

# Checklist Security: de basics



# Zorg dat je bedrijf niet stilvalt

**DDoS-aanvallen, phishing, malware, ransomware en virussen; het zijn allemaal digitale gevaren waar je liever niet mee te maken krijgt. Gelukkig kun je als ondernemer veel doen om deze buiten de deur te houden, zodat je je kunt richten op wat echt belangrijk is: je bedrijf laten groeien. Cyberincidenten komen helaas steeds vaker voor, zeker bij mkb-bedrijven, maar het goede nieuws is dat je met de juiste maatregelen de kans op een aanval aanzienlijk verkleint.**

Uit het rapport [Cybersecuritybeeld Nederland 2023](#) van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) blijkt dat de digitale dreiging groeit, zowel in omvang als in ernst. Toch betekent dit niet dat je machteloos bent. Integendeel, er zijn veel manieren om je bedrijf, data en medewerkers beter te beschermen. Wist je dat het mkb het vaakst wordt getroffen door malware en dat driekwart van de bedrijven al eens te maken heeft gehad met cybercriminaliteit? Dat klinkt





misschien zorgwekkend, maar met een paar simpele stappen kun je je bedrijf een stuk veiliger maken. Helaas blijkt uit hetzelfde rapport dat veel ondernemers nog niet voldoende basismaatregelen nemen. Dat is zonde, want deze maatregelen zijn eenvoudig toe te passen en kunnen veel ellende voorkomen.

Het is belangrijk te beseffen dat je organisatie, net als de rest van de maatschappij, steeds meer afhankelijk is van digitale middelen. Staat je IT stil, dan staat je bedrijf stil. Dat kan grote problemen en onverwachte kosten met zich meebrengen. Daarom is het essentieel om actie te ondernemen.

Het voorkomen van cybercriminaliteit vraagt om een combinatie van technologie en goed geïnformeerde medewerkers. Je medewerkers zijn je eerste verdedigingslinie en met de juiste kennis kunnen zij de grootste risico's vermijden. Vaak begint cybercriminaliteit met simpele fouten, zoals het klikken op verdachte links of het delen van wachtwoorden. Gelukkig zijn deze risico's goed te beheersen met de juiste IT-oplossingen, bewustwording en training.

In dit eBook delen we 15 'best practices' van onze security-experts, feitelijk de belangrijkste maatregelen die je kunt nemen om cybersecurity-incidenten te voorkomen of het risico erop sterk te verkleinen. Deel deze tips met je collega's, want samen maak je de sterkste veiligheidsketting. Hoe beter iedereen meedoet, hoe veiliger jullie bedrijf is.

# Op naar een cybersecure organisatie

**Je wilt serieus werk maken van de security in jouw organisatie. Goed bezig! We hebben ons best gedaan het zo praktisch mogelijk voor je te maken. Met deze 15 'best practice' tips van onze security-experts, weet je zeker dat je jouw bedrijf stukken veiliger maakt.**

## 1. Installeer software updates

Het up-to-date houden van software is een van de makkelijkste en meest effectieve manieren om je bedrijf te beschermen tegen cyberaanvallen. Installeer daarom altijd de nieuwste versies van je besturingssysteem, zoals Windows 11 of de nieuwste MacOS, en houd ook de software op je smartphone up-to-date. Deze updates bevatten vaak beveiligingspatches die bekende kwetsbaarheden verhelpen. Vergeet daarbij niet de firmware van je hardware zoals routers, printers, camera's of andere slimme apparaten. Door regelmatig te updaten, zorg je ervoor dat hackers minder kans krijgen om misbruik te maken van verouderde zwakke plekken. Zet automatische updates aan of plan tijdig een moment in om deze handmatig uit te voeren.

## 2. Gebruik een virusscanner

Op veel computers staat geen virusscanner of firewall. Hierdoor heeft schadelijke software vrij spel.

Controleer op alle apparaten binnen het netwerk of deze wel afdoende beschermd zijn. Draaien de computers op Windows 11, dan heb je Windows Defender. Je hoeft alleen te controleren of deze aan staat. Windows 11 heeft ook een ingebouwde firewall. Deze filtert ongewenst internetverkeer voordat het je pc bereikt en schade aanricht. Heb je Windows 11, controleer dan ook op deze firewall aan staat. Heb je een ander besturingssysteem, kijk dan welke het beste bij je past. Er zijn eenvoudige gratis firewalls maar ook uitgebreidere betaalde opties.



### 3. Beveilig je wifi-verbinding optimaal

Een goed beveiligde wifi-verbinding is essentieel voor een veilige werkomgeving. Zorg ervoor dat je altijd gebruikmaakt van een sterk versleutelde wifi-verbinding, zoals WPA2 met AES-encryptie. Kies daarnaast een uniek, sterk wachtwoord dat moeilijk te raden is. Een sterk wachtwoord bevat minimaal 8 (maar bij voorkeur 16 of meer) tekens en bestaat uit een combinatie van hoofdletters, kleine letters, cijfers en speciale tekens. Vermijd gemakkelijke wachtwoorden zoals "admin1" of "welkom" en gebruik in plaats daarvan bijvoorbeeld iets als "19Pl@n3!t99". Overweeg ook om een apart gastennetwerk aan te maken, zodat bezoekers veilig kunnen inloggen zonder toegang te krijgen tot je interne netwerk. Je kunt bovendien beperkingen instellen op dit gastennetwerk om het nog veiliger te maken.

#### GELIJK REGELEN

##### Extra Veilig Internet

Beveilig alle internetverkeer op de zaak tegen phishing en ransomware met één druk op de knop: Met Extra Veilig Internet van KPN EEN MKB zet je een web- en DNS filter aan op je vaste internetverbinding. Maak [een afspraak](#) met onze mkb-adviseurs voor meer informatie en advies.



### 4. Leer phishing mails en sites herkennen

Phishing-mails worden steeds overtuigender, zeker nu oplichters gebruik maken van AI-tools zoals ChatGPT. Maar je kunt jezelf beschermen door alert te zijn op verdachte kenmerken. Controleer altijd zorgvuldig de afzender en let op de domeinnaam van websites waar je naartoe wordt gestuurd. Een betrouwbaar domein leest van achteren naar voren duidelijk een bekende naam, b.v: "belastingdienst.nl" en niet iets als "belastingdienst.pi.nl". Twijfel je over de echtheid van een e-mail? Klik dan niet meteen op links, maar log rechtstreeks in via de officiële website van de organisatie. Neem de tijd om deze mails goed te controleren en deel deze informatie met je collega's, zodat iedereen waakzaam blijft.

### 5. Zet apparaten op veilige instellingen

Bij de installatie van nieuwe apparatuur is het belangrijk om direct de beveiligingsinstellingen te controleren en aan te passen. Begin met het wijzigen van standaard gebruikersnamen en wachtwoorden,



vooral bij apparaten zoals routers. Cybercriminelen weten vaak wat de standaardinloggegevens (zoals pincode '0000') zijn, dus het aanpassen daarvan is een eenvoudige manier om de veiligheid te verhogen. Neem daarnaast de tijd om de beveiligingsopties van alle nieuwe hardware en software door te lopen, en pas deze aan naar de meest veilige instellingen. Dit geldt ook voor persoonlijke apparaten van medewerkers die toegang hebben tot het bedrijfsnetwerk. Door deze stappen te volgen, maak je het cybercriminelen een stuk moeilijker om toegang te krijgen tot je netwerk en gegevens.

### 6. Stel 2FA (of MFA) in

Een eenvoudige en zeer effectieve manier om alle gebruikersaccounts in je organisatie extra te beveiligen is door tweefactorauthenticatie (2FA) in te schakelen. Met 2FA voeg je een extra laag beveiliging toe, waardoor hackers, zelfs als ze je wachtwoord hebben, niet zomaar toegang kunnen krijgen. Je vindt deze optie vaak onder de beveiligingsinstellingen van je profiel, zowel bij je zakelijke accounts als bij je persoonlijke e-mail, bank of social media. Het instellen van 2FA is een kleine moeite, maar maakt een groot verschil in het beschermen van je gegevens. Als werkgever kun je 2FA ook verplicht stellen, bijvoorbeeld voor Teams of Outlook.

## 7. Zorg voor rechtenbeheer

Een veilige ICT-omgeving begint met het goed regelen van de toegangsrechten voor je medewerkers. Geef mensen alleen toegang tot de gegevens en systemen die ze nodig hebben voor hun werk, en pas dit aan wanneer iemand van rol verandert of het bedrijf verlaat. Door een duidelijke schets te maken van je ICT-infrastructuur kun je beter bepalen wie toegang moet hebben tot welke informatie. Vergeet niet om ex-medewerkers ook te verwijderen uit apps, zoals WhatsApp-groepen en mailinglijsten. Dit helpt om je bedrijfsdata te beschermen en ongewenste toegang te voorkomen. Zorg ervoor dat je regelmatig deze machtigingen controleert en bijwerkt.

## 8. Gebruik geen openbare wifi

Dankzij laptops en smartphones werken we steeds vaker buiten de muren van het kantoor. Ook al worden databundels steeds groter, toch is het fijn om bij een klant, onderweg of in het buitenland gebruik te maken van wifi. Maar log je in op een openbaar wifi-netwerk zonder wachtwoord dan loop

je de kans dat iemand je dataverkeer aftapt of je nepsites voorschotelt. Denk aan een nagemaakte inlogpagina van LinkedIn. Log je hierop in, dan weet de cybercrimineel je inlognaam en wachtwoord. Maak daarom een VPN-verbinding, een soort digitale tunnel waar je internetverkeer goed beveiligd doorheen gaat. Om een VPN-verbinding op te zetten heb je een VPN-dienst nodig. Er zijn zowel betaalde als gratis VPN-diensten beschikbaar. Kijk goed naar de aanbieder of je deze kunt vertrouwen. Start met het lezen van ervaringen van andere gebruikers op het internet.

### GELIJK REGELEN

#### Extra Veilig Mobiel

Werken jij en je team veel op locatie? Dan is internetten met je mobiele hotspot de veiligste optie. Helemaal nu je [Extra Veilig Mobiel](#) aan kunt zetten op al je mobiele abonnementen. [Onze mkb-adviseurs](#) vertellen je graag hoe dat zit.



## 9. Wijs een verantwoordelijke aan

Een goede manier om je securitybeleid naar een hoger plan te trekken, is door iemand met technische kennis verantwoordelijk te maken voor de cybersecurity. Deze persoon kan ervoor zorgen dat zowel de technische als organisatorische beveiliging op orde is. Geef hem of haar de tijd en de middelen om dit goed uit te voeren. Heb je deze expertise niet in huis? Overweeg dan om een externe specialist in te schakelen. Als je werkt met privacygevoelige informatie, is het ook handig om iemand aan te stellen die verantwoordelijk is voor de gegevensbescherming volgens de AVG/GDPR-regelgeving. Dit is niet alleen verplicht, het zorgt er ook voor dat je bedrijf goed voorbereid is op de toekomst.

## 10. Geef awareness trainingen

Een klein foutje is snel gemaakt. Vaak zijn medewerkers zich niet bewust van het gevaar van onveilig digitaal gedrag. Regelmatig zien we dat bijvoorbeeld wachtwoorden op post-its op monitoren zijn geplakt of worden rondgemaild. Iedereen binnen het bedrijf zal daarom bewust moeten zijn van wat onveilig gedrag is. Een awareness training is een goed startpunt, maar geen eindpunt. Blijf elkaar regelmatig checken op goed gedrag en beloon dat.



Straf onveilig gedrag niet af, maar maak het bespreekbaar. Het is namelijk essentieel dat veiligheidsfouten zo snel mogelijk boven tafel komen. Er zijn diverse aanbieders van security awareness trainingen, via KPN EEN MKB kun je gebruik maken van de digitale trainingsomgeving van [Censornet](#). Tijdens dit soort trainingen komen onder andere de volgende punten aan bod:

- Gebruik het gezond verstand en klik niet snel door op websites en e-mails
- Kenmerken van een onveilige e-mail en wat ermee te doen als je er een krijgt
- Wat mag je wel en niet downloaden?
- Welke websites kun je wel en niet bezoeken?
- Gebruik niet overal hetzelfde wachtwoord
- Maak wachtwoorden niet voor de hand liggend
- Verander je wachtwoord regelmatig
- Houd wachtwoorden voor jezelf, deel ze niet met anderen
- Laat geen wachtwoorden slingeren, dus ook niet onder toetsenborden of op monitoren plakken
- Gebruik niet zomaar (onbekende) USB-sticks
- Vertrouwde instanties (banken, creditcardmaatschappijen) zullen nooit per e-mail of telefoon om je wachtwoord vragen
- Even weg van de computer? Log uit via Windows-toets + L of Control + Command + Q op een Apple device

## 11. Gebruik een passwordmanager

Het gebruik van sterke en unieke wachtwoorden vermindert je risico op cyberdreigingen drastisch. Hoe langer en unieker het wachtwoord hoe kleiner de kans dat je gehackt wordt. Wachtwoorden hebben bij voorkeur minimaal 16 tekens, en bestaan uit een combinatie van letters, cijfers en symbolen. Daarnaast gebruik je voor elke tool, website of account een ander wachtwoord. Omdat dit in de praktijk betekent dat mensen vaak wel meer dan 100 wachtwoorden moeten onthouden, is het gebruik van een wachtwoordmanager eigenlijk noodzakelijk geworden. Vaak zijn dit apps die op dekstop en mobiel worden ondersteund zodat inloggen ook nog eens veel makkelijker wordt. Gebruik uiteraard altijd een app of dienst die 2FA gebruikt, bijvoorbeeld de Password Manager van KPN.

### GELIJK REGELEN

#### KPN Cybersecurity voor MKB

Met [KPN Cybersecurity voor MKB](#) krijg jij 4 securitydiensten in één extra veilig pakket. Een wachtwoordmanager, security awareness training, endpoint protection van Acronis én Microsoft 365 back-up. [Advies nodig?](#)



## 12. Filter alle inkomende e-mail

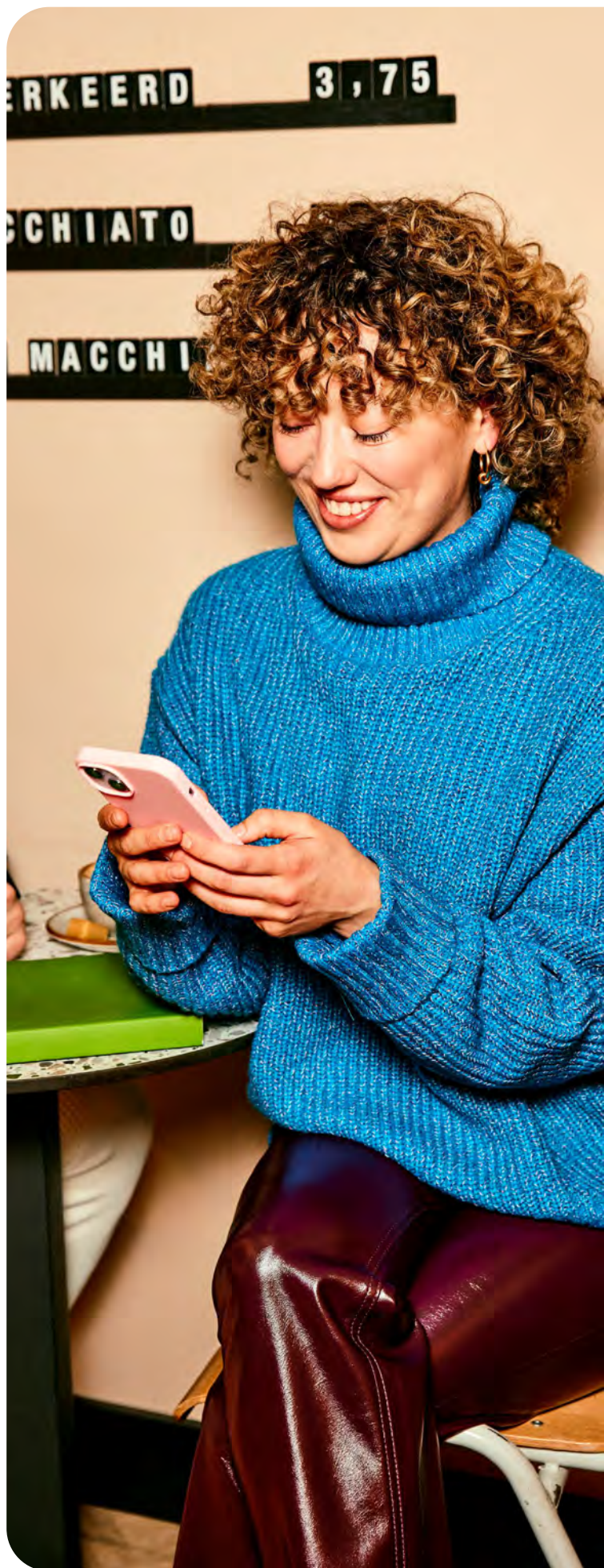
E-mail is nog steeds een van de meest gebruikte ingangen voor cybercriminelen. Door een effectief spamfilter te installeren op de e-mailclients van al je medewerkers, kun je een groot deel van phishing-pogingen en frauduleuze e-mails tegenhouden voordat ze de inbox bereiken. Hoewel sommige verdachte berichten gemakkelijk te herkennen zijn, kunnen anderen er overtuigend uitzien. Met een goed spamfilter worden de meeste risicovolle e-mails automatisch gefilterd, waardoor je bedrijf gelijk beter beschermd is.

## 13. Maak back-ups

Of het nu om brand, waterschade, of een ransomware-aanval gaat: door back-ups te maken voorkom je een hoop leed. Het komt vaak voor dat bedrijven vergeten om lokale servers en computers uit te rusten met een automatische back-up. Stel deze in en zorg ook dat de procedure om de back-ups terug te zetten voor iedereen duidelijk is. Op die manier kun je snel weer aan de slag na een probleem. Beperk je risico's door zowel een back-up 'in de cloud' als op een (andere) fysieke locatie te maken. Maar besef je dat ransomware ook cloud-omgevingen en externe harde schijven kan versleutelen. Denk daarom na over een back-up oplossing die ook back-ups van je cloud-omgeving (zoals Microsoft 365) kan maken, bijvoorbeeld [Acronis Cyber Protect](#).

## 14. Schakel endpoint protection in

Nu steeds meer medewerkers hybride werken in de cloud, heb je als IT'er te maken met een enorme wildgroei aan devices. Bijvoorbeeld omdat medewerkers hun mobiel of tablet zowel zakelijk als privé gebruiken. Dit is waar endpoint protection een oplossing kan bieden. Endpoint protection betekent letterlijk het beschermen van je 'endpoints' oftewel, alle hardware die in je bedrijf en op locatie gebruikt wordt. Het zorgt ervoor dat alle laptops, smartphones, tablets en andere devices voortdurend worden gecontroleerd op verdachte activiteiten en malware. Dit helpt niet alleen om virussen en ransomware buiten de deur te houden, maar beschermt ook tegen phishing-aanvallen en andere vormen van cybercriminaliteit. Door endpoint protection centraal te beheren, zorg je ervoor dat alle apparaten voorzien zijn van de laatste beveiligingsupdates en altijd optimaal beschermd zijn. Dit vermindert het risico op datalekken en andere beveiligingsincidenten aanzienlijk.



## 15. Maak een incident response plan

Een goed voorbereid bedrijf heeft altijd een plan klaarstaan voor als er iets misgaat, en dat geldt ook voor cyberincidenten. Een eenvoudig incident response plan helpt je om snel en effectief te reageren als zich een cybercalamiteit voordoet, zoals een hack, datalek of ransomware-aanval. Dit plan zorgt ervoor dat je direct weet welke stappen je moet nemen om de schade te beperken, de situatie onder controle te krijgen en zo snel mogelijk weer operationeel te zijn.

In een incident response plan moeten in elk geval de volgende elementen staan:

- **Contactpersonen:** Een lijst van wie verantwoordelijk is voor welke taken tijdens een cyberincident, inclusief contactgegevens van interne IT-medewerkers en externe specialisten.
- **Meldingsprocedures:** Een duidelijke beschrijving van hoe en aan wie een incident moet worden gemeld binnen het bedrijf.

- **Actiestappen:** Een stapsgewijze handleiding voor wat er onmiddellijk moet gebeuren bij een aanval, zoals het loskoppelen van geïnfecteerde apparaten van het netwerk, het informeren van het team, en het inschakelen van de IT-afdeling.
- **Herstelplan:** Hoe je het snelst gegevens herstelt, zoals het terugzetten van back-ups en het opnieuw opstarten van systemen.
- **Communicatieplan:** Hoe je zowel intern als extern communiceert over het incident, inclusief het informeren van klanten of toezichthouders als dat nodig is.

Als je een (eenvoudig) incident response plan op de plank hebt liggen neemt dat een hoop stress weg op het moment dat je met een cyberaanval te maken krijgt. Zorg dat je het plan ook fysiek ergens neerlegt en dat iedereen daarvan op de hoogte is. Hoe eerder je (de juiste) stappen onderneemt, hoe beter je een grote crisis kunt voorkomen.



# Beveilig je business met KPN EEN MKB

Cybersecurity, hybride werken en een snelle, stabiele verbinding zijn slechts enkele van de uitdagingen waarmee het mkb op dit moment te maken heeft. Een enorme uitdaging, waarvoor je niet altijd tijd hebt. Daarom bieden wij mkb-bedrijven een uitgebreid scala aan oplossingen én advies op ICT-gebied.

Wil je meer weten wat wij als KPN Zakelijk voor jouw mkb-bedrijf kunnen betekenen? Maak dan nu een afspraak met onze ICT-adviseurs:

→ [kpn.com/adviesgesprek](https://kpn.com/adviesgesprek)