ICT-Basisveiligheid voor Ondernemers

4 aandachtspunten die vaak onderschat worden — en waarom ondersteuning belangrijk is

IQ ICT | ICT voor het MKB
Beveiligd. Verbonden. Ontzorgd. | De ICT Partner in Limburg.
Version : 2025.12.002

Als ondernemer wil je vooral doen waar je goed in bent: je bedrijf laten groeien, klanten helpen en vooruitkijken. ICT speelt daarin een steeds grotere rol, maar tegelijkertijd wordt het ook ingewikkelder. Veel ondernemers gaan ervan uit dat hun ICT “wel goed geregeld is”. Totdat er iets misgaat. Een e-mailaanval, een fout in een back-up, of een apparaat dat ongewenst toegang blijkt te hebben tot bedrijfsdata.

Dit E-book is geschreven om je een helder en inzichtelijk beeld te geven van de meest voorkomende valkuilen in de ICT-veiligheid van kleine en middelgrote bedrijven. Niet om je technisch te maken, maar juist om de risico’s begrijpelijk te maken. Je krijgt praktische inzichten die je helpen beter te begrijpen waar kwetsbaarheden kunnen ontstaan en wat je minimaal zou moeten weten als ondernemer.

We geven kleine adviezen en aandachtspunten, maar geen volledige oplossingen. En dat is bewust: moderne ICT-beveiliging is geen doe-het-zelfklus. De risico’s zijn te groot en de systemen te complex om zonder gericht advies en goede ondersteuning vol vertrouwen te kunnen werken.

Het doel van dit E-book is simpel:
Jou helpen ontdekken welke onderdelen van je ICT-omgeving extra aandacht verdienen zodat je bedrijf veilig, stabiel en toekomstbestendig blijft.

Mocht je tijdens het lezen merken dat sommige onderwerpen toch ingewikkelder zijn dan je dacht, weet dan dat je er niet alleen voor staat. IQ ICT helpt ondernemers dagelijks bij het veilig en zorgeloos maken van hun ICT-omgeving.

Natuurlijk kun je ons altijd bellen bij vragen. Wij zijn bereikbaar op 046 – 202 15 08 of via info@iqict.nl.

E-mailbeveiliging: meer dan alleen een spamfilter

Veel ondernemers gaan ervan uit dat hun e-mail automatisch goed beveiligd is. Er zit toch een spamfilter op? Helaas werkt het in de praktijk heel anders. Cybercriminelen worden steeds slimmer en weten precies hoe ze e-mails zo echt mogelijk kunnen laten lijken.

Goede e-mailbeveiliging gaat daarom veel verder dan het tegenhouden van ongewenste berichten. Het draait onder andere om:

- Zorgen dat niemand anders kan doen alsof hij jouw bedrijf is.
- Voorkomen dat medewerkers op misleidende berichten klikken.
- Zeker weten dat alleen de juiste mensen toegang hebben tot de mailbox.

Als dit niet goed geregeld is, kan iemand letterlijk een e-mail sturen *in jouw naam*, zonder dat jij daar iets van merkt.

Klein advies

Neem eens rustig een moment om te kijken hoe jouw e-mail nu beveiligd is. Standaardinstellingen zijn vaak niet genoeg. Vraag jezelf af: *Kan iemand anders zich voordoen als mijn bedrijf?* Als je dat niet zeker weet, is het verstandig om dit te laten controleren.

Praktijkvoorbeeld

Een ondernemer kreeg een telefoontje van een vaste klant:

“Ik heb de betaling overgemaakt naar het nieuwe rekeningnummer dat jullie hadden doorgegeven, maar klopt dat wel?”

De ondernemer schrok, er was helemaal geen nieuw rekeningnummer.
Wat was er gebeurd?

Een cybercrimineel had een e-mail verstuurd die sprekend leek op die van het bedrijf. Het logo, de naam, de toon… alles klopte. De klant had geen enkele reden om het niet te vertrouwen.

Omdat de e-mailbeveiliging niet goed was ingesteld, kon de crimineel zonder moeite doen alsof hij het bedrijf zelf was.

Het resultaat:

- De klant was geld kwijt.
- Het bedrijf moest het oplossen om de relatie goed te houden.
- De ondernemer had wekenlang stress en herstelwerk.
- En uiteindelijk bleken er meerdere zwakke plekken in de e-mailbeveiliging te zitten.

Dit soort situaties zijn helaas geen uitzondering — en vaak heeft de ondernemer pas door dat er iets mis is als het te laat is.

Waarom begeleiding nodig is

E-mail lijkt simpel, maar de beveiliging erachter is dat niet. De instellingen verschillen per leverancier, per domein en per type bedrijf. Eén klein foutje is genoeg om de deur op een kier te zetten voor criminelen.

Daarom is het verstandig om dit door een specialist te laten checken. Dat geeft rust, zekerheid en voorkomt problemen die veel geld en tijd kunnen kosten.

Back-ups: heb je ze… en werken ze ook echt?

Veel ondernemers denken dat ze “wel ergens een back-up hebben”. Maar in de praktijk blijkt dat het vaak niet zo simpel is. Een back-up is namelijk niet zomaar een kopietje van je bestanden. Er zijn allerlei manieren waarop een back-up gemaakt kan worden, verschillende plekken waar die kopieën staan, én verschillende manieren om ze weer terug te zetten als er iets misgaat.

En juist daar gaat het vaak mis:
Je merkt pas dat je back-up niet werkt op het moment dat je hem echt nodig hebt.

Dat is te laat.

Klein advies

Controleer eens of je back-ups *automatisch* gemaakt worden. Kijk ook of er meerdere momenten per dag of week worden bewaard. Want als er maar één kopie is, en die is kapot, heb je alsnog een probleem.

Praktijkvoorbeeld

Een klein bedrijf had een computercrash.
Geen probleem, dachten ze: *“Wij hebben een back-up”*

Maar toen ze alles probeerden terug te zetten, bleek dat:

- de back-up al maanden niet meer was bijgewerkt,
- sommige mappen nooit waren meegenomen,
- en dat niemand wist hoe de back-up eigenlijk moest worden teruggezet.

Het gevolg?

- Maanden aan bestanden waren weg,
- Klantinformatie moest opnieuw verzameld worden,
- Deadlines werden gemist,
- En de ondernemer moest noodgedwongen omzet missen om alles te herstellen.

De schrik was groot. Want ze dachten dat ze veilig waren — tot bleek dat hun back-up alleen in theorie bestond.

Dit soort situaties komen vaker voor dan je denkt. Niet omdat ondernemers slordig zijn, maar omdat back-ups gewoon veel ingewikkelder zijn dan ze lijken.

Waarom begeleiding nodig is

Een back-up is pas een echte back-up als:

- hij automatisch werkt,
- hij meerdere versies bewaart,
- en hij getest is. Dus gecontroleerd of je alles echt kunt terughalen.

Dat testen wordt vaak vergeten, terwijl het juist het belangrijkste onderdeel is.

Het goed inrichten en bewaken van back-ups is geen eenmalige klus. Het moet continu gecontroleerd worden. En dat is voor veel ondernemers simpelweg niet te doen naast de dagelijkse werkzaamheden.

Daarom is een expert die dit voor je beheert geen luxe, maar een geruststelling:
je weet zeker dat, als er iets gebeurt, jouw gegevens écht veilig zijn.

Apparaten en toegang: wie kan wat, en vanaf waar?

In veel bedrijven groeit het aantal apparaten dat toegang heeft tot bedrijfsinformatie sneller dan je doorhebt. Denk aan privételefoons, oude laptops die “nog wel even mee kunnen”, tablets, thuiscomputers of gedeelde accounts waar meerdere mensen op inloggen.

Het lijkt handig…
Maar het maakt je bedrijf ook kwetsbaar.

Als je niet precies weet wie toegang heeft en vanaf welk apparaat, dan heb je eigenlijk geen grip meer op je eigen bedrijfsdata. En één onveilig apparaat kan genoeg zijn om problemen te veroorzaken.

Klein advies

Maak eens een simpel lijstje:
Welke apparaten kunnen bij mijn e-mail, mijn documenten en mijn systemen?
Alleen al dat overzicht geeft verrassend veel duidelijkheid, en vaak ook de eerste schrik.

Praktijkvoorbeeld

Een medewerker verloor zijn eigen laptop welke hij zakelijk gebruikte in de trein.
Geen ramp, zou je denken. Maar die laptop had toegang tot bedrijfsdocumenten én tot de zakelijke e-mail.

Omdat er geen beveiliging op stond, kon de vinder:

- alle bedrijfsbestanden inzien,
- e-mails versturen vanuit het zakelijke account,

- zelfs toegang krijgen tot interne systemen.

Ondanks dat de medewerker het direct had gemeld, had het bedrijf geen beheer over de laptop waardoor hij niet op afstand geblokkeerd kon worden.

Gevolg:

- reputatieschade,
- paniek binnen het team,
- systemen moesten tijdelijk worden geblokkeerd,
- en het kostte dagen om alles te controleren en beveiligen.

Het hele probleem was te voorkomen geweest als alleen beveiligde, beheerste apparaten toegang hadden gehad.

Waarom begeleiding nodig is

Het beheren van wie toegang heeft tot wat, en op welke apparaten, is veel complexer dan het lijkt. Elk apparaat heeft zijn eigen instellingen, beveiligingsniveaus en risico's. En als je dat niet centraal beheert, ontstaat er langzaam maar zeker een onoverzichtelijke situatie.

Echte veiligheid betekent:

- dat alleen de juiste mensen bij de juiste informatie kunnen,
- dat apparaten veilig zijn en blijven,
- dat toegang kan worden ingetrokken met één klik als dat nodig is,
- en dat alles regelmatig wordt gecontroleerd.

Dat goed regelen vraagt kennis, aandacht en de juiste systemen. Voor de meeste ondernemers is dit geen dagelijks werk — maar voor een ICT-specialist wel.

Professionele ondersteuning geeft rust:
je weet zeker dat jouw gegevens alleen toegankelijk zijn voor wie je vertrouwt.

Infrastructuurveiligheid: wat gebeurt er eigenlijk achter de schermen?

Veel ondernemers richten zich vooral op laptops, telefoons en e-mail, maar vergeten dat daarachter een hele "onzichtbare laag" zit die alles met elkaar verbindt: je netwerk en infrastructuur. Denk aan je internetverbinding, router, wifi, kabels, kastjes, printers en andere apparaten die elkaar nodig hebben om te werken.

Omdat dit allemaal vaak verstopt staat in een meterkast of serverkast, lijkt het iets waar je nooit naar hoeft om te kijken. Maar juist in die verborgen laag ontstaan problemen die je als ondernemer pas merkt als het te laat is.

Infrastructuurveiligheid gaat bijvoorbeeld over:

- wie kan er op jouw wifi?
- staat je router nog ingesteld op oude, onveilige instellingen?
- zijn apparaten in het netwerk gescheiden (bijv. gasten vs. bedrijf)?
- zijn belangrijke apparaten überhaupt wel afgeschermd?

Veel ondernemers hebben hier geen idee van — en dat is niet vreemd. Het is namelijk niet zichtbaar… totdat er iets misgaat.

Klein advies

Kijk eens kritisch naar je bedrijfsnetwerk. Is het één groot geheel waar alles en iedereen op kan? Of zijn belangrijke onderdelen gescheiden? Alleen dit inzicht helpt al om beter te begrijpen waar risico's liggen.

Praktijkvoorbeeld

Een klein bedrijf kreeg te maken met vreemde vertragingen: internet dat uitviel, printers die niet werkten, bestanden die traag openden. Ze dachten dat het een tijdelijk probleem was.

Tot ze ontdekten dat een oud apparaat in het netwerk — ooit door iemand neergezet als "tijdelijke oplossing" — openstond voor iedereen. Ook voor mensen buiten het bedrijf, via de wifi.

Omdat dat apparaat geen beveiliging had, was het een zwakke plek in het hele netwerk. Een cybercrimineel had dit opgemerkt en scande het netwerk op zoek naar toegang. Het bedrijf had geluk: er was nog geen schade, maar het had makkelijk anders kunnen aflopen.

Het probleem was simpel: **het netwerk was nooit goed ingericht of gecontroleerd.**
Alle apparaten zaten in één grote groep, zonder scheiding of beveiligingsregels.

Waarom begeleiding nodig is

Een veilige infrastructuur is als een goed slotenplan in een bedrijfspand. Niet iedereen hoeft overal naar binnen te kunnen, en niet elke deur hoeft open te staan.

Maar in ICT-land ziet elke organisatie er anders uit:

- verschillende routers
- verschillende wifi-netwerken
- apparaten die oud of nieuw door elkaar gebruikt worden
- uitbreidingen die "even snel" zijn gedaan
- instellingen die jarenlang niet nagekeken zijn

Het vraagt specialistische kennis om:

- zwakke plekken te herkennen,
- het netwerk logisch op te bouwen,

- en ervoor te zorgen dat alles veilig blijft terwijl je bedrijf groeit.

Als dit goed geregeld is, merk je het eigenlijk niet en dat is precies de bedoeling. Maar als het níet goed geregeld is, merk je het pas als het te laat is.

Professionele controle geeft rust:
je weet zeker dat je netwerk veilig is, ook al zie je het zelf niet.

ICT-veiligheid is misschien niet het eerste waar je dagelijks mee bezig bent, maar het speelt een grote rol in de continuïteit én betrouwbaarheid van je bedrijf. Met de inzichten uit dit boek heb je nu een duidelijker beeld van waar het vaak misgaat en waarom deze onderwerpen belangrijker zijn dan veel ondernemers denken.

Je hoeft dit allemaal niet alleen te doen. ICT-beveiliging is complex, verandert snel en vraagt om continue aandacht. Het is logisch dat je als ondernemer niet elk detail kunt bijhouden. Je hebt al genoeg andere verantwoordelijkheden.

Bij IQ ICT helpen wij bedrijven om hun ICT overzichtelijk, veilig en zorgeloos te maken. We geloven dat ondernemers moeten kunnen vertrouwen op een stabiele digitale basis, zonder gedoe en zonder verrassingen. Daarom bieden we duidelijke uitleg, praktische oplossingen en ondersteuning die écht aansluit bij de manier waarop jouw organisatie werkt. Geen moeilijke taal, geen onnodige complexiteit. Onze klanten kiezen voor ons omdat ze zeker willen weten dat hun ICT in veilige handen is.

IQ ICT is **aangesloten bij ICTWaarborg**, de brancheorganisatie die staat voor betrouwbaarheid, kwaliteit en transparantie binnen de ICT-sector. Daarnaast zijn wij **officieel geregistreerd bij de Autoriteit Consument & Markt (ACM)**, wat betekent dat we voldoen aan de wettelijke eisen rondom eerlijke dienstverlening en communicatie.

Ook zijn we **gecertificeerd partner van ESET**, één van de meest gerespecteerde beveiligingsleveranciers ter wereld. Hierdoor kunnen we hoogwaardige beveiligingsoplossingen leveren én beheren, altijd up-to-date en afgestemd op jouw bedrijf.

Kortom: met IQ ICT kies je voor een partner die weet wat er nodig is om jouw ICT-omgeving écht veilig, stabiel en toekomstbestendig te maken en die dat doet volgens heldere afspraken, erkende standaarden en bewezen kwaliteit. Wil je weten hoe jouw ICT-omgeving er écht voor staat?
We kijken graag vrijblijvend met je mee. In een kort gesprek brengen we de belangrijkste risico's in kaart en krijg je direct praktische handvatten om mee verder te gaan.

Je kunt ons bereiken via onderstaande contactgegevens.

Bryan Veraart

IQ ICT

046 – 202 15 08

info@iqict.nl

www.iqict.nl