ZEVENTIEN DAGEN EERDER

Cybersecurity voor het Nederlandse mkb

inclusief NIS2 en de Cyberbeveiligingswet

Wilco Foppen

Zeventien dagen eerder

Cybersecurity voor het Nederlandse mkb

Auteur & Coverontwerp: Wilco Foppen

ISBN: 9789465542911

Uitgave: FoppenSecurity, augustus 2026

Eerste druk

Contact en meer informatie: foppensecurity.nl

De in dit boek beschreven onderneming Steenwold Transport & Warehousing en de daarin voorkomende personen zijn fictief. Dit boek is met zorg samengesteld maar biedt geen juridisch advies; voor de vraag wat wet- en regelgeving in een concrete situatie betekent, is de wettekst leidend.

Inhoud

Voorwoord

Bij de meeste ondernemers is het al gebeurd. Zo gewoon dat het niet opviel.

Meestal is het een mail. Van een opdrachtgever waar je al jaren voor werkt, met in de bijlage een vragenlijst van veertig vragen over informatiebeveiliging. Of het is een telefoontje van een collega-ondernemer die vertelt dat ze een week plat hebben gelegen. Of het is een zin die iemand op een verjaardag laat vallen over een nieuwe wet, waarna je 's avonds gaat zoeken en na twintig minuten meer vragen hebt dan antwoorden.

Wat er dan gebeurt, is bijna altijd hetzelfde. Je komt terecht in een wereld die niet voor jou is gemaakt. Adviesbureaus die beginnen met een risicoanalyse van zes weken. Normenkaders met honderdveertien beheersmaatregelen. Aanbieders die je vertellen dat je in gevaar bent en toevallig ook precies het product hebben dat je nodig hebt. Alles is geschreven voor organisaties die twintig keer zo groot zijn als de jouwe, met een securityafdeling die jij niet hebt en niet wilt.

En ergens in dat geweld raakt de eenvoudige vraag zoek waar het je eigenlijk om ging: *wat is hier nu werkelijk aan de hand, en wat moet ik ermee?*

Dit boek probeert die vraag te beantwoorden. Het is geschreven voor de eigenaar of manager van een bedrijf van tien tot tweehonderdvijftig medewerkers, die niet uit de IT komt, die geen zin heeft in jargon, maar die wel wil begrijpen waar hij aan toe is.

Wat het niet is, is een invulboek. Er staan geen formulieren in, geen sjablonen en geen afvinklijsten. Dat is een bewuste keuze, en het is de belangrijkste keuze in dit boek.

Het mkb is namelijk verzadigd van checklists. Er zijn er honderden, ze zijn vrijwel allemaal gratis, en ze werken niet. Niet omdat ze verkeerd zijn, maar omdat een vinkje zetten iets anders is dan een besluit nemen — en omdat niemand een maatregel volhoudt waarvan hij niet begrijpt waarom hij er is. Wie op een lijst leest dat hij drie back-ups moet hebben, maakt drie back-ups op één plek. Wie begrijpt dat aanvallers wekenlang binnen zitten en de back-up als eerste opzoeken, doet het anders. Dat verschil is niet met een formulier over te brengen. Wel met een verhaal.

Daarom loopt er door dit boek één bedrijf mee. Steenwold Transport & Warehousing bestaat niet — het is samengesteld uit situaties die zich in Nederland dagelijks voordoen — maar alles wat hen overkomt, is echt gebeurd bij bedrijven zoals dat van jou. In het eerste hoofdstuk zie je wat er misgaat. In de hoofdstukken daarna zie je per onderwerp waar het werkelijk fout ging, en hoe het anders had gekund.

Aan het eind van dit boek heb je geen ingevuld beleid en geen certificaat. Je weet wat aan een beleid of investering vooraf gaat: een helder beeld van je eigen situatie. Welk van de vier scenario's jou bedreigt. Wat je al goed doet zonder het te weten. Waar je gat zit. En wat de eerstvolgende zinnige stap is — zelf doen, bij je IT-partij neerleggen, of er iemand bij halen.

Nog twee opmerkingen vooraf.

Er wordt in dit vakgebied veel met angst verkocht. Dat werkt kort, en het levert slecht beleid op, omdat angst mensen aanzet tot het kopen van producten in plaats van het maken van keuzes. In dit boek staan daarom geen schrikcijfers en geen rampscenario's die verder gaan dan wat er werkelijk gebeurt. Dat is niet nodig ook: de nuchtere werkelijkheid is dringend genoeg.

En er loopt één woord door alle hoofdstukken heen: **aantoonbaarheid**. Het gaat er niet alleen om dát je iets doet, maar dat je kunt laten zien dat en wanneer je het hebt besloten, uitgevoerd en herzien. Dat klinkt als bureaucratie maar is het niet. Het is het verschil tussen veilig zijn en veilig zijn met bewijs — en dat tweede is wat opdrachten oplevert, wat verzekeraars willen zien, en wat sinds 15 augustus 2026 ook de wet van een deel van de Nederlandse bedrijven vraagt.

Over de peildatum. Dit boek is gepubliceerd in augustus 2026. De Cyberbeveiligingswet is dan in werking, maar de uitwerking eromheen is nog volop in beweging: de regelingen per sector, de drempels voor de meldplicht, het handhavingsbeleid van de toezichthouders. Waar dat speelt, staat het in dit boek erbij, met de plek waar je de actuele stand vindt. Achterin staan die vindplaatsen bij elkaar. Een boek kan uitleggen hoe iets werkt en waar je moet kijken; het kan niet garanderen wat er vandaag geldt.

Tot slot iets wat in de meeste boeken over dit onderwerp te weinig aandacht krijgt: dit is een oplosbaar probleem. Niet volledig — er bestaat geen bedrijf dat niets kan overkomen, en wie jou dat verkoopt, verkoopt je iets anders. Maar het overgrote deel van wat er misgaat, wordt tegengehouden door een handjevol maatregelen die geen securityafdeling vereisen en die meestal geen geld kosten.

Het begint met begrijpen waarom ze werken.

Leeswijzer

Dit boek bestaat uit vier delen.

Deel I legt uit waarom dit jou aangaat. Wat er in de praktijk misgaat en waarom aanvallers uitgerekend bij jou uitkomen, wat de Cyberbeveiligingswet van organisaties vraagt, hoe die eisen via je opdrachtgevers bij je terechtkomen — ook als de wet niet voor jou geldt — wat aantoonbaarheid betekent, en hoe je bepaalt waar je begint. Lees dit deel achter elkaar door; het is de onderbouwing van alles wat volgt.

Deel II is de kern. Dertien hoofdstukken, elk over één onderwerp: beleid, verantwoordelijkheden, informatie en waarde, toegang, gedrag, back-ups, incidenten, leveranciers, persoonsgegevens, bewustzijn, overzicht, prioriteiten en verantwoording. Per onderwerp lees je wat het inhoudt, waar het vandaan komt, waarom het werkt zoals het werkt, en waarom het in de praktijk zo vaak misgaat. Steenwold komt in elk hoofdstuk terug. Vaktermen worden genoemd en meteen vertaald: je hoeft ze niet te kennen of meteen te begrijpen, maar je legt het boek weg met de woordenschat om met je IT-partij of je opdrachtgever een gesprek op niveau te voeren.

Deel III gaat over volhouden — het onderdeel waar de meeste organisaties alsnog stranden. Over het ritme van een jaar, over oefenen, over bewijs bewaren, en over de vraag of je door wilt naar een certificaat en wat dat werkelijk kost.

Achterin staan een begrippenlijst, de vindplaatsen voor actuele regelgeving, en een bronvermelding.

De hoofdstukken van Deel II zijn zelfstandig te lezen en de volgorde is niet dwingend. Wel logisch: beleid en verantwoordelijkheden komen eerst, omdat de rest daarop teruggrijpt.

Heb je haast — een vragenlijst met een deadline — lees dan eerst hoofdstuk 3 en 4. Daar staat wat er werkelijk van je gevraagd wordt en waarom. Valt je organisatie onder de Cyberbeveiligingswet, begin dan bij hoofdstuk 2: daar staat het enige in dit hele boek waar een datum aan hangt.

Wat dit boek niet is

Het is geen juridisch advies. Het legt wetgeving uit in gewone taal, en dat betekent onvermijdelijk dat nuance verloren gaat. Voor de vraag of jouw specifieke organisatie onder de Cyberbeveiligingswet valt, en zeker voor de vraag wat een concrete regel in jouw situatie betekent, is de wettekst leidend en een jurist verstandig.

Het is ook geen technische handleiding. Je leest waarom je tweestapsverificatie aanzet en op welke systemen, niet welke knop je in welk menu indrukt. Die knoppen verschillen per leverancier en veranderen sneller dan een boek kan bijhouden.

En het is geen normenkader. Wie ISO 27001 of het NIS2 Supply Chain-certificaat wil halen, heeft de officiële norm nodig en waarschijnlijk begeleiding. Dit boek brengt je tot dicht bij het punt waar zo'n traject begint, en hoofdstuk 22 legt uit wat de routes zijn en wat ze kosten.

Over de casus

Steenwold Transport & Warehousing is een verzonnen onderneming. De naam, de personen en het bedrijf berusten niet op een bestaande organisatie; de gebeurtenissen zijn samengesteld uit meerdere praktijksituaties. Overeenkomsten met een bestaand bedrijf berusten op toeval — en op het ongemakkelijke feit dat deze verhalen overal hetzelfde verlopen.

DEEL I

Waarom dit jou aangaat

Wat er in de praktijk misgaat en waarom aanvallers uitgerekend bij jou uitkomen, wat de Cyberbeveiligingswet vraagt, hoe die eisen via je opdrachtgevers bij je terechtkomen, wat aantoonbaarheid betekent, en hoe je bepaalt waar je begint.

1 De dinsdag van Steenwold

Het begon niet met een alarm. Het begon met een planning die niet openging.

Dinsdag 2 maart, kwart over zeven. Gerben Mulder, transportplanner bij Steenwold Transport & Warehousing in Emmen, klikte op het bestand waar hij elke ochtend mee begint en kreeg een foutmelding die hij niet kende. Hij deed wat iedereen doet: hij probeerde het nog een keer. Toen liep hij naar het bureau ernaast.

Bij zijn collega ging het ook niet.

Om tien voor half acht belde de eerste chauffeur, die op de oprit van het distributiecentrum in Groningen stond. Hij had geen ritopdracht op zijn boordcomputer, wist niet welke pallets hij mee moest nemen, en had een portier voor zich die hem niet naar binnen liet zonder papieren. Om acht uur belde de tweede. Om vijf over acht liep Marieke Steenwold, directeur en kleindochter van de oprichter, de expeditie op met de mededeling dat niemand meer iets moest opstarten.

Op elk scherm in het gebouw stond op dat moment dezelfde tekst. Engels, zakelijk, bijna beleefd. De bestanden waren versleuteld. Er was een adres om naar te mailen. Er stond een bedrag bij, in bitcoin, met een omrekening naar euro's erachter alsof het een offerte was.

Steenwold Transport & Warehousing bestaat sinds 1974, heeft achtenveertig medewerkers, drieëntwintig trekkers en een loods van vierduizend vierkante meter aan de rand van het bedrijventerrein. Het rijdt door heel Noord- en Oost-Nederland voor een regionale voedselproducent, voor een groothandel in medische hulpmiddelen en voor een handvol vaste industriële klanten.

Het had nog nooit iets meegemaakt wat ook maar in de buurt kwam van wat er die ochtend plaatsvond.

Wat er die dag gebeurde

De eerste twee uur gingen op aan bellen.

De IT-partij — een bedrijf uit Assen waar Steenwold al elf jaar mee werkt en dat "het beheer doet" — kon niet meteen komen. De accountmanager was vriendelijk, hun engineer zat bij een andere klant, ze zouden er om elf uur zijn. Marieke belde haar broer, die medevennoot is. Haar broer belde de accountant. De accountant belde terug met de vraag of de administratie ook plat lag, want er moest die week loon betaald worden.

De administratie lag ook plat.

Om half elf kwam de vraag die in elk van deze situaties komt, en die altijd door iemand wordt gesteld op een toon alsof het de oplossing is: *we hebben toch back-ups?*

Ze hadden back-ups. Er stond een NAS in de meterkast van het kantoorgedeelte — een netwerkschijf waar elke nacht alles naartoe werd gekopieerd. Dat was jaren geleden zo ingericht en het had altijd gewerkt. Niemand had er ooit iets van teruggezet, want dat was nooit nodig geweest.

De NAS was ook versleuteld. Hij hing aan hetzelfde netwerk, met dezelfde inloggegevens, en de software die het kantoor had platgelegd had hem gevonden zoals hij alles vond: door te kijken wat er bereikbaar was.

Om twaalf uur zat Marieke Steenwold in een bespreekkamer met de vraag wie de voedselproducent ging bellen. Die klant had die week zesentwintig ritten ingepland, waaronder gekoeld transport dat niet kon wachten. Om twee uur belde de voedselproducent zelf, want er

stonden trailers stil die geladen hadden moeten zijn. Om drie uur vroeg iemand van de administratie hardop of dit niet ergens gemeld moest worden — er stonden immers persoonsgegevens in die systemen. Niemand wist aan wie. Niemand wist binnen hoeveel tijd. Iemand zei dat het "iets van tweeënzeventig uur" was, wat toevallig klopte, maar niemand wist waarvoor precies.

Om zes uur die avond was er niets hersteld.

Het zou nog negen dagen duren voordat Steenwold weer normaal draaide.

Wat er niet gebeurde

Het interessante aan het verhaal van Steenwold is niet wat er op die dinsdag gebeurde. Het is wat er in de zeventien dagen dáárvoor gebeurde, en wat niemand zag.

Zeventien dagen eerder had Sanne Bergsma een mail geopend op het account dat bij Steenwold op haar naam stond, die eruitzag als een bericht van een leverancier waar Steenwold al jaren mee werkt. Er zat een link in naar een vrachtbrief. De pagina achter die link vroeg haar om in te loggen met haar bedrijfsaccount. Dat deed ze. De pagina gaf een foutmelding, ze probeerde het nog eens, het lukte weer niet, ze haalde haar schouders op en ging iets anders doen.

Ze heeft er nooit meer aan gedacht. Er was ook niets gebeurd. Geen virusmelding, geen waarschuwing, geen zichtbaar gevolg.

Wat er wel gebeurde, was dat iemand anders vanaf dat moment kon inloggen op haar account. Niet door iets te kraken — gewoon, met haar gebruikersnaam en haar wachtwoord, via de voordeur. Twee dagen later logde diegene in vanuit een ander land, en omdat Steenwold geen tweestapsverificatie had, was er niets wat dat tegenhield.

De weken daarna werd er gekeken. Waar staan de bestanden. Wie heeft beheerrechten. Waar staat de back-up. Wat voor bedrijf is dit eigenlijk, en hoeveel zou het kunnen betalen. Ergens in die periode is er een kopie van een deel van de gegevens naar buiten gehaald — dat bleek pas veel later, uit het onderzoek.

Pas toen alles in kaart was, ging de versleuteling aan. Op een dinsdagnacht, want dan is de kans het kleinst dat iemand het in de gaten heeft voordat het klaar is.

Dit is het patroon, en het is belangrijk om het goed te begrijpen, want bijna iedereen heeft het beeld verkeerd om. Mensen denken dat een aanval een moment is: er wordt op een knop gedrukt, er gaat iets kapot. In werkelijkheid is de versleuteling het eindpunt van een proces dat weken duurt. Er is al die tijd iemand binnen geweest. Er zijn al die tijd sporen geweest.

En dat is tegelijk het hoopvolle deel van het verhaal. Een aanval die weken duurt, is een aanval die je op tientallen plekken had kunnen stoppen.

Waarom uitgerekend Steenwold

De eerste vraag die Marieke Steenwold aan de specialist stelde die uiteindelijk het onderzoek deed, was de vraag die iedereen stelt: *waarom wij?*

Het antwoord beviel haar niet, want het antwoord was: om geen enkele reden.

Er is niet naar Steenwold Transport & Warehousing gezocht. Er is niet besloten dat een transportbedrijf in Emmen een interessant doelwit was. Er is helemaal niet over Steenwold nagedacht — niet totdat het account van Sanne Bergsma op een lijst terechtkwam en iemand constateerde dat het werkte.

Dit is het punt waarop het klassieke mkb-argument ineenzakt. "Wij zijn te klein en te oninteressant" was vijftien jaar geleden een redelijke inschatting, toen een aanval nog handwerk was en iemand zich eerst in een doelwit moest verdiepen voordat hij eraan begon. Bij die economie is een bedrijf met achtenveertig man inderdaad de moeite niet.

Maar de economie is veranderd. Aanvallen zijn geïndustrialiseerd. Er wordt continu, geautomatiseerd, over het hele internet gescand: op systemen met een bekend lek, op wachtwoorden die ergens anders zijn gelekt en die hier toevallig ook werken, op mailadressen die te koop zijn per tienduizend. Er zijn partijen die niets anders doen dan toegang verkopen — zij komen binnen en verkopen die toegang door aan een andere partij die de ransomware uitrolt. Er is een HR-afdeling, er is klantenservice, er zijn onderhandelaars.

In die economie is de vraag niet of jij interessant bent. De vraag is of jouw deur openstond toen de scanner langsliep. Of die deur bij een multinational hoorde of bij een transporteur met achtenveertig man, maakt niet uit, want de scan kostte hetzelfde: bijna niets.

Sterker nog, en dit is de onaangename waarheid: een bedrijf als Steenwold is in één opzicht een béter doelwit dan een groot concern. Het betaalt vaker. Een multinational heeft juristen, verzekeraars, een crisisteam en de financiële adem om drie weken uit de lucht te zijn. Steenwold heeft dat niet. Steenwold kan geen negen dagen zonder planning en facturatie zonder dat het pijn doet tot in de botten. Voor Marieke Steenwold was betalen op dag drie een serieuze overweging — en de mensen aan de andere kant weten dat precies. Hun prijsstelling is erop afgestemd.

Er is nog een reden waarom Steenwold interessant was, en die is de laatste jaren belangrijker geworden dan alle andere. Steenwold zit in een keten. Steenwold heeft toegang tot het bestelportaal van de

groothandel in medische hulpmiddelen. Steenwold stuurt facturen naar opdrachtgevers die tien keer zo groot zijn. Steenwold heeft toegangspassen voor distributiecentra, laadadressen, planningen, en een vaste beveiligde verbinding met het systeem van een klant — technisch ook wel VPN genoemd, een soort afgeschermde verbinding over het internet.

Wie bij Steenwold binnenkomt, komt niet alleen bij Steenwold binnen. Dat maakt een klein bedrijf geen klein doelwit, maar een ingang. Hoofdstuk 3 gaat daar helemaal over, en het is het hoofdstuk dat verklaart waarom je opdrachtgevers je de laatste tijd vragenlijsten sturen.

De vier verhalen die zich blijven herhalen

Wat Steenwold overkwam is één van vier scenario's. Niet omdat er niets anders bestaat — er zijn aanvalsvormen die zeldzaam, ingenieus of op maat gemaakt zijn — maar omdat vier patronen samen vrijwel alles verklaren wat een Nederlands mkb-bedrijf in de praktijk overkomt. Ze keren terug in wisselende volgorde en met wisselende schade, en ze lopen regelmatig in elkaar over.

Het eerste is het scenario van de nepmail. Iemand krijgt een bericht dat hem verleidt tot klikken, inloggen, een bijlage openen of een code doorgeven. Het beeld dat de meeste mensen daarbij hebben — de kromme vertaling, de Nigeriaanse prins — is inmiddels een museumstuk. Wat er nu binnenkomt lijkt op een Teams-uitnodiging van een collega, op een factuurherinnering van een leverancier waar je echt zaken mee doet, op een bericht van je eigen boekhoudpakket met het juiste logo en een afzender die op het eerste gezicht klopt. Sinds tekst genereren met AI voor iedereen toegankelijk is, is het advies "je herkent het aan de taalfouten" definitief onbruikbaar geworden.

Dit scenario is zelden het einde. Het is bijna altijd het begin — zoals bij Steenwold, waar het zeventien dagen voor de versleuteling lag en waar niemand het ooit gemeld heeft omdat er niets leek te gebeuren.

Het tweede is het scenario van Steenwold zelf: gijzelsoftware. De bestanden gaan op slot, er wordt betaald voor de sleutel of er wordt niet betaald en alles wordt opnieuw opgebouwd. Wat mensen daarbij structureel onderschatten, is de tweede helft van de chantage. De aanvaller heeft vóór het versleutelen al een kopie van de gegevens naar buiten gehaald. Betaal je niet, dan komt die kopie online. Bij Steenwold ging het om personeelsdossiers en om laad- en losadressen en contactgegevens van klanten. Dat betekent dat zelfs een perfecte back-up het probleem niet helemaal wegneemt — en dat het gesprek met de opdrachtgever daardoor een heel ander gesprek wordt.

Het derde scenario ziet er van buiten uit alsof er niets aan de hand is. Er wordt niets versleuteld, er valt niets uit, er is geen enkel alarm. Er verdwijnt alleen geld. Iemand leest maandenlang mee in een mailbox — vaak die van de administratie of van een projectleider — en leert de lopende projecten kennen, de bedragen, de toon waarop hier met elkaar wordt gemaild. En dan, op het juiste moment in een project, gaat er een bericht naar de klant: *let op, ons rekeningnummer is gewijzigd*. De klant betaalt keurig. Naar de verkeerde rekening.

Het werkt net zo goed andersom: jouw eigen administratie krijgt een nieuw IBAN van een leverancier. En het werkt in een variant waar helemaal geen inbraak aan te pas komt, waarin de financieel medewerker op vrijdagmiddag een appje krijgt dat van de directeur lijkt te komen — spoed, vertrouwelijk, een overname waar nog niemand van mag weten, kun jij dit even overmaken.

Van alle scenario's is dit degene waar de minste techniek en de meeste psychologie bij komt kijken. Het is daarmee ook het scenario dat het goedkoopst te stoppen is: één afspraak, dat je een wijziging van rekeningnummer altijd bevestigt via een ander kanaal met een telefoonnummer dat je zelf opzoekt, haalt het grootste deel van het risico weg. Het kost niets. Het wordt bijna nergens gedaan.

Het vierde scenario is het saaiste en daarom het meest onderschatte. Er is geen aanvaller. Er is een laptop die in de trein blijft liggen. Een klantenbestand dat naar het verkeerde mailadres gaat. Een gedeelde map die per ongeluk voor de hele organisatie openstaat in plaats van voor drie mensen. Een chauffeur die twee jaar geleden vertrok en wiens account nog steeds actief blijkt, met toegang tot alles.

Dit scenario haalt zelden het nieuws, maar het is bij veel bedrijven de meest voorkomende oorzaak van een datalek — met meldplicht en alle gedoe van dien. En het is tegelijk het scenario waar afspraken vrijwel alles oplossen: accounts opheffen als iemand vertrekt, weten welke informatie gevoelig is, laptops versleutelen zodat een verloren apparaat een vervelend maar onschuldig verlies is.

De rekening

Als je mensen vraagt wat een cyberincident kost, noemen ze het losgeld. Dat is bijna altijd de kleinste post, en vaak nul.

Bij Steenwold werd niets betaald. De rekening kwam ergens anders vandaan, en de grootste post was tijd. Negen dagen waarin er niet gepland, niet gefactureerd en nauwelijks gewerkt kon worden. Dat is voor elk bedrijf uit te rekenen, en het is de enige berekening in dit hoofdstuk die de moeite waard is om zelf even te maken: neem je jaaromzet, deel door het aantal werkdagen, en vermenigvuldig met het aantal dagen dat jij denkt nodig te hebben om alles opnieuw op

te bouwen. Bij een bedrijf zonder geteste back-up is een week tot tien dagen realistisch.

Dat getal is het belangrijkste cijfer in dit hele boek. Niet omdat het schrik moet aanjagen, maar omdat het de enige maat is waarmee je alle keuzes verderop kunt afwegen. Elke maatregel in dit boek is goedkoper dan dat getal. Vrijwel elke maatregel is een orde van grootte goedkoper.

Daarna komen de kosten die je wel op een factuur terugziet: specialisten en forensisch onderzoek, tegen tarieven die gelden als je geen keuze hebt. Daarna de kosten die je pas maanden later merkt — de opdrachtgever die zijn vervoer opnieuw aanbesteedt, de groothandel die vragen stelt, de aanbesteding waar je op een securityvraag strandt. En dan is er de post die op geen enkel overzicht staat en die volgens de meeste ondernemers die het hebben meegemaakt de duurste is: een half jaar waarin de directie voor een derde van haar tijd met dit onderwerp bezig is in plaats van met het bedrijf.

De boetes komen daar nog bij, en die zijn sinds 2026 een serieuzere factor geworden dan ze waren. Daarover gaat het volgende hoofdstuk.

Maar we hadden toch antivirus

Steenwold had een virusscanner. Steenwold had een firewall. Steenwold had een IT-partij met een onderhoudscontract en een factuur die elke maand keurig binnenkwam.

Dat is niet uitzonderlijk. Vrijwel elk mkb-bedrijf heeft precies dat, en vrijwel elk mkb-bedrijf gaat er daarom van uit dat het gedekt is. Dat is de belangrijkste misvatting in dit hele onderwerp, en er zijn drie redenen waarom die dekking dunner is dan hij lijkt.

De eerste is dat de aanval niet via een systeem binnenkwam maar via een mens. Toen Sanne haar wachtwoord op die nepsite invulde, is er niets gehackt. Er is niets binnengedrongen, er is geen beveiliging doorbroken, er was voor geen enkele virusscanner iets te zien. Er werd daarna gewoon ingelogd, met geldige gegevens, via dezelfde deur die iedereen bij Steenwold elke ochtend gebruikt. Tegen dat scenario helpt maar één ding werkelijk, en dat is tweestapsverificatie: een tweede bewijs dat jij het bent, iets wat de aanvaller niet kan meenemen. Steenwold had het niet. Als Steenwold het wel had gehad, zou dit hoofdstuk niet bestaan.

De tweede reden is dat techniek zonder afspraken langzaam wegzakt. De back-up van Steenwold draaide — maar niemand had ooit gecontroleerd óf hij nog draaide, en niemand had ooit iets teruggezet om te zien of het werkte. De firewall stond er, maar er was ooit een poort in opengezet voor een leverancier, "voor de duur van het project", en dat project was in 2022 afgelopen. Zo gaat het overal. Techniek is geen toestand maar een proces, en een proces zonder eigenaar en zonder moment waarop iemand kijkt, verloopt.

De derde reden is de lastigste om te bespreken, want hij gaat over een relatie waar meestal jaren vertrouwen in zit. "Dat regelt onze IT'er" is geen maatregel maar een aanname, en die aanname is bijna nooit helemaal juist. Toen Marieke Steenwold na het incident het

contract erbij pakte, bleek dat er over back-ups stond dat er een back-upvoorziening werd geleverd — niet dat die getest werd, niet hoe ver hij terugging, niet binnen welke termijn hersteld zou worden, en met een aansprakelijkheid die was afgetopt op drie maandtermijnen. Haar IT-partij had niets fout gedaan. Ze had geleverd wat er in het contract stond. Alleen stond daar iets anders in dan Marieke dacht.

Van alle dingen die je na dit boek kunt doen, is dat contract erbij pakken misschien wel de nuttigste. Hoofdstuk 14 vertelt waar je dan naar kijkt.

Het goede nieuws

Tot zover het slechte nieuws, en nu het deel dat in de meeste boeken over dit onderwerp te weinig aandacht krijgt: dit is een oplosbaar probleem.

Niet volledig. Er bestaat geen bedrijf dat niets kan overkomen, en iedereen die je dat verkoopt, verkoopt je iets anders. Maar het overgrote deel van wat er in het mkb misgaat, wordt tegengehouden door een kort en eindig lijstje maatregelen. Tweestapsverificatie op alles wat vanaf internet bereikbaar is. Een back-up die niet vanaf je eigen netwerk te bereiken is, en die je één keer per jaar echt terugzet om te zien of het werkt. Updates die daadwerkelijk geïnstalleerd worden, ook op de dingen waar niemand aan denkt. Beheerrechten alleen bij wie ze nodig heeft. Accounts die verdwijnen als iemand vertrekt. Een afspraak over rekeningnummers. Mensen die weten waar ze op moeten letten en waar ze het kunnen melden zonder dat ze zich schamen.

Als Steenwold dat lijstje had gehad, was er nog steeds een nepmail geweest. Er was nog steeds een wachtwoord ingevuld op een verkeerde pagina. Maar er was niemand mee ingelogd, want er was