

Teun Arts

Van EHBO tot Operatiekamer

Wat statelijke cyberdreiging, NIS2 en de Cbw
betekenen voor niet-IT'ers

Uitgeverij Brave New Books bv., Amsterdam

Eerste druk 2026

© 2026 Teun Arts. Alle rechten voorbehouden.

ISBN 9789465545998

Schrijver: Teun Arts

Coverontwerp: Teun Arts

Van EHBO tot Operatiekamer

Wat statelijke cyberdreiging, NIS2 en de Cbw
betekenen voor niet-IT'ers

Leeswijzer

Dit boek is zo geschreven dat u het van voor naar achter kunt lezen als verhaal – maar dat hoeft niet.

Heeft u tien minuten, en wilt u vooral weten of uw organisatie onder de Cyberbeveiligingswet valt en wat u morgen moet doen? Sla dan direct op naar Deel III: De Gereedschapskist. De beslisboom, de directie-checklist en het 90-dagenplan geven u binnen een kwartier houvast, ook zonder de rest van het boek gelezen te hebben.

Heeft u een middag, en wilt u begrijpen waarom de wet is zoals hij is – en waarom cybersecurity niet langer een taak voor de IT-afdeling alleen is? Begin dan bij Deel II: De Wet, het einde van de vrijblijvendheid. Daar vindt u de juridische kern, vertaald naar de taal van de bestuurskamer.

Heeft u een weekend, en bent u nieuwsgierig naar h e we hier terecht zijn gekomen – van de argeloze jaren negentig tot de statelijke sabotage van vandaag? Begin dan bij het begin, met Deel I. Dat deel leest als een geschiedenisboek, maar elke episode legt de basis onder een artikel dat u verderop terugziet.

Door het boek heen volgt u twee organisaties. Peter van Vliet, directeur van een Brabants precisiebedrijf, laat zien wat het betekent om via de keten met de wet te maken te krijgen. Middenin Deel II maakt u kennis met een tweede casus: een regionaal ziekenhuis dat, anders dan Van Vliets bedrijf, rechtstreeks – als Essenti le Entiteit – onder de wet valt. Samen laten deze twee voorbeelden zien dat de Cbw niet  en soort organisatie raakt, maar vrijwel elk bedrijf dat via digitale systemen met de buitenwereld verbonden is.

Waar een technische term voor het eerst opduikt, wordt hij direct vertaald. U hoeft geen ICT-achtergrond te hebben om dit boek te kunnen volgen – dat is precies waarom het zo is geschreven.

Dankwoord

Dit boek was er niet geweest zonder een aantal mensen die ik hier graag bedank.

Allereerst Simon de Luij, directeur-eigenaar van Modderkolk en Technoforum. Simon nam mij in de loop van 2024 aan om de ICT-afdeling te leiden en gaf mij de ruimte om daar een eigen visie op te ontwikkelen. Simon, dank je wel voor dat vertrouwen.

Ook Erik Pols verdient dank. Ik leerde hem kennen eind 2024, toen Modderkolk & Technoforum zich voorbereidden op de nieuwe cyberbeveiligingswetgeving. Hij leerde mij anders kijken naar risico's — vooral via het verhaal van survivorship bias: het Amerikaanse leger wilde teruggekeerde bommenwerpers pantseren op de plekken met kogelgaten, tot statisticus Abraham Wald erop wees dat juist de plekken zónder gaten bescherming nodig hadden — die toestellen kwamen immers nooit terug. Dit boek draagt de sporen van dat inzicht op bijna elke pagina.

Wat begon als een adviesrelatie, groeide uit tot een goede band. Erik, dank je wel voor de kennis en het geduld waarmee je mij leerde zien wat niet meteen zichtbaar is.

Ook mijn team bij Modderkolk ICT verdient een groot woord van dank. Samen hebben we Modderkolk en Technoforum tijdig klaargestoomd voor de Cyberbeveiligingswet (NIS2) — geen kleine klus, maar iets waar we met zijn allen een mooie prestatie hebben neergezet. Dank voor jullie inzet en vakmanschap.

Proloog

De Ochtend van de Rekening

Het begon niet met loeiende sirenes, flinkerend blauw licht op de oprijlaan of een mechanische stem die via een gehackte babyfoon losgeld eiste in ontraceerbare cryptovaluta.

Het begon met de zachte, bijna geruststellende brom van het espressoapparaat op een zonovergoten zaterdagochtend in augustus.

Peter van Vliet, vierenvijftig jaar oud, directeur en enig aandeelhouder van Van Vliet Precisie techniek B.V., schoof met zijn blote voeten over de koele gietvloer van zijn keuken. Het huis aan de rand van Vught ademde rust. Buiten, door de kamerhoge glazen schuifpui, zag hij hoe de ochtenddauw langzaam verdampte van het strak gemaaid gazon. Een koperwiek scharrelde langs de beukenhaag. Geen wolkje aan de lucht. Het was zaterdag 15 augustus 2026. Een dag die in het teken had moeten staan van een rondje op de racefiets door de Meierij en een barbecue met vrienden.

Peter pakte zijn zware aardewerken mok, liep naar het keukeneiland en klapte achteloos zijn laptop open. Het was een ingesleten reflex van een man die zijn bedrijf in vijftwintig jaar tijd had opgebouwd van een tochtige werkplaats met twee tweedehands draaibanken tot een modern toeleveringsbedrijf met zestig man personeel. In de bedrijfshal op het industrieterrein stonden inmiddels vijftien computergestuurde CNC-freesmachines opgesteld. Machines ter waarde van tonnen, die dag en nacht met een nauwkeurigheid van een duizendste millimeter titanium, messing en hoogwaardig aluminium verspaanden.

Van Vliet Precisie techniek was een parel van de Nederlandse maakindustrie. Ze maakten geen eindproducten die je in de

schappen van de bouwmarkt vond. Ze leverden de onzichtbare, kritieke componenten: hogedrukventielen voor industriële gasinstallaties, uiterst complexe koppelstukken voor medische dialyseapparatuur en precisiebehuizingen voor optische sensoren.

Peter logde in. Niet met een ingewikkeld authenticatieprotocol, maar gewoon met zijn vertrouwde wachtwoord — de naam van zijn eerste hond gevolgd door het geboortjaar van zijn jongste dochter — dat hij al sinds 2019 niet meer had gewijzigd. Marco, die twee dagen per week als externe systeembeheerder de kantoorautomatisering deed, had er weleens over gemopperd. *“Peter, je moet die tweestapsverificatie aanzetten met zo’n app op je telefoon.”* Peter had destijds gelachen, zijn hand op Marco’s schouder gelegd en gezegd: *“Marco, wie wil er nou inbreken bij een frezerij in Brabant? Wij maken metaalschilfers, geen staatsgeheimen. Laat mij nou maar gewoon inloggen zonder dat gedoe met die sms-codes.”*

Op zijn scherm verscheen zijn inbox. Geen knipperend rood doodshoofd. Geen geëncrypteerde bestanden met de extensie *.locked*. Gewoon de dagelijkse stroom notificaties.

Maar bovenaan de lijst, binnengekomen om klokslag 08:01 uur, stond een e-mail die direct zijn aandacht trok.

De afzender was niet een vage prins uit Nigeria of een anonieme helpdesk, maar het directiesecretariaat van Holst & Partners Heavy Industries N.V. Holst was een beursgenoteerde gigant met vestigingen in zeven Europese landen, gespecialiseerd in industriële pompsystemen voor drinkwaterbedrijven, chemische raffinaderijen en koelsystemen van energiecentrales.

Holst was bovendien goed voor ruim 42 procent van de jaaromzet van Peters onderneming. Als Holst hoestte, had Van Vliet Precisie techniek een longontsteking.

De onderwerpregel van het bericht had de emotionele lading van een juridisch vonnis: *Urgente kennisgeving: Formele*

*inwerkingtreding Cyberbeveiligingswet (Cbw) – Verplichte
toetsing toeleveranciersketen ex art. 21 lid 2 sub d Richtlijn (EU)
2022/2555 (NIS2).*

Peter zette zijn koffiemok neer. Een kring van condens vormde zich op het composieten aanrechtblad. Hij klikte de mail open.

Geachte heer Van Vliet, beste Peter,

Vandaag, zaterdag 15 augustus 2026, is de Cyberbeveiligingswet (Cbw) in Nederland officieel van kracht geworden, ter implementatie van de Europese NIS2-richtlijn (Richtlijn EU 2022/2555).

Zoals u wellicht uit eerdere communicatie heeft vernomen, is Holst & Partners Heavy Industries N.V. door de bevoegde autoriteiten formeel geclassificeerd als een 'Essentiële Entiteit' binnen de sectoren Energie en Drinkwatervoorziening. Deze status legt onze onderneming dwingende wettelijke verplichtingen op ten aanzien van onze netwerk- en informatiesystemen.

Krachtens Artikel 21, lid 2, onder d van de richtlijn, alsmede de corresponderende bepalingen in de Cyberbeveiligingswet, rust op ons bestuur een rechtstreekse zorgplicht met betrekking tot de beveiliging van onze toeleveringsketen. Wij zijn wettelijk gehouden om de cyberweerbaarheid van onze toeleveranciers niet langer te baseren op goed vertrouwen, maar aantoonbaar en controleerbaar te auditeren.

Aangezien uw onderneming componenten levert die rechtstreeks worden geïntegreerd in onze vitale sturingsmechanismen, deelt u in ons risicoprofiel. Wij kunnen ons geen digitale contaminatie

permitteren via toeleveranciers met ongevalideerde toegang tot onze tekeningen, ordersystemen of fysieke leveringen.

In de bijlage treft u ons geactualiseerde 'Kader Ketenbeveiliging 2026'. Wij verzoeken u om binnen dertig (30) kalenderdagen na dagtekening van dit schrijven het bijgevoegde conformiteitsdossier ingevuld en ondertekend te retourneren, vergezeld van:

1. Een geldig ISO/IEC 27001-certificaat (dan wel een gevalideerd onafhankelijk auditrapport op basis van het BIO- of NIST CSF-kader);
2. Aantoonbaar bewijs van continue 24/7 detectie en monitoring op uw netwerkomgeving;
3. Het protocol waarmee u garandeert dat eventuele beveiligingsincidenten binnen vierentwintig (24) uur na ontdekking formeel worden gemeld aan onze Chief Information Security Officer (CISO);
4. Een recent bestuursbesluit waaruit blijkt dat uw directie periodieke trainingen op het gebied van cybersecurity en risicobeheer volgt.

Indien wij deze documentatie niet binnen de gestelde termijn van 30 dagen in goede orde hebben ontvangen en geverifieerd, zijn wij op grond van ons risicobeheersingsbeleid en de toezichtkaders van de Rijksinspectie Digitale Infrastructuur (RDI) wettelijk verplicht om lopende inkooporders per direct op te schorten en onze raamovereenkomst ter heroverweging voor te leggen aan onze Raad van Bestuur.

Wij vertrouwen op uw medewerking in deze gezamenlijke verantwoordelijkheid.

Hoogachtend,

|
|
| mr. drs. V.R. Smeets, Chief Information Security
| Officer
| ir. H.W. de Graaf, Lid Raad van Bestuur / COO
| Holst & Partners Heavy Industries N.V.

Peter las de brief nog een keer. En daarna nog een keer.

De woorden leken te dansen voor zijn ogen. *Essentiële Entiteit. Zorgplicht. Dertig dagen. Opschorting van inkooporders.*

Zijn blik gleed naar het pdf-icoon in de bijlage: *Kader_Ketenbeveiliging_2026_v4.2.pdf*. Achter de bestandsnaam stond de omvang vermeld: 8,4 megabyte. Peter dubbelklikte erop. Het document telde achtenzestig pagina's vol tabellen, juridische verwijzingen, schema's over cryptografische standaarden, beleidslijnen voor multifactor-authenticatie en strikte contractclausules waarin boetebedragen stonden genoemd die zijn hele winstmarge van de afgelopen drie jaar in één klap konden wegvagen.

ISO 27001? Ze hadden een ISO 9001-certificaat voor kwaliteitsmanagement aan de muur hangen. Dat ging over toleranties van metaal, over afkeurpercentages en kalibratie van meetinstrumenten. Maar informatiebeveiliging?

Tien jaar lang was cybersecurity binnen Van Vliet Precisietechniek een agendapunt geweest dat steevast werd doorgeschoven naar de rondvraag van het directieoverleg. En bij die rondvraag zei Peter steevast hetzelfde: *"Marco zorgt dat de virusscanners groen zijn, toch? Mooi, dan gaan we lunchen."*

Marco. Een aardige kerel van begin veertig die een eenmanszaak runde onder de naam *Marco IT Solutions*. Marco beheerde de server in de bezemkast naast de kantine, verving de toners van de printers en maakte back-ups op harde schijven die hij om de week mee naar huis nam in zijn fietstas. Dat noemde hij gekscherend zijn 'offsite back-up'.

En nu eiste een beursgenoteerde klant binnen dertig dagen een operatiekamer-inrichting. Continue monitoring. 24-uurs incidentrespons. Een getraind bestuur.

Voordat Peter de omvang van de ramp goed en wel tot zich door kon laten dringen, werd de stilte in de keuken ruw doorbroken. Niet door de laptop, maar door het schrille trillen van zijn iPhone op het houten aanrechtblad.

Op het scherm lichtte de naam op van Esther van Dongen, zijn hoofd administratie en al twaalf jaar zijn meest loyale steunpilaar.

Peter nam op. "Mogge Esther. Jij bent er vroeg bij op zater—"

"Peter!" viel Esther hem direct in de rede. Haar stem klonk niet zoals gewoonlijk rustig en beheerst, maar trilde van de opgekropte spanning. "Godzijdank dat je opneemt. Ik ben zó geschrokken. Ben je thuis?"

Peter ging rechtop staan. "Ja, ik sta in de keuken. Wat is er aan de hand?"

"Heb jij mij net gebeld?" vroeg ze met overslaande stem.

"Gebeld? Nee, ik sta net een kwartier beneden. Ik heb koffie gezet en zit net mijn mail te bekijken."

Het bleef een paar seconden angstaanjagend stil aan de andere kant van de lijn. Peter hoorde Esther zwaar ademen.

"Esther? Wat is er gebeurd?"

"Peter... ik werd om kwart voor acht gebeld. Vanaf een buitenlands nummer, iets met +49. Ik nam op en jij was het. Althans... het wás jouw stem. Exact jouw klank, jouw intonatie, zelfs dat kleine kuchje dat je altijd doet als je gehaast bent."

De haartjes op Peters armen gingen overeind staan. "Wat zei die stem dan?"

"Je zei dat je onderweg was naar een spoedoverleg in Duitsland. Dat er een unieke partij speciale titaniumstaven was vrijgekomen uit een faillissementsveiling die we móesten hebben voor de nieuwe order van Holst. Maar dat de curator eiste dat de aanbetsaling van € 87.500 vóór negen uur vanochtend op een rekening in Frankfurt moest staan, anders ging de partij naar een concurrent in Oostenrijk. Je klonk enorm gestrest. Je zei: *'Esther, alsjeblieft, maak het direct over via de spoedmodule, ik zit nu in de auto en stuur de factuur vanmiddag door.'*"

Peter voelde hoe het bloed uit zijn gezicht wegtrok. "En toen?"

"Ik had de bankieren-app al openstaan," fluisterde Esther. "Ik had het bedrag al ingetoetst. Tachtigduizend euro, Peter! Maar toen dacht ik: Peter regelt nooit zélf grondstoffen op zaterdagochtend. Daar hebben we Frank voor op inkoop. En je zou vandaag gaan fietsen. Dus ik belde jouw privénummer om het te dubbelchecken. En toen kreeg ik je voicemail."

"Omdat mijn telefoon nog op stil stond van vannacht," mompelde Peter verdwaasd.

"Precies! En op dat moment stuurde die Duitse beller me een WhatsApp-bericht. Met een foto van jouw paspoort – een kopie die we twee jaar geleden naar de beursorganisatie in Hannover hebben gemaild – en de tekst: *'Esther, waarom wacht je? Maak het nu over, we verliezen de deal!'* Pas toen begonnen al mijn alarmbellen te rinkelen. Ik heb direct de bankpas geblokkeerd en de zakelijke rekening bevroren. Peter... iemand probeert ons leeg te trekken. Met jouw eigen stem."

Peter leunde tegen het keukeneiland. Zijn benen voelden plotseling slap.

Een stemkloon. Een audio-deepfake, gevoed met fragmenten van video's die hij zelf vorig jaar trots op LinkedIn had geplaatst toen ze hun nieuwe vijfvlaksfreesmachine hadden gepresenteerd. Dertig seconden zuivere audio van een directielid is tegenwoordig genoeg voor een neurale netwerk om elke willekeurige zin uit te spreken met exact diens timbre, accent en ademhaling.

Twee gebeurtenissen. Op één ochtend. Binnen een tijdsbestek van een half uur.

Aan de ene kant de brute realiteit van de moderne onderwereld: criminelen die met kunstmatige intelligentie de digitale voordeur intrapten, gebruikmakend van psychologische manipulatie en griezelig accurate techniek om in één klap bijna een ton van zijn rekening te roven.

Aan de andere kant de formele, meedogenloze brief van zijn belangrijkste klant, waarin hem werd meegedeeld dat de wetgever geen genoeg meer nam met amateurisme. Dat hij binnen vier weken moest bewijzen dat hij zijn zaakjes op hetzelfde niveau had georganiseerd als een beursgenoteerde multinational.

Twee kanten van exact dezelfde medaille.

Terwijl Peter het telefoongesprek met de ontredder Esther afrondde en haar bezwoer dat ze fantastisch had gehandeld, dwaalden zijn gedachten af naar een herinnering van achttien maanden geleden.

Zijn vader, de oprichter van het bedrijf, had toen op tweeëntachtigjarige leeftijd een zware hartklepoperatie ondergaan in het Catharina Ziekenhuis in Eindhoven. Peter had urenlang doorgebracht in de kille, functionele gangen van het ziekenhuiscomplex. Hij herinnerde zich levendig het moment dat hij door de dubbele glazen wand van de intensive care had gekeken.

Aan de overkant van de gang bevond zich het operatiecomplex. Het was een wereld van absolute, compromisloze controle.

Voordat een chirurg die ruimte betrad, onderging hij een bijna religieus ritueel. De handen en onderarmen werden vijf minuten lang volgens een vast protocol geboend met desinfecterende zeep. Sieraden waren verboden. Kleding werd achtergelaten in een sluis; daarvoor in de plaats kwamen steriele jassen, mutsen en mondkmaskers.

In de operatiekamer zelf heerste overdruk. Verse, gefilterde lucht werd van bovenaf ingeblazen, zodat bij het openen van een deur de lucht altijd naar buiten stroomde. Geen enkele bacterie of stofdeeltje kon van de gang naar binnen waaien.

Op de operatietafel lag de patiënt aangesloten op een woud van apparatuur. Tientallen sensoren registreerden elke milliseconde de zuurstofsaturatie, de arteriële bloeddruk, de hersenactiviteit en het hartritme. Als een parameter ook maar één millimeter afweek van de veilige bandbreedte, klonk er geen paniekerig geschreeuw, maar een helder, gedoseerd akoestisch signaal. De anesthesist wist binnen een fractie van een seconde welke hendel hij moest overhalen om de balans te herstellen.

Elk instrument – van de kleinste arterieklem tot de meest geavanceerde hart-longmachine – was vooraf gesteriliseerd in een autoclaaf, voorzien van een uniek barcode-label en geregistreerd in een digitaal logboek. Niets werd aan het toeval overgelaten.

De hoofdchirurg was niet alleen een begenadigd vakman met een scalpel; hij was wettelijk verantwoordelijk voor de hygiëne en de protocollen in die ruimte. Als er een fout werd gemaakt door een assistent die zijn handen niet goed had gewassen, kon de chirurg zich niet verschuilen achter de schoonmaakploeg. De tuchtrechter kende geen genade voor het excuus: *“Ik lette even niet op, want ik was aan het snijden.”*

Dat was een operatiekamer. Een omgeving waar falen gelijkstond aan de dood, en waar veiligheid niet werd gezien als een hinderlijke kostenpost, maar als de allereerste voorwaarde om überhaupt te mogen bestaan.

En wat had Peter in zijn eigen bedrijf?

Peter liep naar de bijkeuken, deed het kastje onder de gootsteen open en pakte het voorwerp dat daar al sinds de verhuizing naar dit pand lag: een groen kunststof doosje met een wit kruis erop. De EHBO-kit.

Hij klikte de plastic sluitingen open. Binnenin lagen een paar rollen hydrofiel gaasverband, een mitella van vergeeld katoen, een pincet, een schaartje dat stroef open en dicht ging, en een handvol pleisters waarvan de kleeflaag door de jaren heen waarschijnlijk was vergaan tot een kleverige substantie. Onderin lag een plastic flesje jodium met een houdbaarheidsdatum die ergens in 2021 was verstreken.

Die verbanddoos was het symbool van hoe het Nederlandse bedrijfsleven dertig jaar lang had gekeken naar veiligheid.

Als een medewerker op de werkvloer zich sneed aan een scherpe braam van een aluminium plaat, liep hij naar de kantine, spoelde zijn vinger af onder de koude kraan, drukte er een pleister op uit de EHBO-doos en ging weer aan het werk. Soms deed het even pijn. Soms klopte de vinger een dag of twee na. Maar het menselijk lichaam loste het meestal vanzelf wel op. Een pleister was genoeg voor een schram.

Maar wat doe je als de wond geen schram is, maar een slagaderlijke bloeding? Wat doe je als het gevaar geen roestig spijkertje is, maar een gemuteerd, agressief virus dat met opzet wordt binnengebracht om de vitale organen van je bedrijf plat te leggen?

Met een EHBO-kit kun je geen openhartoperatie uitvoeren. Je kunt een patiënt met een septische shock niet redden met een rolletje verband en een flesje jodium dat over de datum is.

En toch was dat exact wat Peter van Vliet – en met hem honderdduizenden ondernemers, directeuren en managers in Nederland en Europa – decennialang had gedaan. Ze hadden een modern, hypercomplex, digitaal verweven bedrijf gerund met de veiligheidsfilosofie van een campingverbanddoos.

Als er een phishingmail binnenkwam, stuurden ze een waarschuwing rond: *“Let even op, jongens.”* Een pleister.

Als een laptop crashte, installeerde Marco Windows opnieuw vanaf een USB-stick. Een aspirientje.

Als de firewall waarschuwde dat er verdachte inlogpogingen waren vanuit Rusland of Noord-Korea, zette Marco dat IP-adres in een blokkeerlijst. Een toefje jodium op een open wond.

Tot vandaag. Zaterdag 15 augustus 2026.

De datum die in de agenda van menig ICT-consultant met rode viltstift was omcirkeld, maar die door de directiekamers van het MKB massaal was genegeerd als 'weer zo'n Brusselse bureaucratische oprisping'.

De Cyberbeveiligingswet was geen vrijblijvende verzameling adviezen van een welwillend overheidsorgaan. Het was de keiharde, dwingende implementatie van de herziene Europese richtlijn voor netwerk- en informatiebeveiliging: NIS2.

Waar de oude wetgeving uit 2018 zich slechts richtte op een handjevol traditionele giganten – zoals Schiphol, KPN, Gasunie en de grote banken – trok de nieuwe wet het net meedogenloos wijd open. Vanaf vandaag vielen duizenden bedrijven in achttien verschillende sectoren rechtstreeks onder overheidstoezicht. Van afvalverwerkers en chemiebedrijven tot machinebouwers, transporteurs, voedselproducenten en datacenterbeheerders.

En de wetgever had de regels fundamenteel herschreven.

Om te beginnen was er geen formele aanwijzing meer nodig. Bedrijven kregen geen vriendelijke brief van het ministerie waarin stond dat ze vanaf nu gereguleerd waren. De wet werkte *van rechtswege*. Voldeed je aan de criteria qua sector en omvang, dan wás je vanaf 15 augustus 2026 wettelijk plichtig. Geen excuses. Geen overgangsregelingen voor wie niet had opgelet.

Daarnaast had de wetgever definitief de bijl gezet aan de wortel van de 'ik-heb-geen-verstand-van-IT'-verdediging. In artikel 20 van de richtlijn stond het zwart op wit: de leden van het bestuursorgaan zijn persoonlijk verplicht om de maatregelen op het gebied van cyberrisicobeheer goed te keuren, toe te zien op de uitvoering ervan en zélf aantoonbaar periodieke trainingen te volgen. Bestuurders die verzuimden hun digitale zorgplicht na te leven, konden door toezichthouders niet alleen worden beboet tot miljoenen euro's, maar konden zelfs tijdelijk uit hun bestuursfunctie worden onttrokken.

En dan was er nog het meest explosieve onderdeel van de wet: de ketenaansprakelijkheid. Grote, essentiële entiteiten mochten hun eigen veilige vesting niet langer beschouwen als een geïsoleerd eiland. De wet verplichtte hen om hún toeleveranciers door te lichten. De keten was immers zo sterk als de zwakste schakel. Eén ongepatchte server bij een toeleverancier van een schroefje of een ventiel kon de besmettingsroute vormen waarlangs een vijandige staat of een crimineel kartel binnendrong in het hart van de Nederlandse energievoorziening.

Peter liet zich weer op zijn keukenstoel zakken. De koude koffie smaakte bitter.

Hij begreep nu pas de ware tragiek van zijn situatie.

Zijn eigen bedrijf, Van Vliet Precisie techniek B.V., telde zestig man personeel en draaide een jaaromzet van zo'n veertien miljoen euro. Daarmee viel hij volgens de letter van de wet

formeel wellicht buiten de zwaarste categorie. Hij hoefde zich misschien niet direct te registreren in het entiteitenregister van het Nationaal Cyber Security Centrum.

Maar de wet hield geen rekening met de wetten van de markt.

Zijn grootste klant – die 42 procent van zijn omzet vertegenwoordigde – was wél een Essentiële Entiteit. En Holst & Partners kon en mocht het risico niet nemen. Als Holst gecontamineerd raakte via een digitale bouwtekening die besmet was op de slecht beveiligde server van Peter, riskeerde Holst een boete van maximaal 10 miljoen euro of 2 procent van hun wereldwijde jaaromzet.

Holst eiste daarom simpelweg dat Peter zijn EHBO-kit weggooide en op stel en sprong een operatiekamer bouwde. Steriele handschoenen. Luchtzuivering. Sensoren. Certificaten.

En deed hij dat niet binnen dertig dagen? Dan zochten ze een toeleverancier in Duitsland of Denemarken die zijn digitale hygiëne wél op orde had.

Hoe had het zover kunnen komen?

Hoe was een wereld die ooit begon met een handvol idealistische wetenschappers die via een krakende telefoonlijn het woord *LOGIN* probeerden te versturen, geëvolueerd tot een maatschappij waarin een Brabantse metaalbewerker op een zaterdagochtend wordt geconfronteerd met een geavanceerde AI-stemaanval én een Europese wet die zijn bedrijf met de ondergang bedreigt?

Het antwoord op die vraag ligt niet in de honderden pagina's gortdroge wetteksten die op deze vijftiende augustus van kracht zijn geworden. Wie de wet wil begrijpen, moet de geschiedenis begrijpen.

Cybersecurity is geen technisch kunstje van bits, bytes, routers en firewalls. Het is de kroniek van een maatschappij die in zestig

jaar tijd verslaafd raakte aan een technologie die werd gebouwd op puur, grenzeloos vertrouwen – om er vervolgens stap voor stap achter te komen dat de menselijke natuur niet veranderd is. Waar rijkdom zich verplaatst, volgen de dieven. Waar macht zich concentreert, volgen de saboteurs.

Dit boek vertelt dat verhaal.

We reizen terug naar de mistige laboratoria van de jaren zestig, waar de allereerste digitale bacterie werd gekweekt als een onschuldige grap tussen academici. We kijken mee over de schouder van een tiener in de jaren tachtig die vanuit zijn slaapkamer per ongeluk het Pentagon binnendrong en daarmee een Amerikaanse president deed sidderen van angst. We zien hoe de rookpluimen boven Manhattan op 11 september 2001 de wereld definitief dwongen om infrastructuren te beschouwen als potentiële wapens, en hoe het internet in de decennia daarna muteerde van een digitaal marktplaats in een internationaal slagveld van spionage, chantage en ontwijking.

Pas wanneer we die reis hebben afgelegd, keren we terug naar het heden. Naar de harde realiteit van NIS2 en de Cyberbeveiligingswet.

We gaan ontdekken waarom het onderscheid tussen de EHBO-kit en de Operatiekamer het meest cruciale overlevingsconcept is voor elke moderne ondernemer, bestuurder en manager. We gaan zien wat er van jou wordt verwacht als jouw organisatie de operatiekamer in moet – en hoe je voorkomt dat je als kleine toeleverancier vermalen wordt tussen de hygiëne-eisen van de grote spelers.

Je hoeft geen chirurg te zijn om te begrijpen waarom handen wassen levens redt. En je hoeft geen hacker of computerexpert te zijn om je onderneming te beschermen tegen de ondergang.

Het enige wat je nodig hebt, is het besef dat weggijken vanaf vandaag officieel verboden is.

Peter van Vliet keek naar het beeldscherm voor zich. Hij pakte zijn muis, schoof de cursor naar het telefoonnummer van Marco en drukte op bellen.

Het was tijd om te leren opereren.

DEEL I

**Hoe de wereld zijn digitale
onschuld verloor**

1 Het Glazen Huis

De jaren '60 en '70

De kamer rook naar ozon, warme machineolie, filterkoffie die urenlang op een warmhoudplaatje had gestaan en de scherpe, chemische damp van verhitte printplaten. Het was een constante symfonie van laagfrequent gebrom: zware industriële ventilatoren die met een dof geruis wanhopig koele lucht langs rijen metershoge kasten joegen, afgewisseld met het harde, mechanische geratel van Teletype-printers en het schuifelende tikken van magnetische banden die schoksgewijs op gang kwamen op reusachtige haspels.

We schrijven woensdagavond 29 oktober 1969, even na negenen. Plaats van handeling: kamer 3420 van Boelter Hall, de faculteit voor techniek en toegepaste wetenschappen van de University of California in Los Angeles (UCLA).

Wie vandaag aan computers denkt, ziet een ultradunne laptop op een strak opgeruimd bureau voor zich, of een glimmende smartphone in een broekzak. Hier, in de ingewanden van het universiteitsgebouw, stond een machinepark dat meer deed denken aan een machinekamer van een stoomboot dan aan wat wij nu een kantooromgeving noemen. Hier stond de SDS Sigma 7, een wetenschappelijke mainframe ter grootte van een riante kledingkast. Daarnaast stond de ware ster van de avond: de Interface Message Processor, kortweg de IMP. Het was een kolossaal, grijsgekleurd brok militair staal, gebouwd door het ingenieursbureau Bolt Beranek and Newman (BBN) uit Cambridge, Massachusetts. Het ding was zo zwaar en log dat de technici van BBN een vorkheftruck hadden moeten huren om de stalen behuizing onbeschadigd over de drempel van het laboratorium te krijgen.

Rondom de apparatuur stond een groepje jonge mannen. De mouwen van hun witte overhemden waren opgestroopt tot over

de ellebogen, stropdassen hingen half los, en dikke hoornen brillen schitterden in het kille tl-licht. Aan de zijkant stond Leonard Kleinrock, een briljante professor in de informatica met een vlijmscherpe blik en een aanstekelijke rust. Kleinrock had jarenlang gewerkt aan de wiskundige theorie achter packet switching – het revolutionaire concept dat data niet langer in één ononderbroken stroom via een vaste fysieke lijn moest worden verstuurd, maar kon worden opgeknipt in kleine, zelfstandige pakketjes die elk hun eigen weg zochten door een netwerk om aan de overkant weer in de juiste volgorde in elkaar te klikken.

Voor de Teletype-terminal zat Charley Kline, een eenentwintigjarige student met een geconcentreerde blik. Naast hem lag een zware hoorn van een ouderwetse bakelieten telefoon. Via een gewone, ingehuurd telefoonlijn van AT&T – een verbinding met de duizelingwekkende bandbreedte van 50 kilobit per seconde – stond Kline in direct contact met Bill Duvall, een jonge programmeur die zeshonderd kilometer noordelijker zat, in het laboratorium van het Stanford Research Institute (SRI) nabij Palo Alto.

De sfeer in de kamer was niet die van een militaire commandopost in oorlogstijd, hoewel het project werd gefinancierd door het Advance Research Projects Agency (ARPA) van het Amerikaanse ministerie van Defensie. Het was de sfeer van nieuwsgierige jonge honden die aan de rand stonden van een nieuw continent. Het doel van de avond was zo elementair dat het haast komisch was: een student in Los Angeles zou proberen in te loggen op een computer in Stanford.

Kline nam de telefoonhoorn stevig tussen zijn schouder en kin geklemd.

"Ben je er klaar voor, Bill?" vroeg Kline door de krakende lijn.

"Laat maar komen," klonk de stem van Duvall door de luidspreker.

"Goed. Ik typ nu de 'L'."

Kline drukte op de logge metalen toets van de Teletype. De machine bracht met een felle mechanische klap de letter op het papier.

"Zie je de 'L'?" vroeg Kline.

"Ja, de 'L' is binnen," bevestigde Duvall vanuit Stanford.

"Ik typ nu de 'O'."

Weer een harde mechanische tik.

"Ontvangen. De 'O' staat op mijn scherm."

Kline ademde rustig in. "Dan ga ik nu voor de 'G'."

Hij drukte de toets in. Op het scherm in Stanford gebeurde iets onverwachts. In plaats van de letter 'G' op te slaan in het invoerbuffer, liep het geheugenbeheer van de SDS 940-mainframe in Stanford vast door een kleine programmeerfout in de ontvangende software. Het systeem crashte met een doffe stilte.

"Bill?" vroeg Kline in de telefoonlijn. "Ben je er nog?"

"Hij hangt," zei Duvall laconiek. "Het systeem is neergegaan."

Het allereerste bericht dat ooit door de aderen van het netwerk stroomde dat uiteindelijk de hele mensheid zou verbinden, was niet een plechtig, bijbels citaat zoals Samuel Morse ooit had verzonden. Het was geen historische proclamatie. Het was de ongeplande, stomtoevallige kreet: *LO*. Alsof de machine zelf, vlak voor hij in zwijgen verviel, de wereld toeriep: *Lo and behold* – zie en aanschouw.

Een uur later herstartten de technici in Stanford de mainframe, poetsten ze de bufferfout weg en probeerde Kline het opnieuw.

De letters 'G', 'I' en 'N' kwamen storingsvrij binnen. De verbinding was een feit. Het ARPANET had zijn eerste ademtucht uitgeblazen.

Wie die avond in oktober 1969 door de gangen van Boelter Hall liep, zou nooit geraden hebben dat hier het fundament werd gelegd voor een systeem dat een halve eeuw later het wereldwijde bankverkeer, de elektriciteitsnetten, de communicatie van miljarden mensen en de geopolitieke machtsverhoudingen zou dragen.

Wat nog opmerkelijker was: wie zoekt naar de beveiligingsprotocollen van die allereerste verbinding, zoekt vergeefs. Er was geen authenticatie. Er was geen versleuteling. Er was geen mechanisme dat controleerde of Charley Kline wel echt Charley Kline was, of dat iemand anders stiekem meeluisterde op de AT&T-telefoonlijn. Het concept van een 'wachtwoord' bestond lokaal op sommige mainframes wel, maar het netwerk zelf kende geen grendels.

Om te begrijpen waarom dit zo was, moet je afdalen in de ziel van de vroege computergemeenschap.

Het computerveld van de jaren zestig was een elitaire, hechte en bovenal academische broedplaats. Computers waren astronomisch duur, schaars en stonden vrijwel uitsluitend opgesteld in kelders van vooraanstaande universiteiten en militaire onderzoeksfaciliteiten. De mensen die achter de terminals zaten, vormden een kleine sekte van wiskundigen, natuurkundigen en ingenieurs. Ze kenden elkaars publicaties, bezochten dezelfde conferenties, dineerden in dezelfde universiteitskantines en deelden elkaars passie voor het temmen van deze gigantische elektronische rekenmeesters.

Het ARPANET was niet ontworpen om geheimen te bewaren. Het was ontworpen om middelen te delen. Een computer in Los Angeles had speciale rekenkracht; een computer in Stanford beschikte over geavanceerde grafische software; een computer in Salt Lake City specialiseerde zich weer in andere modellen.