker vergrendelt zijn computer als hij van zijn werkplek loopt of aan het einde van de werkdag. Zo voorkomt u dat kwaadwillenden de computer kunnen gebruiken.

- [ ] **Gebruik een kabelslot of kluis als een computer onbeheerd achterblijft**
  Zet een computer vast met een kabel of berg hem op in een kluis als u weg gaat.

- [ ] **Stop data dragers in een kluis**
  Losse data dragers (usb-sticks, usb-schijven, cd-roms, backup tapes etc) bergt u op in een kluis om ze uit handen van kwaadwillenden te houden. Zo voorkomt u ook dat ze besmet raken bij een incident met bijvoorbeeld malware of ransomware.

- [ ] **Encryptie op harde schijven en andere data dragers**
  U heeft encryptie ingeschakeld op al uw harde schijven van computers, laptops en mobiele devices. Zo kan een hacker of iemand die kwaad wil niet bij de gegevens op deze schijven.

- [ ] **Gebruik 2 factor authenticatie**
  Gebruik een '2-factor authenticatie'. Dit is een manier van inloggen waar u naast login en wachtwoord, ook gebruik maakt van een code aangemaakt op een ander apparaat. Zoals een app op een smartphone of via sms naar een vooraf gekozen telefonnummer.

- [ ] **Zorg voor een gedegen en actueel wachtwoordbeleid**
  U heeft een beleid opgesteld dat medewerkers wijst op het aanmaken van sterke wachtwoorden en veilig gebruik hiervan. Hierin staat ook cultuur omschreven: deel nooit wachtwoorden onderling en sla ze veilig op.

- [ ] **Pas netwerksegmentatie toe**
  Pas netwerksegmentatie toe. Hiermee voorkomt u dat iemand die in een deel van uw netwerk inbreekt, toegang krijgt tot het hele netwerk.

## 10. Onderweg gebruik van internet

- [ ] **Gebruik VPN bij het internetten**
  U gebruikt een VPN (virtual Private Network)verbinding. Hierdoor is uw internetverbinding beveiligd en kan niet worden afgeluisterd.

- [ ] **Segmenteer jouw deel van het netwerk**
  Scheidt het netwerk waarop mobiele gebruikers toegang hebben van de rest van uw netwerk. Koppel het los van elkaar.

## 10. Onderweg gebruik van internet (vervolg)

- [ ] **Pas access control maatregelen toe op uw devices binnen dit netwerk**
  U gebruikt de juiste accesscontrol software. Hierdoor krijgen alleen die gebruikers toegang tot dat deel van het netwerk of tot bepaalde software die daar nodig zijn om hun werk goed te kunnen doen.

- [ ] **4G**
  Open of free Wifi is vaak onbeveiligd en gemakkelijk te hacken. Een 4G-verbinding is veilig. Kies altijd voor 4G als dit mogelijk is. Is 4G niet aanwezig, gebruik dan een VPN verbinding.

## 11. Afhankelijkheid 4G onderweg

- [ ] **Goed ingericht patch-management**
  U heeft uw patch management goed ingericht. Een Patch is een stukje software om fouten op te lossen of updates te doen. Patch management is het proces en de tools om software updates te krijgen, te testen en te installeren op uw computersystemen.

- [ ] **Update AV automatisch**
  Zet het automatisch updaten van uw anti-virus programma's altijd aan. Zo heeft u altijd de laatste scanlijsten van uw leverancier. Bij een mogelijke nieuwe dreiging kan de leverancier direct updates doorvoeren.

- [ ] **Alternatief of backup apparaat**
  Als u afhankelijk bent van het gebruik van mobiele apparaten, houdt dan een apparaat achter de hand. Zo kunt u altijd doorwerken als uw apparaat niet meer werkt door een hack of ander incident.

## 12. Datalek na delen klantgegevens

- [ ] **Training en bewustzijn bij medewerkers**
  Uw medewerkers begrijpen dat zij datalekken of het vermoeden daarvan altijd moeten melden.
  Het is voor uw medewerkers duidelijk waar ze een datalek moeten melden.

- [ ] **Intern meldpunt datalekken**
  Er moet een intern meldpunt zijn voor datalekken dat bekend is bij alle medewerkers en 24/7 beschikbaar is.

- [ ] **Datalek response proces**
  Bij een datalek neemt u zo snel mogelijk de noodzakelijke maatregelen. Beschrijf deze maatregelen in een plan dat u deelt met al uw medewerkers. Het is belangrijk om uw medewerkers hierop te trainen zodat ze weten wat ze moeten doen bij een datalek.

- [ ] **Harddisk versleuteling**
  U heeft encryptie ingeschakeld op al uw harde schijven van computers, laptops en mobiele devices.
  Zo kan een hacker of iemand die kwaad wil niet bij de gegevens op deze schijven omdat ze zijn versleuteld.

## 12. Datalek na delen klantgegevens (vervolg)

- [ ] **Versleutel gegevens op USB sticks en andere externe opslagmedia**
  U heeft encryptie ingeschakeld op al uw harde schijven van computers, laptops en mobiele devices. Zo kan een hacker of iemand die kwaad wil niet bij de gegevens op deze schijven.

- [ ] **Dataclassificatie**
  Pas dataclassificatie toe. Hiermee kunt u verschillende niveaus van beveiliging meegeven aan data en informatie. U geeft bijvoorbeeld zware beveiliging aan klantgegevens of patenten.

- [ ] **Data leakage prevention**
  Met 'data leakage prevention software' controleert u de activiteit en toegangsregels rondom uw data. Zo verkleint u de kans op een datalek.

## 13. Bedrijfsautomatisering

- [ ] **Internetverbinding gebruiken**
  Een internetverbinding is altijd een zwak punt in een netwerk of computersysteem. Hoe goed u hem ook beveiligd. Gebruik dan ook alleen een internetverbinding als het echt nodig is.

- [ ] **Connectie met internet alleen als het noodzakelijk is**
  Zorg dat een internetverbinding alleen actief is als het nodig is. Schakel de verbinding daarna direct uit.

- [ ] **Access control software**
  U gebruikt de juiste accesscontrol software. Hierdoor krijgen alleen die gebruikers toegang tot dat deel van het netwerk of tot bepaalde software die daar nodig zijn om hun werk goed te kunnen doen.

- [ ] **Gebruik 2 factor authenticatie**
  Gebruik een '2-factor authenticatie'. Dit is een manier van inloggen waar u naast login en wachtwoord, ook gebruik maakt van een code aangemaakt op een ander apparaat. Zoals een app op een smartphone of via sms naar een vooraf gekozen telefonnummer.

# Goed om te weten

## Bij Centraal Beheer staan we al meer dan 100 jaar klaar voor onze klanten. U kent ons vast van ‘Even Apeldoorn bellen’.

### U kunt bij ons financiële producten en diensten afsluiten

Zoals verzekeringen, pensioenen, hypotheken, spaarrekeningen, beleggingsproducten en diensten voor HR en Risicomanagement. Rechtstreeks en via adviseurs die met ons samenwerken.

### Vanaf 1995 horen wij bij Achmea

Centraal Beheer is een handelsnaam van Achmea Services N.V., statutair gevestigd in Zeist. Ons bezoekadres is Handelsweg 2, 3707 NH Zeist. Ons nummer van de Kamer van Koophandel is 34136016. Achmea Services N.V. behoort tot de Achmea Groep.

### Uw gegevens in vertrouwde handen

Sluit u een verzekering of financiële dienst af? Dan hebben wij uw gegevens nodig. Denk aan uw naam, adres en woonplaats, e-mailadres, telefoonnummer en bankrekeningnummer. Soms hebben wij ook meer gegevens van u nodig. Achmea B.V.  is verantwoordelijk voor een goede verwerking van uw persoonsgegevens.

### Wilt u weten welke gegevens wij verwerken en waarvoor?

Kijk dan in ons Privacy Statement op centraalbeheer.nl/privacy. Daar leest u ook wat uw rechten zijn. En wanneer u bezwaar kunt maken tegen verwerking van uw gegevens. Wilt u ons Privacy Statement op papier ontvangen? Stuur dan een brief naar:
Centraal Beheer Relatiebeheer
Postbus 9150
7300 HZ Apeldoorn

### Staan er fouten in dit formulier?

Ons doel is dat al onze informatie klopt en volledig is. En dat u alles zo goed mogelijk begrijpt. Maar er kan altijd ergens een fout staan. Wij zijn niet aansprakelijk voor eventuele gevolgen van die fout.

### Staat er iets anders in de productvoorwaarden?

Uw en onze rechten en plichten staan in de productvoorwaarden. Staat in dit formulier wat anders dan in de productvoorwaarden? Dan gelden de productvoorwaarden.

### Bent u niet tevreden? Laat het ons weten.

Bent u het niet met ons eens of heeft u een klacht? Dan horen wij dit graag. We willen u namelijk zo goed mogelijk helpen. Kijk voor meer informatie en ons klachtenformulier op centraalbeheer.nl/klachtdoorgeven. U kunt ook een brief sturen naar:
Centraal Beheer Klachtenbureau
Postbus 9150
7300 HZ Apeldoorn

### Meer informatie over Centraal Beheer

Kijk voor meer informatie over ons en ons beleid, onze producten en onze gegevens op centraalbeheer.nl.

Het adres van Centraal Beheer is:
Laan van Malkenschoten 20
7333 NP Apeldoorn