CYBER Fundamentals

Preview Cyber Fundamentals self-assessment Niveau 1 & 2

Hoe cyberweerbaar is uw bedrijf?

Dat gaat u nu ontdekken! Deze ‘Preview op het self-assessment’ geeft u inzicht in waar u staat en voor welk certificaat u in aanmerking komt, maar biedt tegelijkertijd ook de handvatten om te werken aan een verbeterstrategie. Zo biedt Cyber Fundamentals een haalbare, schaalbare en betaalbare manier om grip te krijgen op uw informatiebeveiliging en maken we u als ondernemer weerbaarder tegen cybercriminaliteit en de bijbehorende bedrijfsrisico’s.

Hoe werkt het?

Stap 1: In dit document vindt u 35 vragen over de huidige cybermaatregelen van uw onderneming. Elke vraag die u kun beantwoorden met ‘Ja’ levert één punt op. Tel na het afronden van de vragenlijst alle punten bij elkaar op. Bekijk vervolgens voor elk certificaatniveau u in aanmerking komt.

Certificaat | Niveau 1

Heeft u 16 punten of meer verdient? Dan kunt u via onze website de officiële aanvraag voor het Cyber Fundamentals Certificaat Niveau 1 indienen. Met dit certificaat bent u op de goede weg naar een goede basis voor uw informatiebeveiliging. U heeft inzicht in waar u staat en een heldere verbeterstrategie op weg naar Niveau 2.

Certificaat | Niveau 2

Heeft u 32 punten of meer? Dan kunt u een aanvraag indienen voor Niveau 2. Met dit certificaat kunt u aan uw partners, klanten en leveranciers aantonen dat u voldoet aan de 8 basismaatregelen van het Nationaal Cyber Security Centrum (NCSC), de 5 basisprincipes van het Digital Trust Center (DTC) en hun informatie bij u in veilige handen is.

Certificaat | Niveau 3 & Niveau 4

De certificaten voor niveau 3 en 4 zijn nog in ontwikkeling. Hiervoor werkt Cyber Fundamentals samen met grote werkgevers en brancheorganisaties, de overheid, zzp’ers en mkb’ers, waarvoor ISO27001 de stip op de horizon is. Behaald u bij ons niveau 4? Dan bent u zo goed als klaar om op te gaan voor het ISO27001 certificaat.

Stap 2: Maak een account aan
Kunt u voldoende vragen met ‘ja’ beantwoorden en komt u in aanmerking voor een certificaat? Maak dan een account aan op de website en bevestig uw certificaataanvraag met een betaling.

Stap 3: Start certificeringsproces Eigen Verklaring Cyberweerbaarheid
Dien uw officiële aanvraag in door de digitaal vragen te beantwoorden in uw accountomgeving. U hoeft de vragenlijst niet in één keer in te vullen. Pauzeren is mogelijk. U krijgt direct een score te zien bij het afronden van de vragenlijst. Deze score correspondeert met één van de certificaatniveaus.

Stap 4: Toekenning certificaat Eigen Verklaring Cyberweerbaarheid
U ontvangt een certificaat passend bij het door u behaalde niveau en een digitaal keurmerk die u bijvoorbeeld op uw website kunt plaatsen.

Stap 5: Verlenging
Ongeveer 6-8 weken voordat uw certificaat verloopt ontvangt u van ons een melding dat uw certificaat gaat verlopen. U kunt verlengen door het certificaat voor het komende jaar te betalen en de vragenlijst opnieuw in te vullen.

Heeft u nog vragen?

Neem gerust contact op met onze helpdesk via info@cyberfundamentals.nl of 085 004 6455.

Deel I - Installeer updates

1.1 Heeft u alle software, systemen, webbrowsers in kaart gebracht? Ja / Nee

Om tijdig updates te kunnen uitvoeren, moet u geïnventariseerd hebben wat u heeft en waar u verantwoordelijk voor bent op ICT-gebied. Maak een inventarisatie van de softwareversies die u gebruikt, zowel in de cloud als lokaal geïnstalleerd. Denk daarbij aan: kantoor software, administratie en planning software, personeelssystemen, productie software en besturingssystemen (Windows, macOS, Linux etc..).

Voor industriële bedrijven is het naast de kantoorautomatisering (KA) ook belangrijk om de productiesystemen in de procesautomatisering (PA) in kaart te brengen. Inventariseer ook welke hardware u gebruikt. Denk daarbij aan laptop, pc's, netwerkcomponenten (servers, VM, switches, routers, firewalls), databases en websites, telefonie en alarmsystemen).

1.2 Heeft u een werkwijze voor alle systemen, zodat u tijdig op de hoogte bent van benodigde updates? Ja / Nee

Als u alle software, systemen en webbrowsers in kaart heeft gebracht, dient u vervolgens een werkwijze te formuleren waardoor u altijd op tijd op de hoogte bent van toekomstige updates. Updates dienen zich aan in verschillende vormen. De meest bekende zijn de automatische updates van Windows en macOS. Dat uw laptop of pc en andere bedrijfsmiddelen en apparatuur automatisch worden geüpdatet, dient u overigens wel vooraf juist te configureren. De leverancier stuurt u vervolgens automatisch een update welke u zelf dient te installeren.

Naast automatische updates zijn er ook veel leveranciers die op hun website, service portal of newsfeed een melding geven over een update. Het is dus belangrijk ook deze regelmatig te controleren. Soms zijn er ook forums of gebruikersgroepen die wereldwijde gebruikers erop wijzen dat er een update beschikbaar is. Inventariseer daarom welke leveranciers de updates voor u verzorgen en bij welke u zelf het initiatief moet nemen.

1.3 Installeert u updates tijdig? Ja / Nee

Heeft u een heldere werkwijze die zeker stelt dat uw organisatie de beschikbare updates tijdig installeert? Wie is waarvoor verantwoordelijk en binnen welke termijn moeten de updates zijn geïnstalleerd? Wat zijn de regels bij reguliere- en zeer urgente updates? Het is sterk aan te raden om maandelijks de updates bij te houden van alle operationele systemen en software. Microsoft hanteert voor haar producten kwaliteits- en functie updates. Hanteer voor uzelf een standaard dag en tijdstip om alle beschikbare updates te installeren.

1.4 Bewaakt u of uw ICT-dienstverlener dat alle updates (automatisch of handmatig) tijdig zijn geïnstalleerd? Ja / Nee

Inventariseer waar automatische updates wel of niet zijn ingeschakeld. Het kan zo zijn dat updates wel worden gemeld, maar dat de medewerkers of de afdeling ICT en de ICT-dienstverlener updates niet installeren en 'wegklikken'. Zorg dat dit goed is geconfigureerd en er heldere afspraken over zijn gemaakt. Ook met de externe ICT-dienstverlener moet u

afspraken maken over het tijdig installeren van de updates. Zorg ervoor dat zij u hierover informeren, zodat u te allen tijde weet dat alles op orde is. Zorg dat er een controlemechanisme is ingebouwd, zodat u altijd inzichtelijk heeft of overal alle updates zijn geïnstalleerd. Dit kan handmatig worden beoordeeld, maar ook slimme software kan u hierbij helpen.

1.5 Indien bij een bekende kwetsbaarheid uw leverancier nog geen update heeft, heeft u hiervoor een interne procedure? Wat doet u dan?

Ja / Nee

Het kan voorkomen dat u in het nieuws, op een forum of gebruikersgroep informatie krijgt dat de software of hardware die u gebruikt een kwetsbaarheid heeft. Wat is dan de procedure? Hoe handelt u? Wie overlegt met wie? En welke noodacties kunt u uitvoeren? Zorg dat dit vooraf helder is. Heeft u nagedacht om hierover ook afspraken te maken met uw leveranciers? In de meeste gevallen komt er slechts een 'quick-fix'. Zorg ervoor dat er altijd een 'roll-back' scenario is, zodat u altijd terug kunt vallen op een vorige versie indien de update nog meer problemen geeft.

1.6 Indien een softwareleverancier geen beveiligingsupdates meer levert, staat er in uw beleid omschreven dat deze wordt vervangen?

Ja / Nee

Het komt vaak voor dat oudere software en systemen niet meer door de leverancier worden ondersteund. Dit betekent dat er geen updates meer uitkomen, waarin mogelijk nieuwe cyber kwetsbaarheden worden opgelost. Heeft u helder welke applicaties of systemen dat zijn en wat is hierin uw beleid? Heeft u inzichtelijk welke risico's u hierbij loopt en welke maatregelen hierop worden genomen? Een mogelijk risico kunt u uiteraard ook altijd accepteren. U schat dan zelf de kans in en de mogelijke impact op uw organisatie en ICT-systemen.

Waarom moet u hier iets mee? Veel organisaties zien het risico niet. Een oude hamer is nog steeds een werkende hamer, die wordt niet opeens gevaarlijker. Bij software kan het risico echter wel toenemen.

Deel II - Zorg dat elke applicatie en elk systeem voldoende loginformatie genereert

2.1 Heeft u inzichtelijk of al uw essentiële systemen en applicaties loginformatie genereert?

Ja / Nee

Wat zijn de belangrijkste software, applicaties en systemen die worden gebruikt door uw organisatie? Maken deze gebruik van een logboekbestand waarin meldingen over het gebruik van computers en diensten worden bewaard? In een logfile worden alle acties vastgelegd. Welke acties zijn er uitgevoerd? Door wie en op welk tijdstip?

2.2 Geven de logfiles duidelijke informatie?

Ja / Nee

De logfiles moeten leesbaar zijn en helderheid geven over de acties die hebben plaatsgevonden. Heeft u inzichtelijk of de logfiles leesbaar en begrijpelijk zijn en alle informatie geven?

2.3 Worden auditlogboeken periodiek beoordeeld om afwijkingen of abnormale gebeurtenissen te detecteren die kunnen wijzen op een potentiële bedreiging?

Ja / Nee

Heeft u afspraken gemaakt over de frequentie van de beoordeling van logfiles, door wie het wordt beoordeeld en op basis van welke criteria dit gebeurd? Dit kan ook door het gebruik van geautomatiseerde tooling. Het verzamelen en analyseren van logs is van cruciaal belang voor het vermogen van een onderneming om kwaadaardige activiteiten snel te detecteren. Soms zijn logs het enige bewijs van een succesvolle aanval. Aanvallers weten dat veel bedrijven logs bijhouden voor nalevingsdoeleinden, maar deze zelden analyseren.

2.4 Zijn de logbestanden in een leesbaar en bruikbaar bestand opgeslagen?

Ja / Nee

Mocht u gehackt worden, dan is het belangrijk dat de hacker zijn sporen niet kan wissen. Het is belangrijk om de logfiles dus te beschermen. Sommige applicaties en systemen maken logfiles die nooit aanpasbaar zijn, maar lang niet altijd. Zorg er daarom voor dat de configuratie zo is ingesteld dat logfiles beschermd zijn.

Ter info: in Office 365 zijn de logfiles niet aanpasbaar. Maar let op bij maatwerkapplicaties. Daar gaat het vaak mis. Het beschermen van logfiles is van cruciaal belang. Logs kunnen bijvoorbeeld laten zien wanneer en hoe de aanval plaatsvond, welke informatie is gebruikt en of gegevens zijn geëxporteerd. Het bewaren van logs is belangrijk als vervolgonderzoek nodig is. Bijvoorbeeld in geval van fraude.

2.5 Heeft u de toegang tot de logbestanden beperkt?

Ja / Nee

De toegang tot de logfiles moet zoveel mogelijk worden beperkt tot een kleine groep medewerkers. Hanteer hierbij een ‘need-to-know’ en ‘least privilege principe’. Geef dus alleen toegang aan medewerkers die het nodig hebben voor het uitvoeren van hun werkzaamheden. Dit om te voorkomen dat een medewerker (of een hacker) ongeautoriseerd in de gegevens kan kijken. Zorg ervoor dat de logfiles extra zijn beveiligd.

2.6 Weet u zeker dat de systeemtijden overal juist zijn?

Ja / Nee

Denk hierbij aan zomer- en wintertijden en internationale tijdzones. De geïnventariseerde systemen moeten de juiste tijden aangeven. Windows en macOS passen de zomer en wintertijden automatisch aan. Maar dat is niet standaard in alle software-applicaties of netwerksystemen. Als de tijd niet klopt (soms zelfs jaren, dagen en uren verschil met de realiteit) heeft u ook niet veel aan uw logfiles.

Deel III – Awareness en wachtwoorden

3.1 Heeft u en hebben uw medewerkers een 'awareness-training' gevolgd, zodat iedereen tijdig gevaren herkent? (m.b.t. malware, phishing, CEO fraude etc..)

Ja / Nee

Het is belangrijk om een goede bewustwordingstraining te volgen. Zo'n training is bedoeld is om bijvoorbeeld frauduleuze e-mail te leren herkennen. Wist u dat de meeste 'hacks' zijn begonnen met een malware e-mail? Medewerkers moeten hierin zijn getraind. Zorg ook voor goede onderlinge afstemming over waar malware of een phishing mail gemeld moet worden en hoe medewerkers zelf wel of juist niet moeten handelen.

Daarnaast moeten medewerkers goed weten hoe ze met wachtwoorden omgaan. Welk wachtwoord kies je? Wat moet je zeker niet doen? Ook moeten medewerkers bewust zijn dat ze niet zomaar een onbekende USB stick in de pc of laptop stoppen. Naast deze gevaren zijn er ook fysieke gevaren,. Denk aan onbevoegde personen die proberen uw bedrijfspand binnen te komen en in specifieke ruimtes te komen. Of dit werkelijk een risico is, is uiteraard afhankelijk van uw organisatie en de context.

3.2 Maken uw medewerkers gebruik van tweefactor authenticatie (2FA)?

Ja / Nee

2FA is gebaseerd op;

- iets wat u weet (gebruikersnaam & wachtwoord)
- met iets wat u heeft (een token, telefoon-code)
- of iets wat u bent (vingerafdruk).

Het is belangrijk dat u uw systemen extra beveiligd met 2FA en dan met name voor systemen die persoon- en bedrijfsgegevens verwerken. Hierdoor maakt u het een hacker een stuk lastiger. Alleen een gebruikersnaam en een wachtwoord is niet langer voldoende om u goed te beveiligen. Helaas gebruiken medewerkers vaak nog makkelijke wachtwoorden. Mede om die reden is een extra stap om in te loggen belangrijk voor een goede beveiliging. Dus naast het wachtwoord, moet iemand kunnen aantonen dat hij/zij het ook echt is. Met de toename van cloudapplicaties is er ook een verhoogd risico op gegevenslekken. 2FA is een van de beste veiligheidsmaatregelen om uw organisatie, gebruikers en gevoelige gegevens te beschermen.

3.3 Heeft u beleid of procedure hoe medewerkers dienen om te gaan met wachtwoorden?

Ja / Nee

U wilt voorkomen dat medewerkers hun wachtwoord ergens opschrijven, omdat ze het niet kunnen onthouden. Echter is een heel eenvoudig wachtwoord ook weer gemakkelijk te raden door een computer. Maak gebruik van een goede wachtwoordmanager. Deze helpt medewerkers om alle wachtwoorden op te slaan, waardoor ze slechts 'een enkel 'hoofdwachtwoord' hoeven te onthouden. Een wachtwoordmanager kan ook nieuwe complexe wachtwoorden genereren en onthouden. In de markt is een divers aanbod aan wachtwoordmanagers. Sommige kunt u op uw eigen server installeren, anderen werken 'in de cloud'.

Deel IV - Maak regelmatig back-ups van uw systemen en test deze

4.1 Heeft u bepaald van welke data back-ups noodzakelijk zijn?

Ja / Nee

Inventariseer van alle software-applicaties en systemen waar welke data is opgeslagen. Dit kan op een eigen laptop, pc of server zijn of in de cloud zijn. Bepaal vervolgens van welke data het noodzakelijk is om back-ups te hebben. Denk daarbij aan kritische bedrijfsinformatie (sales, operatie, HR, klantdossiers etc..)

Let op: Office 365 maakt geen back-up van uw gegevens. Dit dient u separaat en eigenhandig in te regelen.

4.2 Heeft u bepaald met welke frequentie back-ups worden gemaakt?

Ja / Nee

Bepaal van uw databestanden hoe vaak de bestanden in een back-up moeten worden opgenomen. Besef dat de frequentie van de back-up invloed heeft op de termijn dat u bestanden kwijt kunt raken. Voorbeeld: als u een maal per week een back-up maakt en uw bestanden worden beschadigd, dan verliest u alle gegevens en mutaties van de afgelopen week. Er zijn ook organisaties die iedere dag of nacht een back-up maken. Dan bent u dus van maximaal 1 dag uw gegevens kwijt. Hoe vaker u een back-up maakt, hoe lager het risico. Echter de kosten nemen wel toe, want u zult meer data moeten opslaan. U bewaard immers meestal een back-up over een bepaalde periode.

4.3 Heeft u bepaald hoe lang u de back-ups zult bewaren?

Ja / Nee

De periode dat u de back-up gaat bewaren is een belangrijke keuze. Deze is sterk afhankelijk van uw bedrijfssituatie. Sommige organisaties bewaren de back-ups 1 tot 3 maanden, anderen 1 jaar of zelfs wel 20 jaar (zoals bij gezondheidsgegevens). Let wel op dat de bewaartermijn in lijn is met de AVG-wetgeving en persoonlijke gegevens niet langer bewaard worden dan strikt noodzakelijk.

4.4 Heeft u een beleid of procedure voor hoe de back-ups worden getest?

Ja / Nee

Een back-up moet getest worden. Soms worden ze op een bepaalde formaat/manier opgeslagen en blijkt achteraf dat de back-up helemaal niet werkt of bruikbaar is. Test dus met een bepaalde regelmaat of de back-ups wel werken. Tip: Sommige back-up tools voorzien in het (technisch) testen van de back-up. Dan nog is het aan te raden om periodiek een back-up terug te zetten en functioneel te testen.

4.5 Maakt u gebruik van de 3-2-1 regel? (3 back-up versies van uw data, op 2 verschillende media, 1 op een fysiek andere locatie)

Ja / Nee

Deze regel geeft een goed uitgangspunt voor uw back-ups. Bewaar minimaal 3 versies van uw back-ups. Sla deze op, op 2 verschillende media (aparte externe harde schijf of separate

cloud opslag). Sla de back-up ook op op een andere locatie. Mocht er iets gebeuren op 1 locatie, dan heeft u op de andere locatie altijd nog een reserve kopie.

4.6 Is de toegang tot de back-ups beperkt?

Ja / Nee

De toegang tot de back-ups dient zoveel mogelijk te worden beperkt tot een kleine groep medewerkers. Hanteer hierbij een ‘need-to-know’ en ‘least privilege principe’. Geef dus alleen toegang aan medewerkers die het nodig hebben voor het uitvoeren van hun werkzaamheden. Weet u wie deze geautoriseerde personen zijn en zijn back-ups met een extra wachtwoord en 2FA goed beveiligd?

Deel V – Segmenteer netwerken

5.1 Heeft u uw (thuis of bedrijfs-) netwerk in meerdere zones ingedeeld?

Ja / Nee

Het is verstandig om het netwerk in te delen in verschillende zones. Zo kunt u voorkomen dat iemand (een gast/klant/externe) met een besmette laptop een ander apparaat kan besmetten. Maak daarom een apart netwerk aan voor gasten, maar doe dit ook voor alle apparaten die op het netwerk zijn aangesloten. Denk aan printers, tv's, beamers, zonwering, alarmsystemen etc. Netwerksegmentatie kan uw algehele beveiliging een boost geven door toegang te beperken tot degenen die het nodig hebben en het netwerk te beschermen tegen hackers.

5.2 Worden de verschillende zones beveiligd door een firewall?

Ja / Nee

Bijna elke computer beschikt over een softwarematige firewall. Deze firewall controleert het verkeer dat in en uit de computer gaat en controleert deze op gevaren. In uw Windows of Apple computer zit ook al standaard een softwarematige firewall. Veelal zit er in 'anti-virus' software (ook wel End-Point protection genoemd), ook een aanvullende softwarematige firewall. Let op dat deze software alleen uw computer beschermd en niet de rest van het netwerk. Controleer of de instellingen in de softwarematige firewall goed staan ingesteld. Verleen alleen toegang tot wat echt noodzakelijk is.

Een hardwarematige firewall beveiligt niet alleen een specifieke computer, maar alle andere computers/laptops/netwerkcomponenten in het netwerk. Voor thuisgebruik of klein MKB: in de modem of router zit ook vaak al een hardware matige firewall. Zorg ervoor dat deze ook juist is ingesteld m.b.t. de poorten die open staan. Veelal zijn de default settings al goed, maar controleer dit voor de zekerheid. Verleen alleen toegang tot wat strikt noodzakelijk is.

Een hardwarematige firewall wordt vaak achter een modem of router geplaatst, maar soms is het systeem alles in één. Het apparaat fungeert dus zowel als modem of router en als firewall. De firewall zal de complete deur naar het internet beveiligen. Om bedrijfsnetwerken betrouwbaar af te schermen tegen aanvallen vanuit het publieke netwerk (het internet/WAN) wordt normaal gesproken gebruik gemaakt van een DMZ-concept. Met een DMZ (demilitarized zone) wordt ervoor gezorgd dat het kantoornetwerk gescheiden is van de systemen welke benaderbaar zijn vanaf het internet. Mocht het een hacker lukken om via een systeem binnen te komen dat bereikbaar is vanaf het internet, dan is er met een DMZ een extra bescherming naar uw kantoornetwerk ingeregeld.

5.3 Is de toegang tot de verschillende Wifi netwerken gescheiden, met unieke wachtwoorden? Ja / Nee

De verschillende Wifi netwerken moeten worden beveiligd met unieke sterke wachtwoorden.

Deel VI – Bepaal wie toegang heeft tot uw data en diensten

6.1 Is de logische toegang zo ingeregeld dat medewerkers alleen toegang hebben tot de data en systemen die ze nodig hebben voor hun werk? Ja / Nee

De toegang tot systemen en applicaties moet voor medewerkers zo zijn ingericht dat ze alleen toegang hebben waarvoor ze bevoegd zijn en wat ze echt nodig hebben om hun werk uit te voeren. Dit dient te worden ingericht op basis van vooraf gedefinieerde groepen en rollen. Zorg dat de groepen en rollen zijn bepaald in een 'rechtenoverzicht' en dat dit ook overeenkomt met wat is ingericht. Houd daarnaast ook de controle op toegang en rechten van cloudapplicaties.

6.2 Heeft u een indiensttredingsprocedure waarbij de rechten worden toegekend conform het rechtenoverzicht? Ja / Nee

Als medewerkers in dienst komen (of al in dienst zijn) dienen hun rechten te worden toegekend in lijn met het 'rechtenoverzicht' (autorisatiematrix). Voorkom willekeur en vele uitzonderingen. Maak inzichtelijk tot welke systemen en applicaties medewerkers toegang mogen hebben.

6.3 Heeft u een uitdiensttredingsprocedure waarbij de rechten zo spoedig mogelijk op alle systemen worden ingetrokken? Ja / Nee

Indien medewerkers uit dienst gaan, moeten rechten direct worden ingetrokken. Een overzicht van alle medewerkers en hun toegangsrechten is dus erg belangrijk. Vervolgens moet er een heldere procedure in werking worden gesteld, waarbij personeelszaken, administratie en ICT samenwerken. Immers weet de afdeling HR wanneer de desbetreffende medewerker uit dienst gaat en moet ICT daarop acteren en veiligheidsmaatregelen treffen. Er zijn ook 'ticket'- en workflow systemen die dit binnen uw organisatie kunnen ondersteunen.

6.4 Is de toegang tot data en diensten alleen mogelijk met persoonlijke accounts? Ja / Nee

Het gebruik van generieke admin- en groepsaccounts is sterk af te raden. De reden hiervoor is dat een account extra kwetsbaar wordt indien deze door meerdere personen wordt gebruikt. De gebruikersnaam en wachtwoord blijven vaak lang bestaan en kunnen worden misbruikt door ex- medewerkers. Daarnaast is het zo dat een logfile weinig toegevoegde waarde meer heeft, omdat niet met zekerheid kan worden vastgesteld welke medewerker heeft ingelogd. Wij raden sterk aan om het gebruik van generieke en groepsaccounts te verbieden.

6.5 Controleert u met regelmaat de uitgegeven rechten en of deze conform de rechtenstructuur is?

Ja / Nee

Met een vooraf vastgestelde periode dienen uitgegeven accounts en rechten te worden beoordeeld of deze (nog) in lijn zijn met het rechtenoverzicht.

Deel 7 – Versleutel opslagmedia met gevoelige bedrijfsinformatie

7.1 Zijn uw laptops, desktop pc etc, versleuteld?

Ja / Nee

Mocht een laptop worden gestolen, dan is het belangrijk dat eventuele data die erop staat goed is beveiligd. U wilt immers voorkomen dat deze data door anderen kan worden benaderd en misbruikt. De data op de harde schijf moet daarom worden versleuteld. Dit kunt u op een Windows computer doen door middel van bijvoorbeeld Bitlocker of Filevault op een Mac computer.

7.2 Versleuteld u uw belangrijkste data, zoals uw back-ups?

Ja / Nee

De data die is opgeslagen moet ook worden beveiligd, met name uw back-ups. Mocht u toch te maken krijgen met een hack, dan zijn uw back-ups extra beschermd omdat deze zijn versleuteld. Zorg er dus voor dat de configuratie juist is ingericht en dat uw back-ups zijn versleuteld (encrypted).

7.3 Is uw Wifi-netwerk goed ingesteld met de juiste encryptie?

Ja / Nee

Uw Wifi-netwerk moet op een juiste manier zijn geconfigureerd. Als dit niet juist is ingesteld, bent u kwetsbaar voor externen die onbevoegd kunnen inloggen. Gebruik minimaal WPA2 of WPA3.

Deel VIII - Controleer welke apparaten en diensten bereikbaar zijn vanaf het internet en bescherm deze

8.1 Heeft u inzichtelijk welke IT-apparatuur gekoppeld en benaderbaar zijn vanaf het internet?

Ja / Nee

U dient inzichtelijk te hebben welke apparaten vanaf het internet te benaderen zijn. Denk daarbij aan (NAS) servers, computers, telefonie, printers, alarmsystemen.

8.2 Is de toegang van deze apparaten geminimaliseerd tot alleen noodzakelijk?

Ja / Nee

U moet helder hebben wie toegang heeft tot deze apparaten. Zijn dit eigen medewerkers of ook externen? Naast wie er toegang heeft, is het ook belangrijk dat er enkel toegang is via de poorten die nodig zijn. Er mogen dus niet hele reeksen openstaan. Wees er ook alert op dat

niet alle verkeer gerouteerd wordt naar een enkel apparaat of pc, alleen ‘omdat het handig is’. Want als dat handig is, dan is dat het ook zeker voor iemand die kwaad wil. Wees al laatste alert op gebouwbeheer en facilitaire diensten. Zij werken vaak met verouderde software en systemen. Uiteraard is dit wel geheel afhankelijk van uw organisatie en het gebouw.

8.3 Heeft u uw IT-apparatuur (printers, camera’s etc.) in een separaat netwerk-segment geplaatst? Ja / Nee

Zorg ervoor dat deze apparaten op een apart netwerk zijn aangesloten. Het komt regelmatig voor dat deze apparaten een kwetsbaarheid hebben en een patch niet direct door de leverancier beschikbaar is. Om het risico te verkleinen is het daarom verstandig om deze apparaten via een apart netwerk op het internet aan te sluiten. Mocht u via deze apparaten worden gehackt, dan is de kans kleiner dat ze ook bij andere systemen kunnen.

Heeft u nog vragen?

Neem gerust contact op met onze helpdesk via info@cyberfundamentals.nl of 085 004 6455.