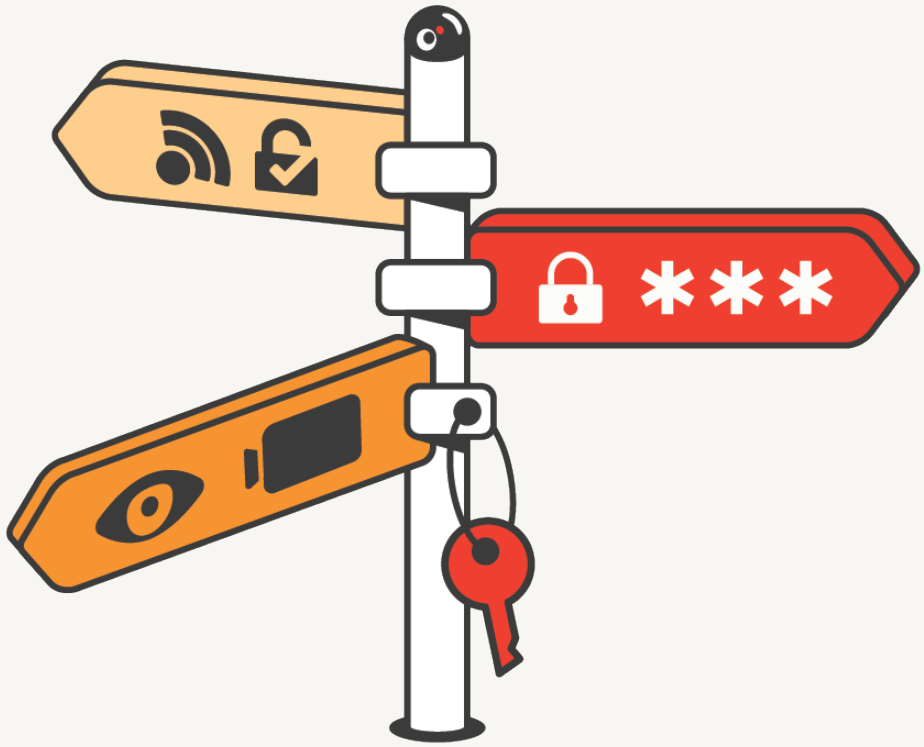


Aan de slag met de Wegwijzer

voor cybersecure gedrag binnen iedere organisatie

Redactie Compacte Wegwijzer: Lourens Dijkstra, CISM MMC
Redactie Compacte Wegwijzer Alert Online: Joyce Martina, Renée Mötter, Myrthe Tiemessen

alertonline.nl

Inhoudsopgave

Wegwijzer in een notendop

De Wegwijzer helpt organisaties om cybersecure gedrag stap-voor-stap te verbeteren. Hiernaast zie je alle zes de stappen in één oogopslag. Elke stap wordt verder in dit document uitgebreid toegelicht.

Een concrete casus als rode draad
Aan de hand van de casus 'het melden van een datalek' lichten we alles toe en wordt duidelijk hoe de Wegwijzer in de praktijk werkt.

alertonline.nl

Stap 1 – Voorbereiden

Bepaal het belangrijkste cyberveiligheidsprobleem waarbij gedrag van medewerkers een rol speelt. Stel een multidisciplinair kernteam samen met voldoende kennis en mandaat. Schrijf een plan van aanpak en bespreek dit met het kernteam.

Stap 2 – Doelgedrag bepalen

Formuleer helder welk gewenst gedrag je van medewerkers verwacht. Dit maakt de gewenste verandering concreet en meetbaar en vormt de basis voor verdere analyse en interventies.

Stap 3 – Gedragsfactoren onderzoeken

Onderzoek waarom medewerkers het huidige gedrag vertonen in plaats van het gewenste gedrag. Gebruik het COM-B-model om de factoren capaciteit, omgeving en motivatie te analyseren. Voer interviews uit en verzamel de belangrijkste bevorderende en belemmerende factoren.

Stap 4 – Interventies kiezen

Selecteer interventies op huidige ongewenste gedragingen. Betrek het kernteam en eventueel andere relevante collega's bij het brainstormen over effectieve maatregelen.

Stap 5 – Interventies uitvoeren

Implementeer de gekozen interventies met aandacht voor communicatie, timing en betrokkenheid. Meet vooraf (nulmeting) en na afloop (1-meting) het effect op het doelgedrag om de effectiviteit te bepalen.

Stap 6 – Verankeren en rapporteren

Borg het gewenste gedrag structureel in de organisatie en geef aandacht aan herhaling. Zorg voor overdracht naar de lijnorganisatie, evalueer het traject en leg de resultaten vast in een eindverslag. Rond het project zorgvuldig af en gebruik de leerpunten voor toekomstige trajecten.

Voorwoord

1/2

Om de digitale weerbaarheid bij organisaties te stimuleren, is het verbeteren van cybersecure gedrag essentieel. Naast campagnes, trainingen en e-learnings ten behoeve van bewustwording, kunnen organisaties zelf ook onderzoek doen naar onderliggende privacy- en veiligheidswaarden van het gedrag van medewerkers. Gedrag verandert namelijk alleen duurzaam wanneer de onderliggende oorzaken van het gedrag goed begrepen worden.

Deze Wegwijzer biedt een praktische, stapsgewijze aanpak om cybersecure gedrag te versterken. Het uitgangspunt is dat een organisatie zelf aan de slag gaat met een vraagstuk op het gebied van digitale weerbaarheid. Hiervoor wordt een doelgedrag bepaald. Vervolgens worden met het COM-B-model de oorzaken van het huidige (ongewenste) gedrag onderzocht. Op basis van de uitkomsten worden interventies gekozen die daadwerkelijk aansluiten bij de belemmeringen in de praktijk. Om de effectiviteit van de interventies te kunnen beoordelen wordt voor de uitvoering een nulmeting uitgevoerd en na afloop van de interventie een vervolgmeting.

De kracht van deze aanpak zit in de gedragsanalyse: het zorgvuldig doorgronden van wat medewerkers nodig hebben om het gewenste gedrag te kunnen en willen vertonen. Door deze methode toe te passen, wordt veilig gedrag niet langer bijkomstig of aanvullend, maar een vanzelfsprekend onderdeel van de dagelijkse praktijk.

De Wegwijzer is bedoeld voor de persoon of het team dat cyberveiligheidsproblemen wil aanpakken. Dat kan een CISO, privacy officer, communicatieadviseur of manager zijn die ziet dat medewerkers onveilig gedrag vertonen en hier verandering in wil brengen. In de Wegwijzer noemen we deze persoon de opdrachtgever: degene die het initiatief neemt, het traject aanstuurt én uiteindelijk de beslissingen neemt.

Voor de aanpak van de Wegwijzer is gebruik gemaakt van het gedragsveranderingswiel van Michie. Deze is opgesteld vanuit negentien gedragsveranderingsraamwerken en biedt hiermee een samenvatting van de meest actuele kennis op dit gebied. De praktische toepasbaarheid is getoetst in 2020 door middel van pilots in verschillende zorgorganisaties.

Voorwoord

2/2

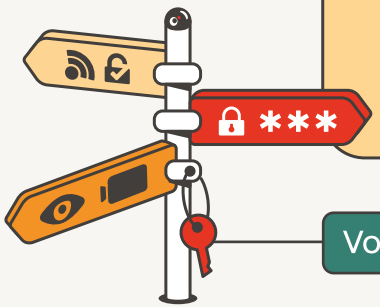
Deze uitgave van de Wegwijzer is een voor Alert Online samengestelde compacte versie naar voorbeeld van Informatieveilig Gedrag in de Zorg. De Wegwijzer van Alert Online is toepasbaar voor iedere organisatie, groot en klein, binnen en buiten de zorg. De originele versie vind je op www.informatieveiliggedragzorg.nl/toolkit/wegwijzer

We wensen je veel succes en plezier bij het doorlopen van alle stappen! En vergeet niet: ga vooral samen aan de slag met cybersecure gedrag!

Team Alert Online

Aan de slag met de <WegWijzer>

> voor cybersecure gedrag binnen iedere organisatie



Voorbereiden

1

- Probleem kiezen
- Vormen multidiciplinair kernteam
- Opstellen plan van aanpak

Doelgedrag bepalen

2

- Probleem nader analyseren
- Keuzelijst doelgedrag opstellen
- Doelgedrag kiezen
- Doelgroep bepalen

START → Kick-off → Doel

Meting

Een 0-meting uitvoeren (optioneel)

Doelgedrag bepalen

3

- Doelgedrag toetsen in de praktijk
- Onderzoeken van de drie factoren (COM) die het gedrag (B) beinvloeden.

COM-B: Capability (capaciteit), Opportunity (omgeving) en Motivation (motivatie)-Behaviour (gedrag)

← Gedragsanalyse

Meting

Voorbereiden van de meting

Interventies kiezen

4

Interventies →

- Koppelen interventiefunctie(s) aan gedragsanalyse
- Interventie(s) bepalen

Zet de gekozen interventies gezamenlijk weg in een planning met verantwoordelijke personen erbij. Dit zorgt voor betrokkenheid en effectiviteit.

Soms is het nodig om een stap terug te gaan om daarna je weg weer te kunnen vervolgen.

Interventies uitvoeren

5

- Implementatiewijze bepalen
- Interventie(s) realiseren

Is de informatie-veiligheid voldoende toegenomen?

Nee

Ja

Meting

Uitvoering meting of 1-meting

Borging

- Verankeren
- Rapporteren en overdragen

Verankeren en rapporteren

6

Stap 1 – Voorbereiden

Een goede voorbereiding is het halve werk. In deze stap leg je de basis voor het succes van de rest van het traject. Neem hierbij de tijd voor de keuze van het probleem en de samenstelling van het kernteam dat dit samen met jou gaat oppakken. Zorg ook voor voldoende draagvlak en urgentie in jouw organisatie om juist met dit probleem aan de slag te gaan.

1.1 Probleem kiezen

Je start met het definiëren van je belangrijkste informatieveiligheidsprobleem. Kies hier een probleem waarvan je vermoedt dat het gedrag van medewerkers de informatieveiligheid belemmert.

Voorbeeld: medewerkers melden datalekken niet (of te laat) via de servicedesk. Dit leidt onder andere tot het niet goed informeren van de mensen die het betreft, het missen van verplichte meldingen aan de Autoriteit Persoonsgegevens en het verhogen van kans op imagoschade.

1.2 Vormen multidisciplinair kernteam

In het kernteam heb je mensen nodig die de organisatie goed kennen en voldoende zeggenschap hebben. Denk aan:

- Een of enkele medewerkers die in de dagelijkse praktijk te maken (kunnen) krijgen met het probleem;
- Een vertegenwoordiger vanuit het bestuur of management;
- Een privacy officer en/of een CISO;
- Een communicatieadviseur;
- Een opleidingsadviseur.

Het kernteam komt regelmatig bij elkaar om alle stappen gezamenlijk te doorlopen. Maak ook afspraken over wie de opdrachtgever is: de persoon die initiatiefnemer is en uiteindelijk beslissingen neemt en producten goedkeurt. De grootte van het kernteam bepaal je zelf en hangt waarschijnlijk af van het aantal mensen, teams of afdelingen in de organisatie.

1.3. Opstellen plan van aanpak

In deze stap maakt het kernteam een plan van aanpak en legt dit ter goedkeuring voor aan de opdrachtgever. Door vooraf goed met elkaar na te gaan wat er nodig is om je project tot een goed einde te brengen, voorkom je verrassingen gedurende het traject.

Stap 2 – Doelgedrag bepalen

Het doelgedrag, het gewenste gedrag dat je bij medewerkers zou willen zien, formuleren schept duidelijkheid over wat de organisatie precies van medewerkers verwacht. Door het doelgedrag nauwkeurig te bepalen, weet je welk gedrag je wilt zien en maak je de beoogde verandering meetbaar. Het geformuleerde doelgedrag is de basis voor een scherpe gedragsanalyse en het ontwikkelen van een effectieve interventie.

Een goed doelgredrag is altijd specifiek, waarneembaar en meetbaar. Formuleer het als een concrete actie die een medewerker uitvoert. Gebruik hiervoor de volgende vragen als leidraad:

- Wie voeren het gedrag uit?
- Wat doen ze concreet?
- Wanneer of in welke situatie?
- Hoe vaak of in welke frequentie?

Voorbeeld: doelgedrag = alle medewerkers melden een (vermoedelijk) datalek direct, uiterlijk binnen 24 uur, via het meldformulier op intranet. Ook als ze twijfelen of het écht een lek is.

Stap 3 – Gedragsfactoren onderzoeken

In deze stap onderzoek je waarom medewerkers het gewenste gedrag nog niet (voldoende) vertonen. Dit doe je met het COM-B-model: een gestructureerde methode om de oorzaken van gedrag te analyseren. De uitkomsten zijn de basis voor de interventies in stap 4.

Het COM-B model: wat is het?

Het COM-B-model gaat ervan uit dat gedrag, oftewel "behavior" (B) wordt bepaald door drie factoren:

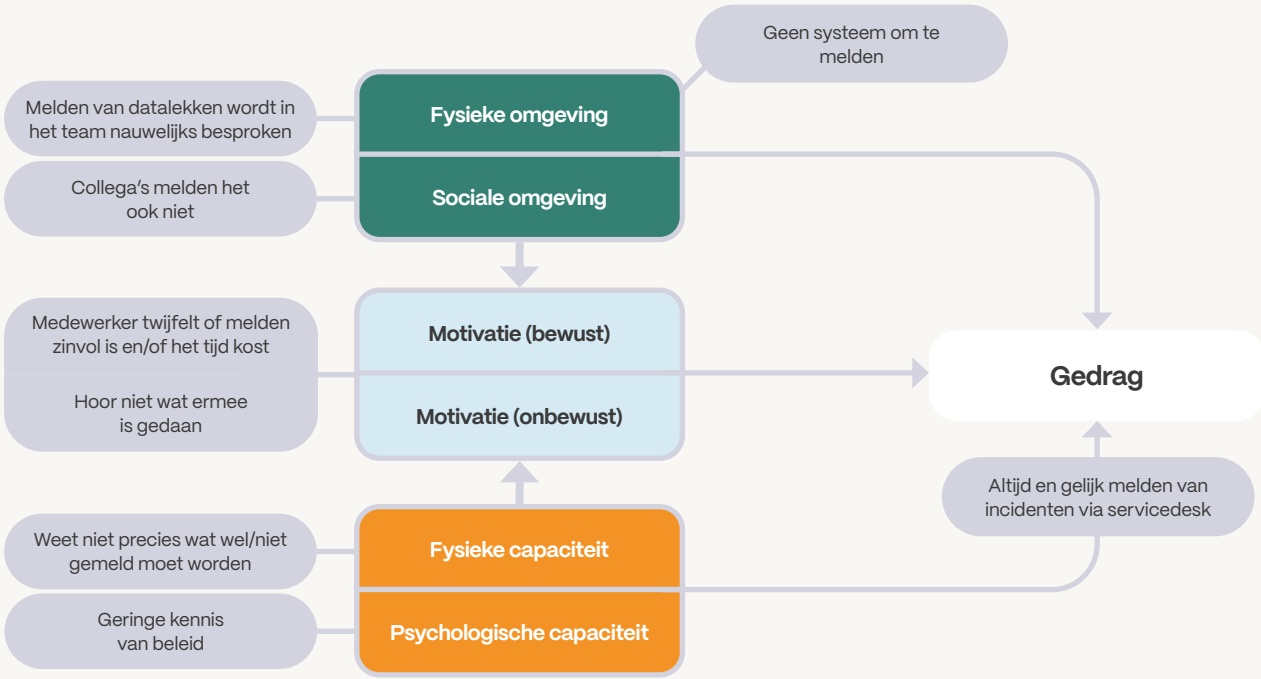
1. Capaciteit (C): heeft de medewerker kennis, vaardigheden en het zelfvertrouwen om het gedrag uit te voeren?
2. Omgeving (O): maakt de fysieke of sociale omgeving het gedrag makkelijk of juist moeilijk?
3. Motivatie (M): wil de medewerker het gedrag uitvoeren, bewust of onbewust?

Per factor onderscheiden we twee typen en komen zo tot zes categorieën:

- Fysieke capaciteit
- Psychologische capaciteit
- Fysieke omgeving
- Sociale omgeving
- Bewuste motivatie
- Onbewuste motivatie

Een voorbeeld van COM-B

Doelgedrag: medewerkers melden een datalek



3.1. Doelgedrag toetsen in de praktijk
Voordat je een vragenlijst opstelt voor de nulmeting, ga je de praktijk in. Dat doe je door individuele interviews te houden met medewerkers uit de doelgroep van je gekozen gedrag dat je wilt veranderen. Deze gesprekken geven kwalitatief inzicht in de belemmeringen en bevorderende factoren. Hoeveel interviews je nodig hebt, hangt af van de omvang van je organisatie en diversiteit van je doelgroep. Werk met een vaste gespreksleidraad, zodat je de uitkomsten goed kunt vergelijken. Noteer na elk gesprek eigen observaties. Stel voor elke COM-B-categorie gerichte vragen.

3.2 Analyse
Als je alle interviews hebt afgerond, zoek je de rode draad. Verzamel per gesprek de COM-B-factoren en onderscheid de factoren die het doelgedrag bevorderen van de factoren die het belemmeren. Verzamel daarna de meest genoemde factoren per categorie in één overzicht. Je weet welke factoren het doelgedrag beïnvloeden, zodat je passende interventies kunt kiezen.

Voorbeeld: uit interviews blijkt dat de meeste medewerkers niet precies weten wat een meldplichtig datalek is (fysieke capaciteit). Bovendien horen ze nooit terugkoppeling na een melding, waardoor melden als zinloos wordt ervaren (onbewuste/bewuste motivatie).

3.3 Nulmeting
Voordat je de interventies uitvoert, is het belangrijk een nulmeting te doen. In deze stap ga je bepalen op welke manier je de effecten van je interventie(s) op je doelgedrag op een systematische manier gaat meten. Met deze meting wil je na de inzet van je interventie(s) kunnen vaststellen of deze effectief zijn geweest bij het veranderen van het gedrag.

Het meten van de effecten van je interventie(s) vereist tijd en middelen van je organisatie. Ook vraagt het vaak om samenwerking met collega's van andere afdelingen en teams. Daarom is het belangrijk dat je op tijd en ruim voor het ontwikkelen van je interventie begint met het voorbereiden van deze meting.

Zorg ook dat je de nulmeting zo opzet dat je hem later kunt herhalen (dezelfde methode en doelgroep).

Voorbeeld: via een korte enquête onder alle medewerkers vraag je of ze in de afgelopen maand een (mogelijk) datalek hebben meegemaakt en deze hebben gemeld.

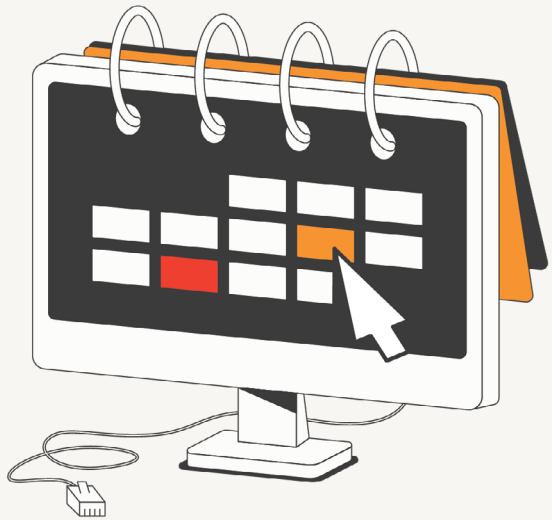
Stap 4 – Interventies kiezen

Om de beoogde verandering daadwerkelijk te bereiken, kies je in deze stap passende gedrags-interventies. Daarbij maak je gebruik van alle kennis die je hebt verzameld. Door te kiezen op basis van de gevonden COM-B-factoren, vergroot je de kans op succes.

Brainstorm met het kernteam over welke interventies mogelijk zijn. Haak hier indien nodig andere mensen bij aan, zoals medewerkers uit de doelgroep, communicatie, HR-management of collega's die zich bezighouden met opleidingen. Hou hierbij de inzichten uit de gedragsanalyse over de doelgroep en de context steeds voor ogen, zoals het doelgedrag dat je nu nog onvoldoende ziet.

Koppel interventies aan COM-B-factoren.
Elke COM-B-factor vraagt om een ander type interventie, denk daar goed over na.

Voorbeeld: gekozen interventies voor de casus: 1) Kennissessies voor medewerkers over wat een datalek is en hoe je het meldt; 2) Directe link naar het meldformulier op het startscherm van intranet; 3) Maandelijkse terugkoppeling aan het team over het aantal meldingen en de afhandeling ervan.



Stap 5 – Interventies uitvoeren

Nu is het tijd om de gekozen interventies daadwerkelijk uit te voeren. Let op de manier waarop je ze implementeert. Denk aan de communicatie, het kanaal en de timing. De gedragsanalyse geeft waardevolle informatie die je ook bij dit onderdeel kunt gebruiken.

Denk bij de implementatie na over de volgende onderwerpen:

- Welk communicatiekanaal is het meest effectief?
- Wat is de juiste tone of voice?
- Namens wie wordt de boodschap verstuurd?
- Wat is een handige timing?

Voorbeeld: de kennissessie wordt gegeven door de privacy officer. De uitnodiging wordt verstuurd door de teamleider. De sessie wordt ingepland in het maandelijkse teamoverleg. Medewerkers die niet aanwezig zijn, worden op een andere wijze geïnformeerd (bijvoorbeeld door het verslag via de mail te versturen).

Vervolgmeting (1-meting)

Na het uitvoeren van de interventies herhaal je de nulmeting die je eerder hebt gedaan. Bij deze 1-meting kan je ook in kaart brengen hoe je doelgroep de interventie(s) heeft ervaren. Vergelijk de resultaten: zijn er verschillen in de frequentie van het uitvoeren van het doelgedrag? Wordt het gedrag vaker of minder vaak uitgevoerd?

Voorbeeld: dezelfde enquête wordt opnieuw uitgezet. Het percentage medewerkers dat een datalek heeft gemeld is gestegen van 18% naar 54%. Medewerkers geven aan nu beter te weten waar en wanneer ze wat moeten melden.

Stap 6 – Verankeren en rapporteren

Een verandering is geen eenmalige actie. Als je wil dat de verandering het nieuwe normaal wordt, moet hier structureel aandacht aan worden besteed. Daarvoor moet het worden verankerd in de organisatie.

6.1 Verankeren

Bepaal samen met je kernteam wat nodig is om het doelgedrag te verankeren binnen de organisatie. Zorg voor een goede overdracht van het project naar de 'lijn', de staande organisatie. Vervolgens maak je een compact eindverslag van je traject. Verwerk hierin ook aandachtspunten voor wanneer de Wegwijzer wordt ingezet over een ander thema.

Voorbeeld: het meldformulier wordt permanent geplaatst op het startscherm van intranet. Het thema 'datalek melden' wordt onderdeel van de jaarlijkse cybersecurity awareness training.

6.2 Rapporteren

Evalueer samen met het kernteam het traject: wat ging goed en wat kon beter? Vervolgens zorg je voor een juiste archivering van de documenten en rond je het project af. Je kunt aan het eind dit project met een gerust hart achter je laten en een nieuw traject starten gericht op cyberveilig gedrag!

Tot slot

De kracht van de aanpak van deze Wegwijzer ligt in de eenvoud en de focus.

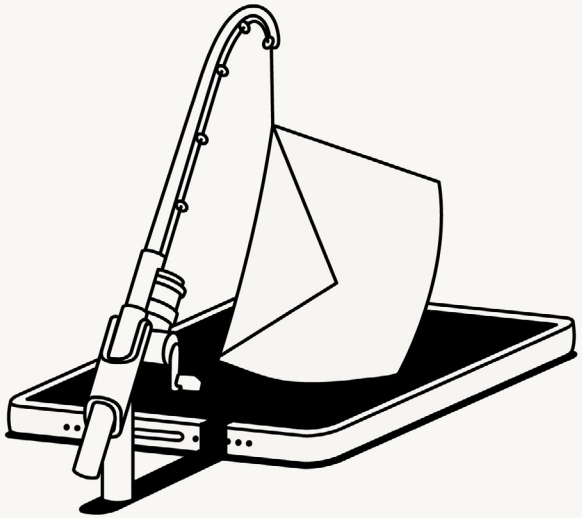
Door klein te beginnen, gedrag concreet te maken en interventies te baseren op feitelijke analyse, ontstaat een aanpak die werkt. Niet omdat medewerkers 'moeten' veranderen, maar omdat de organisatie en collega's hen helpen om veilig gedrag vanzelfsprekend te maken. We danken Informatieveilig gedrag in de zorg voor het mede tot stand komen van deze editie van de Wegwijzer".

Veel succes en plezier met de volgende stappen richting optimale cybersecurity!

Samen richting de cybersecuritymaand
Bedankt dat je de Wegwijzer hebt ingezet om cyberveiligheid in je organisatie te verbeteren. Alleen samen kunnen we aan de slag met cybersecure gedrag!

Alert Online is hét netwerk rondom digitale weerbaarheid. Meer tips, informatie en inspiratie over online veiligheid en cybersecure gedrag in organisaties vind je bij Alert Online (LinkedIn) of op www.alertonline.nl.

Alert Online: Samen richting de Cybersecuritymaand.



alertonline.nl