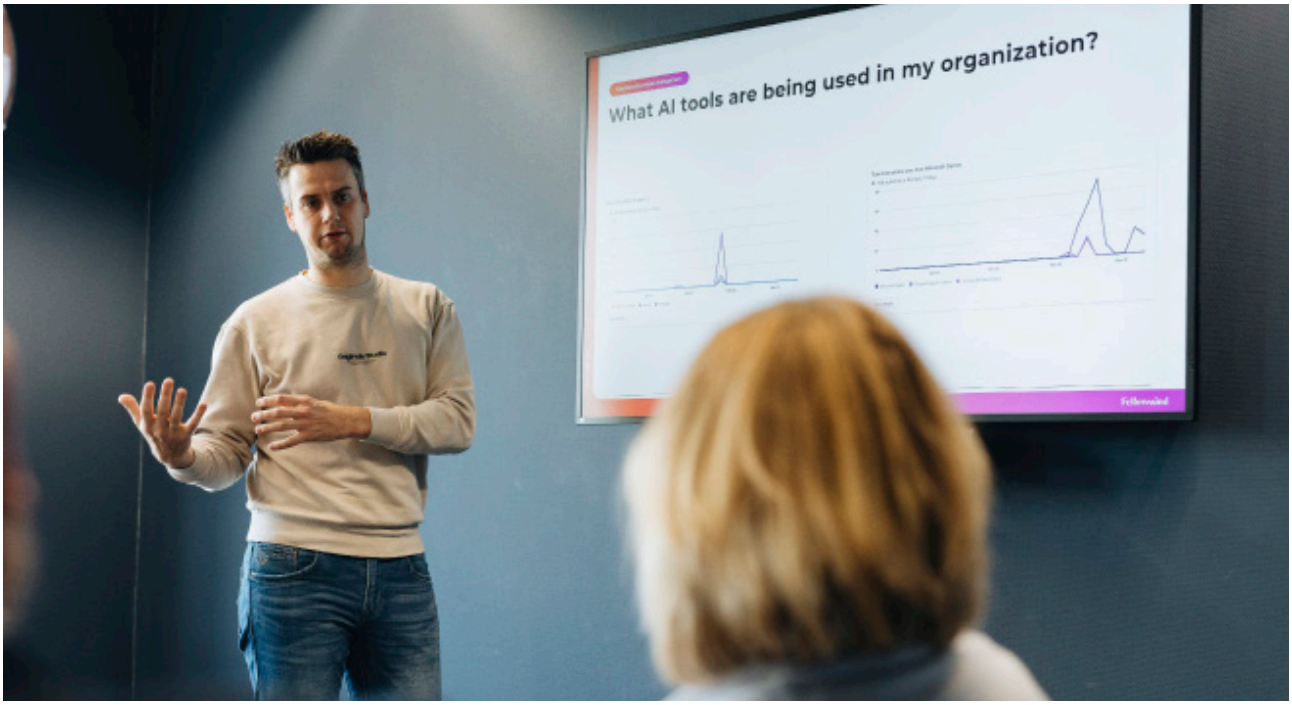
Overal veilig

Cybersecurity volgens Fellowmind

Overal werken is nog nooit zo makkelijk geweest. Met laptops, ergonomische schermen, snelle glasvezelverbindingen en platforms als Microsoft 365 is het voor veel organisaties vanzelfsprekend geworden dat medewerkers altijd en overal toegang hebben tot hun werk. Op kantoor, thuis, onderweg of bij klanten: de digitale werkplek is overal aanwezig.



Maar die flexibiliteit heeft ook een keerzijde. Hoe meer systemen, apparaten en verbindingen een organisatie gebruikt, hoe groter het digitale aanvalsoppervlak wordt. Cybersecurity is niet langer alleen een technische uitdaging voor de IT-afdeling, maar een allesomvattend vraagstuk.

Bij Fellowmind houden ze zich dagelijks bezig met die balans tussen flexibiliteit en veiligheid. Het bedrijf is in 2019 ontstaan uit een fusie, met als doel organisaties te helpen toekomstbestendig te worden in een steeds digitalere wereld. De focus ligt op het slimmer inzetten van technologie om organisaties efficiënter, veiliger en wendbaarder te maken.

Dat gebeurt inmiddels op grote schaal. Met meer dan 2100 medewerkers, verspreid over 31 kantoren in vijf landen, ondersteunt het bedrijf wereldwijd ruim 3000 organisaties bij hun digitale ontwikkeling.

Johan Voerman en Richard Verbeek zijn twee van die medewerkers bij Fellowmind. Johan is gespecialiseerd in security, Richard op het gebied van Modern Work - de moderne, digitale werkplek - maar de twee werken veel samen: ‘Onze expertisegebieden zijn echt verweven.’

En dat is niet zo gek. Want in een organisatie waar iedereen altijd en overal toegang heeft tot data, zijn security en de digitale werkplek simpelweg niet meer los van elkaar te zien.

Ondernemen in een digitale wereld

De digitale werkplek heeft de afgelopen tien jaar een enorme ontwikkeling doorgemaakt. Waar cloudoplossingen ooit vooral werden gebruikt voor e-mail en een

paar gedeelde documenten, vormt de cloud inmiddels de kern van veel organisaties.

Richard ziet die ontwikkeling duidelijk terug bij bedrijven waar Fellowmind mee werkt: 'Als je het tien jaar geleden over modern work had, betekende dat misschien dat je iets in de cloud had, zoals je mail of wat verdwaalde documenten. Nou, dat is nu wel anders.' De vragen die organisaties stellen is daardoor veranderd: 'Tegenwoordig is het bijna nooit meer: hoe kom ik in de cloud? Modern Work gaat vandaag niet alleen over waar je werkt, maar vooral over hoe je veilig, flexibel en productief samenwerkt met data, applicaties en collega's, ongeacht locatie.'

Voor veel organisaties verlopen vrijwel alle bedrijfsprocessen tegenwoordig digitaal. Documenten, communicatie, planningen en applicaties zitten in de cloud en zijn vanaf verschillende apparaten toegankelijk. En daar begint het securitygedeelte: 'Je moet dan natuurlijk wel goed duidelijk hebben wie waarbij mag en welke data direct beschikbaar is.'

Bij Fellowmind kijken ze daarom niet alleen naar de technologie zelf, maar naar de bredere inrichting van een organisatie. Aan apparatuur heb je volgens deze twee een stuk minder, als er niet het juiste beleid omheen zit: 'Governance begint waar security eindigt.'

De grootste misvatting

Wanneer organisaties nadenken over cybersecurity, gaat de aandacht vaak direct naar technologie. Nieuwe tools, firewalls of monitoringsoftware moeten de organisatie beschermen tegen digitale dreigingen. Maar volgens Johan en Richard ligt het echte risico vaak ergens anders. 'Zonder mensen heb je natuurlijk geen organisatie', zegt Johan. 'Je kan met de huidige technologie alle data achter slot en grendel zetten, maar als je medewerkers er vervolgens niets meer mee kunnen doen, wat heb je er dan aan?' Cybersecurity gaat daarom niet alleen over systemen, maar ook over processen en gedrag. 'Alleen mensen begrijpen precies wat er in een organisatie gebeurt.'

Dat merkt Fellowmind in de praktijk bij veel organisaties. Sommige bedrijven zijn technologisch al ver gevorderd, terwijl andere organisaties nog werken met systemen die jaren geleden zijn ingericht. 'Elk bedrijf is ook anders', zegt Richard. 'Niet alleen in de opbouw, maar ook in de mate van vooruitgang. En dan is er ook nog wetgeving; de eisen in zorgorganisaties zijn bijvoorbeeld heel anders dan in de maakindustrie.'

> **'Technologie werkt pas als mensen ermee werken'**

De menselijke factor

Maar elk bedrijf heeft volgens Richard één ding gemeen: 'Er is geen enkele organisatie, of er nou 30 of 3000 man rondlopen, waar je niet met de menselijke kant bezig moet.' Nieuwe systemen invoeren is relatief eenvoudig; medewerkers meenemen is vaak een grotere uitdaging. 'Als je de technologie aanpast, maar vergeet de medewerkers mee te nemen, dan loop je vast; als iemand die onderdeel is van een kritiek proces 20 jaar lang op één knopje heeft gedrukt, en dat knopje werkt ineens anders of niet meer, dan krijg je problemen.'

Johan knikt instemmend. Beleid en technologie moeten dan ook hand in hand gaan in de security: 'Zonder mensen heb je natuurlijk geen organisatie. Je kan alle data achter slot en grendel zetten, maar als je medewerkers er vervolgens niets meer mee kunnen doen, wat heb je er dan aan? Technologie werkt pas als mensen ermee werken.'

Tegelijkertijd liggen de grootste kwetsbaarheden óók bij de mens: 'Het aanvalspunt is de persoon. Een cyberincident is geen technisch probleem, criminelen zijn gewoon op zoek naar inlogggevens; het is bijna geen hacken te noemen.' Johan ziet wel dat nieuwe techniek helpt je hiertegen te wapenen: 'Met AI kan je tegenwoordig met een klein team, of zelfs alleen, een enorme impact maken. Daarvoor moet de technologie ook weer op orde zijn. Door slimme beveiliging en automatisering zoveel mogelijk technisch af te vangen, maak je het voor medewerkers makkelijker om het juiste te doen.'

Technologie en de mens gaan op de moderne werkplek dus hand in hand. Het is volgens Fellowmind van belang dat er juist ingezet wordt op bewustwording en adoptie, zeker nu die werkplek niet langer gelimiteerd is aan een kantoor.

Security op een digitale werkvloer

De opkomst van hybride werken heeft de digitale werkplek ingrijpend veranderd. Medewerkers werken niet meer alleen binnen het netwerk van hun organisatie, maar vanaf verschillende locaties en apparaten.

Voor IT-managers betekent dat dat controle over systemen complexer is geworden. Vroeger was duidelijk waar iedereen werkte, maar tegenwoordig kan iedereen vanaf vrijwel elke gewenste plek inloggen. Toch hoeft dat volgens Richard geen probleem te zijn:

‘De technologie om veilig thuis te werken, die is er wel, dat is niet zo spannend. De vraag is alleen hoe je het toepast. Alles valt en staat met beleid.’ Veel organisaties werken tegenwoordig met cloudplatforms waarbij apparaten centraal beheerd kunnen worden. ‘Wij werken met Microsoft, waarbij je alle apparaten op een veilige en gestructureerde manier kan runnen, en dat geldt voor de meeste bedrijven.’

In de praktijk helpt Fellowmind organisaties om die omgeving goed in te richten: van toegangsbeheer tot device management en databeveiliging. Daarna blijft het contact bestaan; technologie staat immers nooit stil.

Een constant proces

Cybersecurity is geen eenmalig project, maar een continu proces. Nieuwe dreigingen ontstaan voortdurend en systemen veranderen continu. Johan vergelijkt de digitale omgeving vaak met een huis: ‘Na het schoonmaken is het even netjes. Maar als je vervolgens maanden of een jaar niet schoonmaakt, dan is het één grote troep. Datzelfde geldt ook in ieder IT-landschap.’

Volgens hem moeten organisaties daarom voortdurend blijven investeren in hun digitale veiligheid: ‘Je moet constant met de techniek bezig blijven en nieuwe securitymaatregelen adopteren. Wat vandaag veilig is, kan morgen alweer voor een lek zorgen.’ Dat klinkt misschien als een grote opgave, maar Johan stelt ons gerust: ‘Als je er eenmaal mee bezig bent, is bijbenen niet moeilijk.’

Bij Fellowmind zelf krijgen ze bijvoorbeeld elke maand een korte online training om bedreigingen te begrijpen en erop te anticiperen. Daarmee zorgen ze dat iedereen weet wat er speelt: ‘Die trainingen komen niet alleen bij mij, op de security-afdeling, maar ook bij Richard, bij communicatiemedewerkers, bij de klantenservice. Iedereen heeft met security te maken, niet alleen de IT.’

En die constante veranderingen komen niet alleen door nieuwe technologieën of aanvalstechnieken, maar ook aan de hand van wetgeving. De Cyberbeveiligingswet legt de verantwoordelijkheid voor cybersecurity bijvoorbeeld expliciet bij managers en ondernemers. Niet alleen IT, maar de hele organisatie moet aantoonbaar maatregelen nemen. ‘Het zorgt ervoor dat ons bedrijfsleven toekomstbestendig is en blijft’, zegt Johan. ‘Het dwingt je ergens actie te ondernemen, anders riskeer je bijvoorbeeld boetes.’ Dat ziet hij niet als vervelend, maar als springplank om je beveiliging goed te gaan inrichten.

De rol van Fellowmind

En daar komt Fellowmind om de hoek kijken. Johan en Richard gaven eerder in dit artikel al aan dat er geen standaardoplossing voor cybersecurity of de digitale werkplek is. Daarom beginnen ze met het in kaart brengen van de bestaande situatie. ‘We beginnen met een assessment, kijken wat nodig is en helpen je vanuit daar verder’, zegt Johan.

Op basis daarvan wordt een roadmap opgesteld die kan bestaan uit verschillende stappen: het verbeteren van de digitale werkplek, het versterken van securitymaatregelen of het opzetten van duidelijke governance.

Zeven stappen voor een betere cyberweerbaarheid
De Cybersecurity Assessment van Fellowmind

1

Train je mensen als eerste verdedigingslinie
Ga verder dan een eenmalige phishing-test:
- Zet in op het herkennen van AI-gegenereerde phishingmails
- Kadreer hoe verdachte signalen gerapporteerd en besproken worden
- Creëer een open meldcultuur

2

Breng je assets in kaart
Inventariseer alle assets die medewerkers gebruiken - ook Shadow IT.

3

Breng patchbeleid naar de voorgrond
Bijna elke hack maakt gebruik van een bekend lek. Updates kunnen daarom niet blijven liggen. Prioriteer daarbij kritieke plekken, die bijvoorbeeld via het internet te bereiken zijn. Leg verantwoordelijkheden vast.

4

Weet wie je netwerk in en uit gaat
Leveranciers, partners en ex-medewerkers blijven vaak toegang houden. Controleer periodiek op rechten en zorg dat toegang beperkt is tot noodzakelijke systemen.

5

Segmenteer je netwerk
Zorg dat aanvallers niet via de mailserver direct de financiële omgeving binnen kunnen komen. Extra tip: combineer dit met Zero Trust Access, zodat er geen bruggen tussen netwerken open blijven.

6

Oefen je Incident Response Plan
Opschrijven is niet genoeg; test je beveiligingsplannen:
- Leg taken en rollen vast
- Simuleer jaarlijks een aanval
- Leer van de evaluatie

7

Test je weerbaarheid regelmatig
Fellowmind ziet dat organisaties die jaarlijks een Cybersecurity Assessment uitvoeren, veel beter in staat zijn om risico's te beperken en snel te reageren.

'Sommige bedrijven moeten echt een compleet nieuwe inrichting krijgen, sommige hoeven alleen hun voorsprong verder uit te breiden.' In andere gevallen ligt de uitdaging juist in beleid of adoptie: 'Sommige hebben veel technologie klaarstaan, maar nog niets aan beleid. Nou, ook daar kunnen we helpen.'

Een kant-en-klaar stappenplan is er dus ook niet. Niet alleen door de opbouw van een bedrijf, maar ook door de achterliggende beveiligingsgedachte: 'Het doorgronden van de waarom is het belangrijkst; die is voor iedereen anders.' Daarom gaat Fellowmind eerst bezig met mens en beleid, en richt daarna de technologie daarop in.

Security als groei-enabler
Cybersecurity wordt nog te vaak gezien als een kostenpost of een noodzakelijk kwaad. Volgens Richard is dat een verkeerde manier van kijken: 'Als je in een sector zit waar je standaard met vijf concurrenten in een race zit, moet je harder gaan dan de rest.' Beveiliging helpt daarbij: 'In een auto durf je ook harder te rijden wanneer je weet dat je goede remmen hebt.'

Goede beveiliging zorgt ervoor dat organisaties met vertrouwen kunnen werken, innoveren en groeien. Johan ziet dat ook bij klanten: 'Als je alles op z'n plaats hebt en duidelijk hebt wie waar bij kan, dan kun je inderdaad knallen.' Het alternatief? Dat is onzekerheid. 'Als het onduidelijk is wie waarvandaan inlogt en waar alles staat, dan zou ik ook even op de rem trappen.'

Cybersecurity is volgens de twee experts daarom geen rem op, maar een voorwaarde voor innovatie. Johan weet: 'De toekomst is soms een blur, maar er is altijd een pad zichtbaar.'

Fellowmind helpt je graag op dat pad: 'Als ondernemer hoef je niet alles zelf te weten', zegt Johan. 'Maar je moet wel weten waar je staat. Vanuit daar helpen wij organisaties om hun digitale fundament toekomstbestendig te maken.'