

KPN EEN Security Checklist:

De basis voor jouw digitale bescherming



Introductie

Zorg dat je bedrijf niet stilvalt.

Cybergevaaren zoals DDoS-aanvallen, phishing, malware, ransomware en virussen zijn bedreigingen die je liever vermijdt. Gelukkig kun je als ondernemer veel doen om ze buiten de deur te houden, zodat jij je kunt concentreren op wat echt telt: je bedrijf laten groeien. Cyberincidenten komen steeds vaker voor, vooral bij mkb-bedrijven. Maar er is goed nieuws: met de juiste maatregelen verklein je de kans op een aanval aanzienlijk.

Volgens het rapport Cybersecuritybeeld Nederland 2023 van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) neemt de digitale dreiging toe in zowel omvang als ernst. Maar dat betekent niet dat je machteloos bent. Integendeel, er zijn volop mogelijkheden om je bedrijf, data en medewerkers beter te beschermen. Het mkb wordt vaakst getroffen door malware en driekwart van de bedrijven heeft al eens cybercriminaliteit ervaren. Dat klinkt misschien zorgelijk, maar met een paar simpele stappen kun je je bedrijf veel veiliger maken. Helaas blijkt dat veel ondernemers nog niet genoeg basismaatregelen nemen. Dat is jammer, want deze maatregelen zijn eenvoudig toe te passen en kunnen veel problemen voorkomen.

Je organisatie hangt steeds meer af van digitale middelen, net als de rest van de maatschappij. Als je communicatie oplossingen stoppen, sta je stil. Dit brengt zelfs mogelijke problemen en onverwachte kosten tot gevolg. Daarom is actie noodzakelijk.

Het bestrijden van cybercriminaliteit vraagt om technologie en goed geïnformeerde medewerkers. Zij zijn je eerste verdedigingslinie en met de juiste kennis kunnen ze grote risico's vermijden. Cybercriminaliteit begint vaak met simpele fouten, zoals klikken op verdachte links of wachtwoorden delen. Gelukkig zijn deze risico's met goede te beheren.

In dit e-book delen wij de beste tips met jou om cybersecurityincidenten te voorkomen of het risico aanzienlijk te verkleinen. Deel deze tips met je collega's, want samen vormen jullie de sterkste veiligheidsketting. Hoe beter iedereen meedoet, hoe veiliger jullie bedrijf is.



“De oplossingen van
Connipion zijn de oplossing
voor ITN Groep.”

Johan Niewenhuijse
Eigenaar ITN Groep

➡ [Klik & lees het verhaal](#)

Het aanbod

Op naar een cybersecure bedrijf.

Je wilt serieus werk maken van de security in jouw bedrijf, goed bezig! Met deze 'best practice' tips van onze support collega's, 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 en belsoftware, zowel op je computer als op je telefoon. 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 en een ingebouwde firewall. Je hoeft alleen te controleren of deze aanstaan. Heb je een ander besturingssysteem, kijk dan welke beveiligingsmogelijkheden er zijn.



**Meer weten?
Neem contact met ons op!**



0113 40 50 00



verkoop@conniption.nl

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.

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 standaard inloggegevens (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 en telefonie 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 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.

je de kans dat iemand je dataverkeer aftapt of je nepsites voorschotelt. Denk aan een nagmaakte 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.

8. Gebruik geen openbare wifi

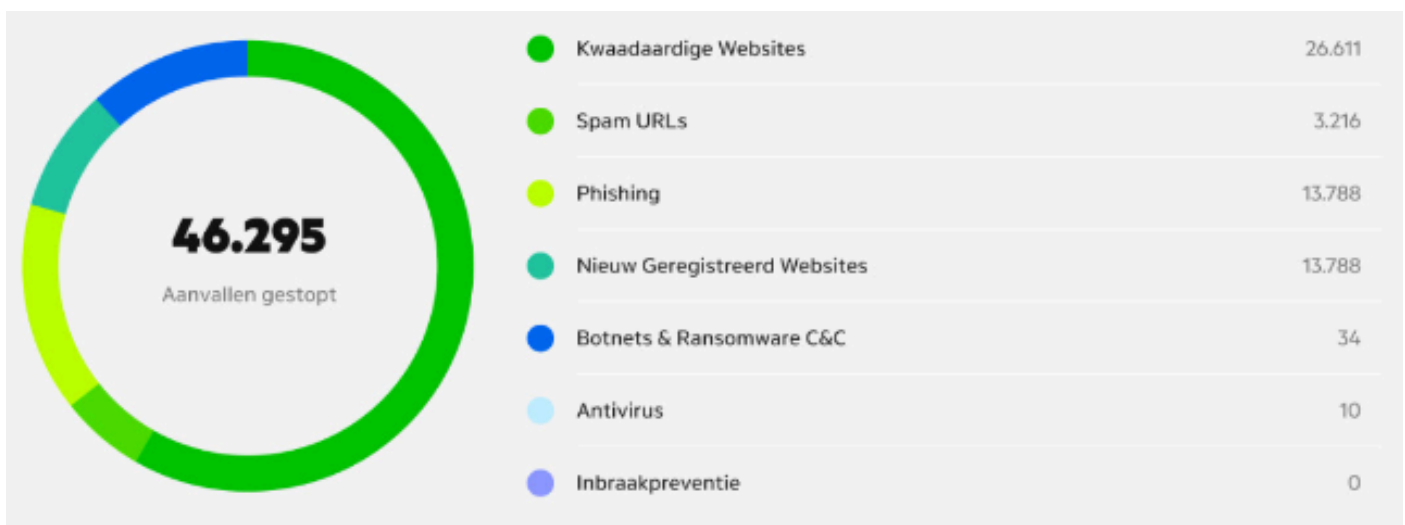
Dankzij laptops en smartphones werken we steeds vaker buiten de muren van het kantoor. Ook al worden databundels steeds groter, toch is het fijn om bij een klant, onderweg of in het buitenland gebruik te maken van wifi. Maar log je in op een openbaar wifi-netwerk zonder wachtwoord dan loop

Gelijk Regelen

KPN 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. [We 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.

10. 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.

11. 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.

12. 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 kan maken.

Meer weten? Neem contact met ons op!



0113 40 50 00



verkoop@conniption.nl

Beveilig je bedrijf met KPN EEN

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 draait bij ons alles om kwalitatieve gesprekken en betrouwbare communicatie.

We bieden telefonieoplossingen met soepele onboarding, integraties en uitstekende ondersteuning waardoor jouw klantinteracties altijd efficiënt en effectief verlopen.

Wil je meer weten wat wij voor jouw bedrijf kunnen betekenen? Kijk dan op onze website of neem contact met ons op via verkoop@connaption.nl of 0113 40 50 00.

