Veilig op weg naar morgen

De factoren die bedrijven succesvol maken

"Wie cybersecurity serieus neemt, bereikt meer dan alleen bescherming."

Together we can

vodafone business

8 niet te missen inzichten die dit e-book u oplevert

Sommige bedrijven doen het gewoon beter dan andere. Ze zijn veiliger. Veerkrachtiger. Daar kunnen tal van factoren in meespelen – en daar hebben we niet altijd invloed op. Maar een aantal factoren maakt deze bedrijven Fit For the Future (FFtF). En dat blijkt een kwestie van keuzes maken. Zij beschermen zich bijvoorbeeld beter tegen cyberdreigingen en baseren hun keuzes en ervaringen op inzichten zoals deze:

1. **Slechts 25% (FFtF bedrijven: 39%) heeft een duidelijk plan voor cybersecurity.**
2. **Bedrijven zetten cybersecurity op de 9e plaats (van de negen) in hun Top Prioriteiten.**
3. **Twee derde noemt meerdere zwakke punten in hun cloudbased en hosted servers.**
4. **Een derde zegt dat zij afgelopen jaar niet goed konden omgaan met een bedrijfsverstoring.**
5. **Succesvolle cybersecurity vraagt om een gestructureerde aanpak – niet om toevalstreffers.**
6. **Nieuwe technologie biedt veel meer kansen dan alleen besparing op arbeidskosten.**
7. **Cybersecurity fungeert als onderscheidende factor bij het binnenhalen van nieuwe opdrachten.**
8. **Bedrijven die Fit For the Future zijn komen sneller, beter en veiliger uit een crisis.**

De Top 5 uitdagingen die bedrijven zien in cyberdreiging

Veiligheid in de cloud	Bescherming van gevoelige bedrijfs- en persoonlijke gegevens	Beveiliging van alle verschillende apparaten in ons bedrijf (incl. mobiele, persoonlijke, IoT-apparaten enz.)	Bestrijding van ransomware en andere malware	Ervoor zorgen dat alleen geautoriseerde mensen toegang tot onze systemen hebben
32%	32%	31%	31%	30%
27%	43%	30%	28%	36%

% ranking binnen de top 5 (van de 15 getest)

% 'zeer veel vertrouwen' in het vermogen van de organisatie om het probleem aan te pakken

Hoe groot is uw
bedrijfsveerkracht & cybersecurity?

We voerden ons jaarlijkse Fit For the Future onderzoek uit onder 3.101 bedrijven in vijftien landen. In Nederland namen 322 bedrijven deel aan de online enquête. Naast belangrijke onderwerpen als duurzaamheid, innovatie & IoT vroegen we dit jaar met name naar bedrijfsveerkracht & cybersecurity.

Minder voorbereid op incidenten

Als het om cybersecurity gaat, laat het onderzoek opvallende resultaten zien. Zo zeggen veel bedrijven in Nederland dat ze goed kunnen omgaan met bedrijfsverstoringen. 66% van de bedrijven in Nederland meldt bijvoorbeeld dat zij in het afgelopen jaar goed konden omgaan met zo'n incident. Echter, als we naar de grote ondernemingen kijken, daalt het percentage dat denkt goed voorbereid te zijn om risico's en uitdagingen het hoofd te bieden. En het is interessant hoe zij specifiek tegen cybersecurity aankijken.

Welke risico's zien bedrijven?

Economische risico's worden veel genoemd, maar ook een reeks andere opkomende risico's, waaronder arbeidsrisico's, het milieu en uitdagingen in verband met opkomende technologie. Gevraagd waar zij hun veerkracht moesten verbeteren, zetten bedrijven cybersecurity op de negende plaats (van de negen)...

In Nederland lopen we flink achter op het wereldwijde gemiddelde qua 'maturity' van de cybersecurity: 16% geeft toe er niet veel over nagedacht te hebben.

Slechts 25% van de bedrijven (FFtF bedrijven: 39%) heeft een duidelijk plan voor cybersecurity en heeft de meeste van de geplande maatregelen genomen. Dat komt omdat 29% van de bedrijven denkt dat zij niet getroffen zullen worden door cybersecurityproblemen en zich dus niet hoeven voor te bereiden op incidenten! Overigens zijn FFtF bedrijven wel aanzienlijk vaker 'zeer goed voorbereid' met allerlei incidentbestrijdingsmaatregelen dan non-FFTH bedrijven.

Driekwart heeft geen plan voor cybersecurity

75% heeft dus geen betrouwbare aanpak klaarliggen voor incidenten. Cybersecurity heeft voor Nederlandse bedrijven duidelijk (nog) geen hoge prioriteit. Toch zien de meeste bedrijven de toenemende ernst van cyberdreigingen in. De dreiging van cybercriminaliteit neemt volgens bedrijven toe door drie zaken:

- Kans voor cybercriminelen om geld te verdienen aan aanvallen
- Acties van vijandige buitenlandse regeringen/cyber-'oorlogsvoering'
- Gemakkelijke toegang tot instrumenten om aanvallen mee te plegen

Met elkaar samenwerken

Essentieel voor succesvolle bescherming

Andere uitdagingen ziet men in de veiligheid in de keten. Toch controleren veel Nederlandse bedrijven hun toeleveranciers onvoldoende of maken geen noodplannen. Er lijkt wel verbetering op komst: 49% van de bedrijven is het ermee eens dat er 'meer samenwerking tussen organisaties moet zijn om uitdagingen op het gebied van cybersecurity aan te pakken'.

Onvoldoende voorbereid

Slechts 24% van de bedrijven actualiseert hun beveiligingsaudits van toeleveranciers regelmatig 51% van de bedrijven zei dat zelfs als een toeleverancier een beveiligingsprobleem of lek had, ze waarschijnlijk daarmee zouden blijven werken. Dit kan deels te wijten zijn aan een gebrek aan alternatieven: slechts 25% (FFtF bedrijven: 52%) vindt dat ze 'zeer goed voorbereid' zijn wat betreft het hebben van alternatieve/vervangende leveranciers in geval van een cybersecurityprobleem.

Boven aan de agenda: beveiliging van de cloud

Van de 20 verschillende technologieën waarover gevraagd werd, stond cloud-gerelateerde technologie in de top van gebieden waarvan de beveiliging als zwak wordt ervaren. En maatregelen tegen bedreigingen van cloudtechnologie worden zeer inconsequent genomen – zelfs bij FFtF bedrijven... Twee voorbeelden: slechts 23% van de bedrijven met cloudtechnologieën gebruikt vulnerability-assessmentdiensten. En slechts 20% van de bedrijven met cloudtechnologieën gebruikt penetratie-testdiensten.

Met elkaar samenwerken
Essentieel voor succesvolle bescherming

29% van de bedrijven denkt dat zij niet getroffen zullen worden door cyber cybersecurityproblemen. En dat zij zich dus niet hoeven voor te bereiden op incidenten... Hoopgevend: hoewel cybersecurity een aanzienlijke last en kostenpost kan zijn, zien Fit For the Future bedrijven dit duidelijker als een katalysator voor de invoering van nieuwe technologie.

> **“Wij zien informatiebeveiliging als iets wat nieuwe kansen schept in plaats van een obstakel.”**

FFtF bedrijven zien cybersecurity ook vaker als een potentiële onderscheidende factor bij het binnenhalen van nieuwe opdrachten. “Een goede reputatie op het gebied van informatiebeveiliging is een onderscheidende factor waarmee we nieuwe klanten kunnen winnen”, zegt 58% van de FFtF ondernemingen, tegen 45% van het gemiddelde bij bedrijven.

Wat FFtF bedrijven onderscheidt in hun cybersecurity

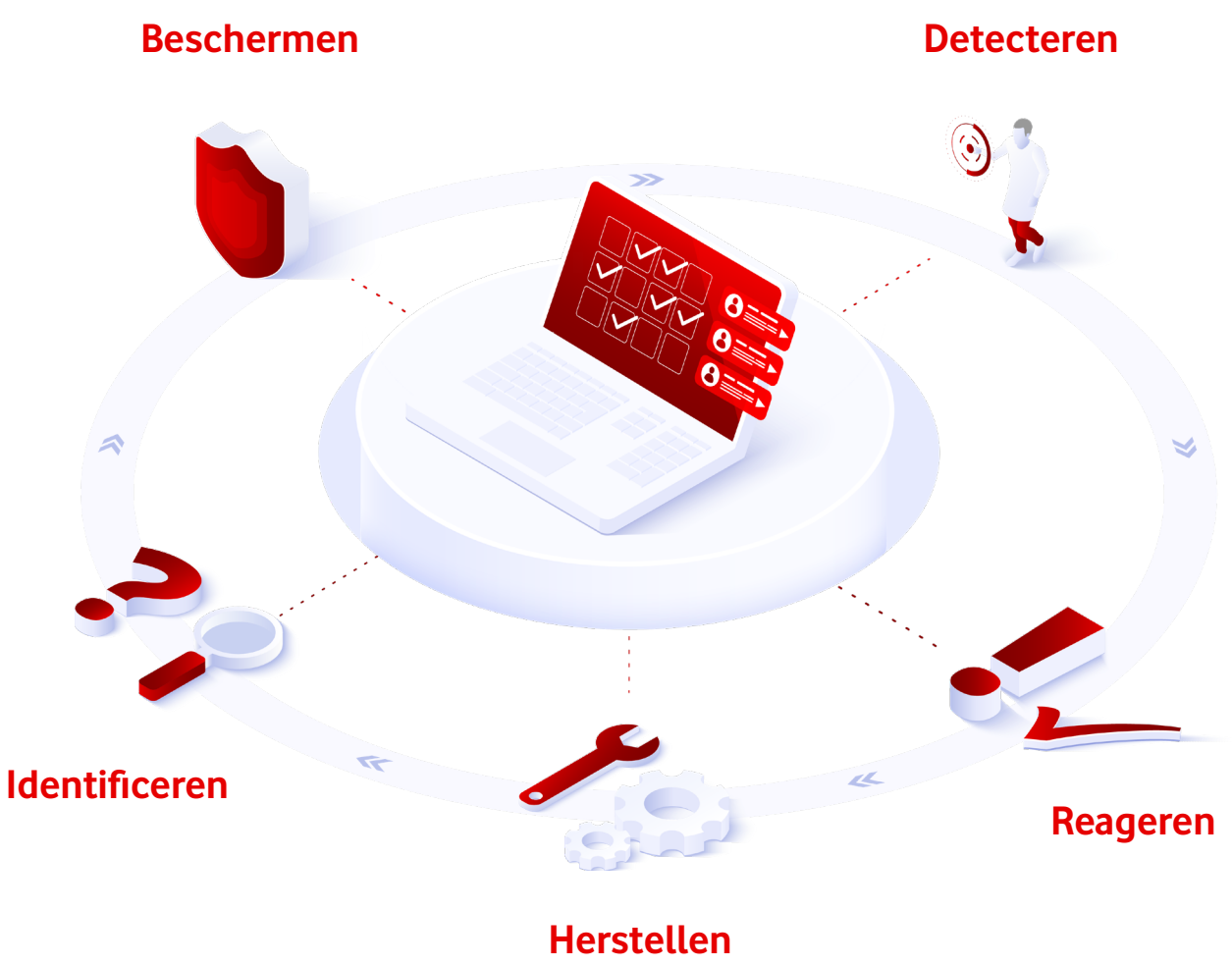
1. Ze zijn iets meer geneigd aandacht te geven aan externe risico’s.
2. Ze lopen voor op de rest als het gaat om cybersecurity.
3. Hun leidende positie blijkt uit het vertrouwen van hun stakeholders.
4. Ze zijn optimistisch over de kansen die cybersecurity hen kan bieden.

Waar kunt u op letten?

In vijf stappen naar betere beveiliging

Bij Vodafone Business hanteren we het NIST-model. Dit model biedt een goed framework voor uw cybersecurity. Het is ontwikkeld door het Amerikaanse National Institute of Standards and Technology en reikt bedrijven kaders aan voor het verminderen en beheren van cyberbeveiligingsrisico's. En ook nationale overheden gebruiken het model met succes, onder andere in Japan en Israël.

Het model biedt handvatten om bedreigingen en aanvallen te identificeren en organisaties te beschermen. En mocht het dan toch nog fout gaan: om te detecteren, te reageren en te herstellen. Dit zijn de vijf pijlers in het model. Handig als checklist, maar ook als conversation starters in een gesprek over uw cybersecurity.



1. Identificeren

Inzicht ontwikkelen om cybersecurity risico's te beheersen voor systemen, applicaties en data.

Doe een uitgebreide audit op alle apparaten en software binnen uw netwerk. Bedenk daarbij dat elk apparaat dat aan het internet wordt blootgesteld een mogelijke ingang is voor hackers. Blijf dus beducht op mogelijke risico's. Is alles goed geconfigureerd? Zijn de wachtwoorden sterk en willekeurig? En hoe zit het met uw leveranciers: hebben zij toegang tot uw gegevens? Zo ja, zijn hun systemen veilig? Slaan ze uw wachtwoorden ergens op in een willekeurig document?

2. Beschermen

Oplossingen waarmee u de dienstverlening van kritieke infrastructuur kunt garanderen.

Houd bijvoorbeeld uw apparaten en software up-to-date door altijd de nieuwste versies te installeren. Verwijder alles wat u niet gebruikt of schakel dit uit. En stel waar mogelijk multifactorauthenticatie in. Zorg bovendien dat u over een back-up beschikt van al uw gegevens. Zo voorkomt u dat u losgeld moet betalen. Back-up regelmatig en maak meerdere kopieën. En bewaar minimaal één back-up offline op een andere plek, zodat hackers deze niet kunnen wissen.

3. Detecteren

Hoe u effectief onregelmatigheden in cybersecurity signaleert.

Maak gebruik van diensten als een firewall, Intrusion Prevention System (IPS) en Intrusion Detection System (IDS) voor preventie en detectie. Deze diensten monitoren uw netwerk en waarschuwen u bij mogelijke inbreuken en ongebruikelijke activiteiten. Stuur al uw logs naar een centrale server en laat ze monitoren en checken op verdachte activiteiten.

4. Reageren

Welke acties te ondernemen bij een cybersecurityincident.

Bent u toch gehackt, dan is het belangrijk dat u er klaar voor bent. Door snel te reageren voorkomt u meer schade. Zodra u hoort over een inbreuk, verbreekt u de verbinding met het netwerk en volgt u de actiepunten in uw Incident Response plan. Haal de servers offline. Scan ze en controleer of er geen kwaadaardige code in de gegevens is verstopt. Update al uw systemen naar de laatste versie en verander alle wachtwoorden. Zorg dat u een betrouwbare partner heeft die gespecialiseerd is in cyberbeveiliging en die u bij een inbreuk kan helpen effectieve maatregelen te nemen.

5. Herstellen

De herstelplannen om getroffen systemen of diensten te repareren.

In deze laatste fase gaat het erom weer naar de toekomst te kijken. Wat is er nodig om de schade zo goed mogelijk te herstellen na een beveiligingsincident? Is er voldoende veerkracht in stelling gebracht om getroffen systemen, processen en diensten te kunnen repareren? Is er een plan van aanpak voor-het-geval-dat? Leg deze stappen ook weer vast in procedures.

Wij helpen FFtF bedrijven om het anders te doen.
Beter. Veiliger.

FFtF bedrijven geven prioriteit aan het opstellen van een bedrijfscontinuïteitsplan en ze vertrouwen erop. Hun houding speelt een grote rol om weerbaar en veerkrachtig te blijven – tijdens crisissen zoals de pandemie, dwars door periodes van prijsstijgingen en inflatie heen. En vooral: ze zijn beter bestand tegen cyberdreigingen.

FFtF bedrijven doen het beter in crises, bij nieuwe kansen en bedreigingen. Ze zijn veerkrachtiger en komen er sneller uit.

Vodafone Business als partner for progress

Cybersecurity is essentieel om uw bedrijf maximale veerkracht te geven. Vanuit Vodafone Business helpen we u daar graag bij. We bieden diensten en inzichten voor alle bedrijven, van startup tot multinational. We helpen als **partner for progress** om fit for the future te worden én te blijven. Door uw systemen veilig te houden en uw mensen, werkplekken, bedrijfsmiddelen en gegevens te beschermen. Daarbij werken we samen met toonaangevende bedrijven op het gebied van beveiligingsinformatie en met gerenommeerde leveranciers.

Misschien heeft u vragen. Twijfels? Plannen? Of wilt u weten hoe wij u kunnen helpen uw bedrijf weerbaarder te maken? Neem dan een kijkje op onze website. Of (vertrouw nooit een link) zoek op internet naar 'Vodafone NIST cyberbeveiliging'.

U bent natuurlijk ook van harte welkom om rechtstreeks contact op te nemen met een van onze accountmanagers (grootzakelijk) of een van onze business consultants (midden-kleinbedrijf).

vodafone
business

Together we can