DE ONVERMIJDELIJKE HACK

Jan Hoogstra

Praktijklessen voor digitaal weerbare organisaties

Met een voorwoord van Dave Maasland

VANDUUREN MEDIA

Inhoud

Voorwoord ix

Inleiding 1

Impact van een cybercrisis 2
Maatschappelijke impact van een cyberaanval 4
Voorbereiding uit de praktijk 7
Een veilig huis begint met een goede voorbereiding 8

1 Anatomie van een cybercrisis 11

Cyber- versus gewone crisis 14
Maatschappelijke ontwrichting, wetgeving en normenkaders 16
Actuele dreigingen 17
Soorten aanvallen 18
Wie zijn de hackers? 27
Verloop van de cyberaanval: Unified Kill Chain 29
De toekomst van cyberaanvallen 31
Cyberweerbaarheid: meer dan techniek 32

2 Hoe een cybercrisis mensen raakt 35

Fight, flight, freeze en fawn 36
De ui van betrokkenheid 38
Schuldvraag versus schuldgevoel 45
Meetbare impact op mensen 47

Verborgen mentale impact 50
Psychologische hulp 51
Oefening: wie wordt vergeten? 52
Leerpunt: zorg voor de verzorging 53

3 Hoe een cybercrisis organisaties raakt 55

Reikwijdte van de cybercrisis 56
Bedrijfscontinuïteit als beleidsonderwerp 58
Het moment waarop de organisatie verandert 62
Crisismanagementteam: hiërarchie versus competentie 62
Externe partijen: onmisbaar tijdens een crisis, maar vaak te laat 65
Verantwoordelijkheden 69
Contact opnemen of niet? 72
Betalen of niet betalen? 72
Kosten van een cybercrisis 76
Cyberverzekeringen: vangnet én sturingsmechanisme 78
Oefening – De organisatie tijdens een cybercrisis 80
Leerpunt: organiseer de crisis vóór de crisis 81

4 Hoe een cybercrisis de techniek raakt 83

De basismaatregelen 86
Assetmanagement: weten wat je hebt voordat je het kwijt bent 93
Cloud, leveranciers en digitale afhankelijkheden 95
SANS Incident Response-model 97
Data: het werkelijke doelwit 104
Oefening: ken jij jouw digitale omgeving? 107
Leerpunt: ken je digitale omgeving 108

5 Hoe je over een cybercrisis communiceert 109

Doelstelling crisiscommunicatie 110
Hoeveel pleuris breekt er eigenlijk uit? 112
Zeven valkuilen bij crisiscommunicatie 115
Oefening: De eerste boodschap 131
Leerpunt: communicatie gaat niet over wat jij wilt vertellen, maar over wat anderen willen weten 132

6 Voorbereiden op de slechtste dag 137

Een cybercrisis is ook gewoon een crisis 138
Een plan voor mensen, niet voor systemen 139
Een plan voor de dag waarop het toch misgaat 139
Vier plannen die samen één geheel vormen 140
Hoe maak je je plannen? 154
Het proces om tot goede plannen te komen 154
Waar bewaar je het plan? 157
Een plan is nooit af 158
Oefening: de zoektest 159
Leerpunt: zorg voor plannen die samen één aanpak vormen 160

7 Liever zweten tijdens een oefening dan tijdens een crisis 161

De eerste tien minuten 162
Opleiden, trainen en oefenen 163
Testen of oefenen? 164
Bewustwording ontstaat door te ervaren 165
Oefenvormen 167
Kies een oefening die past 171
Oefenprogramma opbouwen 172
Oefenen voor de verschillende fasen van een cybercrisis 173
Groeien in cyberweerbaarheid 176
Oefening – Tabletop: "Maandagochtend 08.30 uur" 179
Leerpunt: oefenen maakt het verschil 181

Epiloog 183

A Wet- en regelgeving en normenkaders 187

B Geïnterviewden 189

Dankwoord 195

Bronnen 199

Inleiding

"Bij een inbraak ben je een paar spullen kwijt. Een cyberaanval raakt het bestaan van je organisatie."

– Menno Smidts, directeur Smidts Autogroep met zes Ford-vestigingen.

Een inbraak in je huis laat sporen achter. Je voelt je onveilig en vraagt je af of het nog eens gebeurt. Een cyberaanval doet iets vergelijkbaars met een organisatie, maar de gevolgen reiken vaak veel verder. Niet alleen systemen vallen uit, ook mensen, processen en vertrouwen komen onder druk te staan.

Toen ik Smidts vroeg wat hem het meest was bijgebleven van de cyberaanval op zijn organisatie, begon hij niet over de hackers, de ransomware of de technische schade. Hij vertelde over de onzekerheid en de verantwoordelijkheid die hij voelde voor zijn medewerkers. Hij had vijf nachten nauwelijks geslapen en besefte dat het voortbestaan van zijn bedrijf op het spel stond.

Dat gesprek bleef mij bij. Ik hoorde daarna dezelfde rode draad. Voor dit boek sprak ik bestuurders, directeuren, incidentresponders, communicatieadviseurs, ethische hackers, psychologen, advocaten en andere professionals die een cybercrisis van dichtbij hebben meegemaakt. Hun organisaties verschilden in omvang, sector en omstandigheden, maar hun ervaringen kwamen opvallend overeen.

Een cybercrisis begint misschien met techniek, maar verandert al snel in een crisis van mensen. Bestuurders moeten onder grote druk besluiten nemen. Medewerkers raken onzeker of vallen uit. Communicatie wordt minstens zo belangrijk als techniek. En juist de manier waarop een organisatie zich hierop voorbereidt, bepaalt uiteindelijk hoe groot de impact wordt.

Misschien denk je dat zoiets jouw organisatie niet zal overkomen. Dat hoop ik oprecht. Maar de vraag is steeds minder óf organisaties met een cyberaanval te maken krijgen en steeds vaker wanneer. De hack is onvermijdelijk. Iedere organisatie is afhankelijk van digitale systemen. Daarmee is ook iedere organisatie kwetsbaar.

Veel boeken gaan over het voorkomen van een cyberaanval. Preventie blijft natuurlijk belangrijk, maar je wilt vooral weten wat je doet als het tóch misgaat. Dat onderschrijft ook CISO en securitystrateeg Jeroen Prinse. Volgens hem verschuift de aandacht binnen informatiebeveiliging van beveiliging naar digitale weerbaarheid. Zodra je accepteert dat een cyberincident ooit kan plaatsvinden, wordt de vraag: hoe snel kunnen we herstellen en onze dienstverlening voortzetten? Digitale weerbaarheid combineert daarom bescherming met herstelvermogen en continuïteit.

Juist in de eerste uren van een cybercrisis worden beslissingen genomen die mede bepalen hoe groot de uiteindelijke schade is: financieel, maar ook voor het vertrouwen, de samenwerking, de dienstverlening en de mensen die de crisis moeten oplossen.

Dat is waar dit boek over gaat: de impact van een cybercrisis en de vraag hoe je die kunt beperken.

Impact van een cybercrisis

Digitalisering is niet meer weg te denken uit organisaties en uit onze samenleving. Wat ooit ondersteunend was, is inmiddels bedrijfskritisch geworden. Die ontwikkeling heeft organisaties veel gebracht. Maar ze kent ook een duidelijke schaduwkant. Hoe afhankelijker organisaties worden van IT, hoe groter de gevolgen als het misgaat.

Cyberincidenten beperken zich allang niet meer tot technische omgevingen. Ze raken organisaties in hun kern en ook de mensen en organisaties daaromheen. Systemen vallen uit, processen komen stil te liggen en herstelwerkzaamheden zijn nodig. Dat kost tijd en geld, maar ook menselijke inzet en vertrouwen. Medewerkers kunnen hun werk niet doen en klanten krijgen geen dienstverlening. Informatie kan op straat belanden, waardoor het vertrouwen in de organisatie beschadigd raakt. Direct betrokkenen kunnen last krijgen van stress en onmacht, soms nog lang na het incident. Zo ging het bedrijf van ondernemer Xander Koppelmans uiteindelijk failliet en belandde hij in een burn-out.

In 2015 werd het communicatie- en ontwerpbureau van ondernemer Xander Koppelmans getroffen door een ransomwareaanval. Het bedrijf werkte voor honderden klanten en was voor de dagelijkse dienstverlening sterk afhankelijk van digitale systemen en opgeslagen klantbestanden.

De aanvallers wisten toegang te krijgen tot de IT-omgeving via externe toegangsvoorzieningen die werden gebruikt door freelancers. Nadat zij toegang hadden verkregen, werden niet alleen de productieservers geraakt, maar ook de back-upomgeving. Daardoor bleek het grootste deel van de beschikbare data niet meer bruikbaar voor herstel. Hoewel later een aanzienlijk deel van de bestanden werd teruggevonden, ontbraken mappenstructuren en waren veel (klant)bestanden beschadigd.

De gevolgen werden in de weken na de aanval steeds duidelijker. Lopende opdrachten konden niet of slechts gedeeltelijk worden uitgevoerd. Medewerkers moesten hun tijd besteden aan herstelwerkzaamheden in plaats van aan nieuwe projecten. Klanten wachtten op bestanden, campagnes en ontwerpen die niet meer beschikbaar waren. De omzet viel terug terwijl de kosten voor herstel en reparatie bleven doorlopen. In de eerste periode na het incident werd het omzetverlies door Koppelmans geschat op ongeveer een kwart miljoen euro. Enkele maanden later was de totale schade opgelopen tot ongeveer een half miljoen euro.

De aanval had niet alleen gevolgen voor de bedrijfsvoering, maar ook voor de mensen achter het bedrijf. Medewerkers vertrokken, klanten beëindigden de samenwerking en het vertrouwen in een herstel van de organisatie nam af. Uiteindelijk leidde de situatie tot een faillissement. Ook

meer dan tien jaar later merkt hij nog dagelijks de emotionele gevolgen van de cybercrisis.

Hoe een organisatie reageert, bepaalt in hoge mate hoe groot de uiteindelijke schade wordt.

Maatschappelijke impact van een cyberaanval

De afgelopen jaren hebben we in Nederland en België meerdere voorbeelden gezien die dit pijnlijk zichtbaar maken. Deze en andere voorbeelden komen in dit boek vaker terug. Stuk voor stuk laten ze zien dat een aanval verder reikt dan de eigen organisatie en ook de maatschappij raakt. De lessen zijn voor zowel Nederland als België relevant; cybercriminelen trekken zich immers niets aan van landsgrenzen.

Gegevens uit afzonderlijke datalekken kunnen worden gecombineerd. Wie bijvoorbeeld klant is van Odido en voorkomt in gegevens die bij een zorg- of overheidsorganisatie zijn buitgemaakt, kan zeer gericht worden benaderd met phishing of andere vormen van social engineering. Elk incident kan zo de kans op nieuwe incidenten vergroten.

Odido-hack

In februari 2026 maakte telecomprovider Odido bekend slachtoffer te zijn geworden van een cyberaanval waarbij gegevens van miljoenen klanten waren buitgemaakt. Aanvallers kregen toegang tot een klantcontactsysteem met persoonsgegevens van huidige en voormalige klanten. Uiteindelijk bleken ongeveer 6,39 miljoen personen te zijn geraakt.

De aanval vond plaats via social engineering. Aanvallers benaderden medewerkers en deden zich voor als interne IT-medewerkers. Door een combinatie van phishing en telefonische misleiding kregen de cybercriminelen toegang tot een Salesforce-omgeving waarin klantgegevens waren opgeslagen. Daarbij werd ook tweefactorauthenticatie omzeild doordat medewerkers werden overtuigd om inlogverzoeken goed te keuren.

Volgens Odido en betrokken onderzoekers zijn onder meer namen, adressen, telefoonnummers, e-mailadressen, klantnummers, geboortedata en

IBAN-nummers buitgemaakt. Van een deel van de betrokkenen werden ook identificatiegegevens, zoals paspoort- of rijbewijsnummers, gestolen. Wachtwoorden van klantaccounts, locatiegegevens, belgegevens en scans van identiteitsdocumenten maakten volgens het bedrijf geen deel uit van het datalek.

De dienstverlening van Odido bleef tijdens het incident beschikbaar. Klanten konden blijven bellen, internetten en televisiekijken. De impact lag vooral op het gebied van privacy en gegevensbescherming. Klanten werden gewaarschuwd voor verhoogde risico's op phishing, identiteitsfraude en andere vormen van misbruik van persoonsgegevens.

Het incident leidde tot grote maatschappelijke aandacht. De Autoriteit Persoonsgegevens ontving in korte tijd een groot aantal meldingen en klachten. Daarnaast ontstonden initiatieven voor collectieve schadeclaims en werden vragen gesteld over de bewaartermijnen van klantgegevens en hoe deze gegevens waren beschermd.

Voor veel betrokkenen leidde het incident tot onzekerheid over welke gegevens waren buitgemaakt, hoe deze gebruikt konden worden en welke gevolgen dit op langere termijn zou kunnen hebben.

Bij de cyberaanval op het ziekenhuis AZ Monica in Antwerpen moesten zorgverleners tijdelijk terugvallen op papieren dossiers, werden afspraken uitgesteld en werkprocessen aangepast om de patiëntenzorg veilig voort te zetten. Artsen, verpleegkundigen en ondersteunende medewerkers moesten in korte tijd overschakelen. De aanval maakte zichtbaar hoe afhankelijk een modern ziekenhuis is van digitale systemen, maar vooral hoeveel improvisatie, samenwerking en veerkracht nodig zijn om de zorg te waarborgen. Op deze casus kom ik in het volgende hoofdstuk uitgebreider terug.

Bij Bevolkingsonderzoek Nederland lag de kwetsbaarheid niet in de eigen organisatie, maar bij een extern laboratorium. De impact was vooral groot voor de mensen van wie gevoelige persoonsgegevens waren buitgemaakt. Ook het vertrouwen in het bevolkingsonderzoek kwam onder druk te staan.

Clinical Diagnostics-hack

In juli 2025 werd laboratorium Clinical Diagnostics NMDL in Rijswijk getroffen door een cyberaanval. Het laboratorium voerde in opdracht van Bevolkingsonderzoek Nederland onderzoeken uit voor het bevolkingsonderzoek naar baarmoederhalskanker. Daarbij werden uitstrijkjes en zelftesten van deelnemers geanalyseerd. Na de aanval bleek dat aanvallers toegang hadden gekregen tot systemen waarin persoonsgegevens en medische gegevens waren opgeslagen.

Op 11 augustus 2025 maakte Bevolkingsonderzoek Nederland bekend dat gegevens van ruim 485.000 deelnemers aan het bevolkingsonderzoek waren buitgemaakt. Het ging onder meer om namen, adressen, geboortedata, burgerservicenummers, gegevens van zorgverleners en mogelijk testuitslagen. Bevolkingsonderzoek Nederland gaf aan dat de eigen systemen niet waren gehackt, maar dat het datalek was ontstaan bij het externe laboratorium waarmee werd samengewerkt.

In de weken daarna bleek de omvang van het incident groter dan aanvankelijk gedacht. Clinical Diagnostics meldde dat gegevens van nog eens bijna 230.000 deelnemers waren gelekt. Omdat het laboratorium niet kon bevestigen dat daarmee de volledige omvang bekend was, besloot Bevolkingsonderzoek Nederland uiteindelijk alle 941.000 personen te informeren van wie ooit gegevens met het laboratorium waren gedeeld.

De impact van het incident lag vooral op het gebied van privacy en vertrouwen. Anders dan bij veel ransomwareaanvallen stonden zorgprocessen niet direct stil en bleef het bevolkingsonderzoek doorgaan via andere laboratoria. De onrust ontstond vooral doordat medische gegevens en persoonsgegevens in één bestand aanwezig waren. Voor veel deelnemers betekende dit onzekerheid over welke informatie precies was buitgemaakt en hoe deze gegevens mogelijk gebruikt konden worden voor fraude, phishing of identiteitsmisbruik.

Het incident leidde tot onderzoeken door onder meer de Autoriteit Persoonsgegevens. Ook ontstond brede maatschappelijke aandacht vanwege de aard van de gegevens en de schaal van het datalek. Naast deelnemers aan het bevolkingsonderzoek bleken volgens Z-CERT ook andere zorginstel-

lingen en zorgverleners geraakt door de aanval op Clinical Diagnostics. Daarmee bleef de impact niet beperkt tot één organisatie, maar strekte deze zich uit over meerdere onderdelen van de zorgketen.

Toen de Stad Antwerpen eind 2022 werd getroffen door een ransomwareaanval, vielen honderden digitale systemen uit. Medewerkers konden niet meer bij dossiers, digitale loketten waren beperkt beschikbaar en inwoners merkten de gevolgen direct. Achter de schermen werkte een grote crisisorganisatie dag en nacht aan het indammen van de aanval, het herstellen van systemen en het beantwoorden van vragen van bestuurders, media en inwoners.

Deze voorbeelden laten zien dat cyberincidenten niet op zichzelf staan. Ze raken ketens, afhankelijkheden en uiteindelijk de maatschappij als geheel. Dat maakt cyberweerbaarheid ook een maatschappelijke verantwoordelijkheid.

Voorbereiding uit de praktijk

In *Cyberweerbaar Nederland 2026*, een onderzoek van KPN en Security Innovation Stories, beoordelen organisaties hun eigen cyberweerbaarheid gemiddeld met een 7,1. Tegelijk blijkt dat essentiële onderdelen zoals oefenen, ketenbeveiliging en integrale samenwerking vaak beperkt zijn ontwikkeld. Plannen zijn aanwezig, maar niet altijd in realistische omstandigheden getest. Slechts 28 procent van de organisaties test het crisismanagementbeleid regelmatig.

Zoals Caroline Sander van de unit High Tech van de Nationale Politie het tijdens ons interview samenvatte: “De vraag is niet óf je getroffen wordt, maar wanneer. Bereid je daarop voor.”

Hoe je je voorbereidt, is vooral te leren uit de praktijk. Voor dit boek sprak ik met meer dan twintig bestuurders, onderzoekers en specialisten, maar ook met organisaties die zelf een cybercrisis hebben meegemaakt. Hun ervaringen, inzichten en praktijkvoorbeelden vormen de basis van de lessen in dit boek. Een uitgebreid overzicht van de geïnterviewden en hun achtergrond is opgenomen in bijlage B.

Niet iedereen wilde daarbij met naam en toenaam worden genoemd. Dat is begrijpelijk. Een cyberincident kan nog jarenlang gevolgen hebben voor een

organisatie en de mensen die erbij betrokken waren. Daarom zijn sommige personen en organisaties geanonimiseerd of slechts beperkt herkenbaar beschreven. De inhoud van hun verhaal is niet aangepast; juist doordat anonimiteit mogelijk was, durfden veel geïnterviewden openhartig te vertellen over onzekerheid, fouten, dilemma's en de lessen die zij onderweg hebben geleerd.

Hoewel iedere cybercrisis anders verloopt, kwam in vrijwel alle gesprekken één boodschap steeds terug: een cybercrisis is nooit alleen een technisch probleem. De grootste uitdagingen ontstaan vaak op het snijvlak van mens, organisatie, techniek, communicatie en bestuur. Vanuit die gedachte heb ik bewust gekozen voor een brede groep geïnterviewden.

Dennis Gerlof, Menno Smidts, Niels Golsteijn en Xander Koppelmans vertellen openhartig over de impact die een aanval had op hun organisatie. Daarnaast sprak ik meerdere betrokkenen bij een gehackt leerwerkbedrijf, van de betrokken wethouder tot de manager bedrijfsvoering. Zo kreeg ik zicht op de verschillende perspectieven die tijdens een cybercrisis samenkomen en op de vraag wat herstel vraagt van mensen en organisaties.

De specialisten die ik sprak, vullen die praktijkervaring aan met expertise op het gebied van incidentrespons, crisiscommunicatie, bedrijfscontinuïteit, menselijk gedrag, leiderschap, juridische vraagstukken, cyberverzekeringen, ethical hacking en het actuele dreigingslandschap.

Een veilig huis begint met een goede voorbereiding

Een cybercrisis laat zich niet plannen. De voorbereiding wel.

Dat is de centrale gedachte van dit boek.

Een organisatie is in veel opzichten te vergelijken met een huis. Je kunt goede sloten plaatsen, rookmelders ophangen en een brandblusser aan de muur hangen. Daarmee verklein je de kans dat er iets misgaat, maar je kunt nooit uitsluiten dat er wordt ingebroken of brand uitbreekt. Vrijwel iedereen weet instinctief wat hij moet doen wanneer er brand uitbreekt. Er wordt 112 gebeld, bewoners verlaten het gebouw en de brandweer neemt de leiding. Voor cyberincidenten bestaat die reflex veel minder. Organisaties weten vaak niet wie ze

moeten bellen, wie de leiding neemt of welke eerste stappen nodig zijn. Incidentresponder Tom de Laet vergelijkt dat met een huis waarin de rookmelder afgaat, maar niemand weet waar de brandblusser hangt of wie de brandweer moet bellen.

In het eerste deel van dit boek kijken we naar wat een cybercrisis eigenlijk is en waarom de impact vaak veel groter is dan een regulier technisch incident. We beginnen met de vraag: wanneer spreken we eigenlijk van een cybercrisis? Vervolgens bekijken we de gevolgen vanuit vier perspectieven: **mens, organisatie, techniek en crisiscommunicatie**. De samenhang tussen deze vier bepaalt hoe een crisis zich ontwikkelt en uiteindelijk wordt beheerst.

De theorie komt tot leven in praktijkverhalen. Van de Stad Antwerpen tot AZ Monica, van de Universiteit Maastricht tot QuaWonen. Iedere casus laat een andere kant van een cybercrisis zien: de onzekerheid tijdens de eerste uren, de druk op bestuurders, de technische uitdagingen, de dilemma's rondom communicatie en de keuzes die uiteindelijk het verschil maakten.

In het tweede deel van dit boek gaat het over de praktische kant van het voorbereiden. Je leert hoe je een organisatie voorbereidt met een crisismanagementplan, een incidentresponsplan, een bedrijfscontinuïteitsplan en een herstelplan. Vervolgens laat ik zien hoe je deze plannen vertaalt naar realistische oefeningen, zodat mensen niet alleen weten wat er op papier staat, maar ook ervaren hoe zij onder druk moeten samenwerken, communiceren en besluiten nemen.

Dit boek is nadrukkelijk geen technisch handboek. Het is een praktisch boek voor bestuurders, managers, informatiebeveiligers en andere professionals die verantwoordelijkheid dragen voor de continuïteit van hun organisatie. Daarom bevat ieder hoofdstuk een korte praktijkopdracht. Deze zijn eenvoudig uit te voeren en helpen je om de inzichten uit het hoofdstuk direct toe te passen binnen je eigen organisatie. Vaak levert het gesprek dat daardoor ontstaat al waardevolle nieuwe inzichten op.

Net als in mijn eerdere boeken staat ook in dit boek de mens centraal. In veel publicaties over informatiebeveiliging wordt de mens vooral gezien als de zwakste schakel. Ik geloof juist het tegenovergestelde: de mens bepaalt uiteindelijk

of een organisatie veerkrachtig is. Dat begint bij medewerkers die afwijkingen herkennen, bestuurders die onder onzekerheid besluiten durven nemen, communicatieprofessionals die vertrouwen weten te behouden en IT-professionals die niet alleen systemen herstellen, maar ook bijdragen aan overzicht, samenwerking en herstel.

De belangrijkste boodschap van dit boek is dat technische maatregelen en plannen alleen waarde hebben wanneer mensen er effectief mee kunnen werken. Ook bij een huis bepalen niet alleen de sloten hoe groot de schade is, maar ook de mate waarin de bewoners zijn voorbereid wanneer het alarm afgaat.

Want uiteindelijk gaat een cybercrisis over mensen die onder grote druk de juiste keuzes moeten maken. En daarop kun je je voorbereiden.

Daarom beginnen we in hoofdstuk 1 bij de basis: wat is een cybercrisis eigenlijk?