Veel lof voor *Cybercrime en cyberwar* van Marc Goodman

Een *Wall Street Journal*-bestseller

'Voor een ijzingwekkende toer langs de duistere kanten van de technologie heb je aan Marc Goodman een eersteklas gids.'
New Scientist

'Een absolute aanrader.'
Larry King

'In *Cybercrime en cyberwar* geeft Goodman het ene na het andere voorbeeld van illegaal gebruik van technologie… De auteur sluit af met een reeks aanbevelingen die ambitieus mogen lijken, maar ook verstandig en constructief… Als we willen voorkomen dat de ergste voorspellingen uitkomen, doen we er goed aan Goodman op zijn tocht te volgen.'
Financial Times

'Een op gedegen onderzoek gebaseerd boek dat de lezer in razend tempo langs de internetcriminaliteit leidt.'
Science Magazine

'Zodra zich in cyberspace nieuwe mazen in de wet voordoen, zullen er altijd mensen zijn die daar dankbaar gebruik van maken. Lees Goodman en maak jezelf toekomstbestendig. Niemand heeft beter overzicht over de situatie dan hij, en je wilt beslist geen toetsenbord meer aanraken totdat je de inhoud van dit boek kent.'
David Eagleman, schrijver van de *New York Times*-bestseller *Incognito: het geheime leven van ons brein*

'In *Cybercrime en cyberwar* worden hacks en kraken beschreven die het goed zouden doen in een thriller, maar cybercriminaliteit is helaas maar al te echt. Je kunt je op deze rondleiding door de digitale onderwereld geen betrouwbaarder en deskundiger reisleider voorstellen dan Marc Goodman. Iedereen, maar met name het bedrijfsleven, moet zijn adviezen ter harte nemen.'
Daniel H. Pink, schrijver van *Drive* en *Verkocht!*

‘Een fascinerend boek.’
Nassim Nicholas Taleb, auteur van *De zwarte zwaan*

‘Je haren gaan overeind staan van dit lesje cybercriminaliteit. Een waarschuwing die precies op tijd komt.’
Publishers Weekly

‘Een briljant inkijkje in de verborgen wereld van criminele innovatie in de eenentwintigste eeuw… *Cybercrime en cyberwar* stelt lastige vragen over de steeds grotere rol die technologie in ons leven speelt en over de noodzaak om die te beheersen, ten behoeve van de gehele mensheid.’
Peter H. Diamandis, medeauteur van de bestseller *Abundance*; voorzitter van de XPRIZE Foundation en directeur van de Singularity University

‘Een meesterlijke pageturner die waarschuwt voor honderd inktzwarte scenario’s die je zelf nooit had bedacht. Gelukkig biedt het boek ook slimme en doortastende strategieën om ze tegen te gaan.’
Jane McGonigal, auteur van *Beter dan echt*

‘Enorm verhelderend… [Goodman] heeft dezelfde filosofie als ik: gebruik de belofte van de exponentieel groeiende informatietechnologieën om aloude problemen van de mensheid te overwinnen en zorg er tegelijkertijd voor dat je de gevaren kent en beheerst. Dit boek levert daarvoor een overtuigende routekaart.’
Ray Kurzweil, uitvinder, schrijver en futuroloog

‘Als de juiste mensen dit boek lezen, zou het de wereld wel eens kunnen redden.’
Steven Chabinsky, voormalig *Deputy Assistant Director* van de Cyber Division van de FBI

‘Dit boek geeft antwoord op de vraag wat we kunnen doen om onszelf te wapenen tegen de bedreigingen van cybercrime.’
Khoo Boon Hui, voormalig president van Interpol

Marc Goodman

Cybercrime en cyberwar

De toekomst van de misdaad in een wereld die altijd online is

Karakter Uitgevers B.V.

Inhoud

Voorwoord

De irrationele optimist: hoe ik zo geworden ben

Mijn intrede in de wereld van de hightechmisdaad begon heel onschuldig in 1995. Ik was toen achtentwintig en werkte als brigadier bij de recherche in het beroemde Parker Center, het toenmalige hoofdbureau van politie in Los Angeles. Op een dag brulde mijn superieur mijn naam door het volle, bedrijvige politiebureau: 'Goooooooodmaaan, als de sodemieter hier komen!' Ik nam aan dat ik een uitbrander zou krijgen, maar in plaats daarvan stelde de inspecteur de vraag die mijn leven zou veranderen: 'Weet jij hoe de spellingchecker van WordPerfect werkt?'

'Ja hoor, gewoon op Ctrl+F2 drukken.'

Hij antwoordde grijnzend: 'Ik wist wel dat jij de juiste man voor deze zaak was.'

Zo begon mijn carrière in het hightechpolitiewerk met mijn allereerste geval van computercriminaliteit. Ik wist hoe de spellingchecker van WordPerfect werkte, en daarmee behoorde ik begin jaren negentig tot de IT-elite van de politie. Sinds die zaak ben ik technologie, en het illegale gebruik daarvan, altijd met veel belangstelling blijven volgen. Ik ben me bewust van de schade en het kwaad die misbruik ervan kunnen aanrichten, maar de slimme, innovatieve methoden die misdadigers hanteren om hun doelen te bereiken, blijven me fascineren.

Criminelen passen hun werkwijzen voortdurend aan en nemen de allernieuwste technologieën over. De dagen dat ze als eersten met kilo's zware draagbare telefoons over straat liepen om elkaar gecodeerde be-

richten te sturen, liggen ver achter ons. Tegenwoordig zetten ze versleutelde landelijke mobiele netwerken op, zoals die van de Mexicaanse narcoticakartels. Stel je eens voor wat er allemaal bij komt kijken om over het hele land een goed werkend, versleuteld netwerk voor mobiele communicatie op te zetten: een ongelooflijke prestatie, vooral gezien het feit dat veel Amerikanen nog altijd een groot deel van de tijd geen fatsoenlijk mobiel bereik hebben.

De georganiseerde misdaad heeft naam gemaakt als *early adopter* van nieuwe technologie. Criminelen waren volop online actief lang voordat de politie daarop bedacht was en ze zijn de autoriteiten steeds een paar stappen voorgebleven. Er komen voortdurend verhalen in het nieuws over honderd miljoen gehackte accounts hier en onlinediefstal van vijftig miljoen dollar daar. Dit soort misdaad neemt hand over hand toe en ontwikkelt zich in hoog tempo de verkeerde kant op.

Het onderwerp van dit boek is niet hoe er het gisteren aan toeging of zelfs wat er op dit moment gebeurt. En ook niet hoe lang je wachtwoord zou moeten zijn. Het gaat over de toekomst. Bij mijn eigen rechercheswerk en onderzoek, eerst bij de politie van Los Angeles en daarna bij federale en internationale politie- en justitieorganisaties, heb ik criminelen opgespoord die al veel verder waren dan de cybercriminaliteit van nu en die nieuwe, net opkomende technologieën benutten, zoals robotica, virtual reality, kunstmatige of artificiële intelligentie (AI), 3D-printen en synthetische biologie. Mijn collega's bij politie- en justitiediensten over de hele wereld zijn meestal niet bekend met deze nieuwe technologische ontwikkelingen, laat staan met het toenemende gebruik dat terroristen en de georganiseerde misdaad ervan maken. Als iemand die zijn leven in dienst heeft gesteld van de maatschappij en de openbare veiligheid, maak ik me grote zorgen over de ontwikkelingen die ik overal om me heen zie.

Sommige mensen vinden misschien dat ik angst probeer te zaaien of tot op het bot pessimistisch ben, maar geen van beide is het geval. Ik ben juist een optimist, misschien wel een 'irrationele optimist', als je nagaat wat ik van de toekomst weet. Voor alle duidelijkheid: ik ben geen tegenstander van technologische vooruitgang en ik ben ook niet zo dwaas dat ik technologie als de bron van al het kwaad in de wereld beschouw. Integendeel zelfs, ik denk dat technologie ongelooflijk veel goeds kan brengen. Het kan individuen en de maatschappij bovendien op allerlei

manieren beschermen, en doet dat ook. Maar technologie is altijd een tweesnijdend zwaard geweest. Mijn ervaring met echte criminelen en terroristen op zes continenten heeft me geleerd dat misdadigers deze nieuwe technologieën zonder aarzelen zullen overnemen en inzetten tegen de bevolking. Ik wil blijven geloven in de IT-utopie die ons door Silicon Valley wordt beloofd, maar ik weet, intuïtief en omdat er genoeg bewijs voor is, dat er nog flinke hobbels genomen moeten worden en dat overheden en de industrie daar veel te weinig mensen en middelen voor vrijmaken.

In dit boek wordt beschreven welke maatschappij we met onze technologie aan het opbouwen zijn en hoe diezelfde technologische hulpmiddelen tegen ons gebruikt kunnen worden. Naarmate we onze apparaten en levens verder verknopen met het mondiale informatienetwerk (of dat nu via smartphones, sociale netwerken, liften of zelfrijdende auto's is), krijgen we meer te duchten van mensen die weten hoe de achterliggende technologie werkt en hoe ze die voor eigen voordeel en ten koste van de gewone man kunnen inzetten. Simpel gezegd: als alles met alles verbonden is, is iedereen kwetsbaar. De technologie die we als vanzelfsprekend in ons leven toelaten, vaak zonder die goed te onderzoeken of erover na te denken, kan ons nog duur komen te staan.

Door de schijnwerpers te richten op de allernieuwste ontwikkelingen in het criminele handwerk hoop ik een levendige en al veel te lang uitgestelde discussie los te maken onder mijn vrienden en collega's bij politie- en nationale veiligheidsdiensten. Hoewel zij al meer dan genoeg traditionele misdaad op hun bordje hebben, zullen ze toch iets moeten stellen tegenover de zich exponentieel ontwikkelende technologie, die op ons afkomt als een wereldwijde tsunami van mogelijke bedreigingen van ons aller veiligheid – en hoe eerder ze dat doen, hoe beter.

Maar belangrijker nog is dat ik ooit heb gezworen mijn medeburgers 'te beschermen en te dienen' en ik hen daarom wil wapenen met de feiten die ze nodig hebben om zichzelf, hun gezin, bedrijf en gemeenschap te beschermen tegen de golf aan naderende gevaren, die veel sneller zullen arriveren dan verwacht. Het is domweg niet genoeg om deze kennis alleen beschikbaar te stellen aan insiders bij de overheid, binnen de veiligheids- en beveiligingsdiensten en in Silicon Valley.

Tijdens mijn diensttijd bij allerlei overheidsorganisaties, zoals de po-

litie van Los Angeles (LAPD), de FBI, de Amerikaanse geheime dienst en Interpol, werd het me steeds duidelijker dat overal ter wereld criminelen en terroristen sneller innoveerden dan de politie en dat de *good guys* in hoog tempo steeds verder achteropraakten. Op zoek naar effectievere methoden om de groeiende schare criminelen te bestrijden die supergeavanceerde technologieën misbruiken, ben ik bij de overheid weggegaan en naar Silicon Valley verhuisd om mezelf bij te scholen over wat er nog staat te gebeuren.

Om te achterhalen hoe de nieuwste technologie uitpakt voor gewone mensen, heb ik me in Californië aangesloten bij een community van innovatieve IT'ers. Ik ben op bezoek geweest bij vertegenwoordigers van Silicon Valley, ben bevriend geraakt met mensen uit de zeer getalenteerde start-upwereld rond San Francisco Bay en werd gevraagd als medewerker van de Singularity University, een verbazingwekkende instelling op de campus van het Ames Research Center van de NASA. Daar heb ik samengewerkt met een reeks briljante astronauten, robotspecialisten, datawetenschappers, computerbouwers en synthetisch biologen. Deze pioniers zijn in staat om verder te kijken dan de wereld van vandaag en de geweldige technologische mogelijkheden te ontdekken waarmee de mensheid haar grootste uitdagingen kan aangaan.

Veel van deze ondernemers uit Silicon Valley, die zich met hart en ziel wijden aan onze technologische toekomst, hebben echter bijzonder weinig aandacht voor de beleidsmatige, juridische, ethische en veiligheidsrisico's van hun ontdekkingen voor de rest van de maatschappij. Maar omdat ik zelf criminelen in de boeien heb geslagen en in meer dan zeventig landen met politiekorpsen heb samengewerkt, kijk ik toch wat anders naar het mogelijke misbruik van de nieuwe technologieën die door onschuldige burgers vaak zonder meer omarmd worden.

Daarom heb ik het Future Crimes Institute opgericht. Daarmee wil ik mijn eigen ervaring als straatagent, rechercheur, internationaal contraterrorismedeskundige en sinds kort ook insider in Silicon Valley inzetten om een gemeenschap van gelijkgezinde experts in het leven te roepen die zich bezighouden met zowel de negatieve als de positieve gevolgen van de zich snel ontwikkelende technologie.

Als ik naar de toekomst kijk, maak ik me vooral zorgen om het feit

dat ons leven volledig is gedigitaliseerd en dat onze totale afhankelijkheid van IT ons kwetsbaar maakt op manieren waarvan maar heel weinig mensen zich überhaupt een voorstelling kunnen maken. De verwevenheid en de complexiteit van het systeem zijn groot en worden steeds groter. Toch zijn er (groepen) mensen die in hoog tempo doorkrijgen hoe het systeem werkt en in real time innoveren, ten koste van ons allemaal.

Het is het verhaal van georganiseerde criminelen, hackers, schurkenstaten, substatelijke actoren en terroristen die allemaal met elkaar concurreren om voor eigen gewin de nieuwste technologieën in handen te krijgen.

Misschien is de door Silicon Valley beloofde techno-utopie best mogelijk, maar die zal niet als bij toverslag verschijnen. Het zal burgers, overheden, bedrijven en NGO's enorme moeite, inspanningen en strijd kosten om haar tot stand te brengen. Er is sinds kort een gevecht gaande tussen de mensen die technologie ten bate van de mensheid willen inzetten en degenen die deze hulpmiddelen voor andere doelen willen misbruiken, ongeacht de schade voor anderen. Dit is de strijd om het wezen en de toekomst van de technologie. Die strijd wordt op de achtergrond gestreden, meestal sub rosa en daardoor goed verborgen voor de gemiddelde burger.

Dit boek is meer dan een opsomming van de meest recente criminele innovaties en technische achilleshielen, het schetst tevens mogelijke manieren waarop we de vele gevaren die ons wachten kunnen afwenden. Als we op de juiste wijze anticiperen, moet het volgens mij mogelijk zijn om vandaag al de misdaden van morgen te voorzien en te voorkomen, voordat we het point of no return bereiken. De toekomstige generaties zullen terugkijken en een oordeel vellen over onze pogingen om deze gevaren voor onze eigen veiligheid de kop in te drukken en het wezen van de technologie te beschermen, zodat die de mensheid uiteindelijk ten goede komt.

Tot slot een vriendelijk bedoelde waarschuwing: als je de rest van dit boek ook leest, zul je je auto, smartphone of stofzuiger nooit meer op dezelfde manier bekijken.

1

Verbonden, afhankelijk en kwetsbaar

> 'Technologie is toch iets raars: met de ene hand deelt het de mooiste geschenken uit, met de andere steekt het een mes in je rug.'
>
> CHARLES PERCY SNOW

Op het scherm zag het leven van Mat Honan er pico bello uit: onder één tabblad van zijn browser zaten foto's van zijn pasgeboren dochtertje, onder een ander streamden de tweets van zijn duizenden volgers op Twitter. Als verslaggever van het tijdschrift *Wired* uit San Francisco leefde hij het leven van de online levende stedeling en had hij minstens zoveel verstand van IT als de meeste mensen. Toch had hij er geen idee van dat zijn hele digitale wereld met slechts een paar toetsaanslagen gewist kon worden. Tot dat op een dag in augustus gebeurde. Zijn foto's, e-mails en nog veel meer vielen in handen van een hacker. Binnen een paar minuten had een tiener aan de andere kant van de wereld alles gestolen. Honan was een gemakkelijk doelwit, maar dat zijn we allemaal.

Hij herinnert zich die middag dat alles misging nog goed. Hij zat op de grond met zijn dochtertje te spelen toen zijn iPhone er plotseling mee ophield. Misschien was de accu leeg. Hij verwachtte een belangrijk telefoontje, dus sloot hij de telefoon aan op de lader en startte hem opnieuw op. In plaats van het opstartscherm en de apps die normaal verschenen, zag hij een groot, wit Apple-logo en een beginscherm in ver-

schillende talen, met het verzoek zijn nieuwe telefoon in te stellen. Vreemd.

Hij was niet echt ongerust, want hij maakte elke avond een back-up van zijn telefoon. Het was volkomen duidelijk wat hij nu moest doen: inloggen bij iCloud en zijn instellingen en data terugzetten op zijn smartphone. Toen hij op zijn Apple-account inlogde, kreeg hij de mededeling dat zijn wachtwoord, waarvan hij zeker wist dat het klopte, door de goden van iCloud niet juist was bevonden. Honan, een slimme journalist bij het belangrijkste tech-tijdschrift ter wereld, had nog een troef achter de hand. Hij zou gewoon de iPhone op zijn laptop aansluiten en de data van de harde schijf halen. Maar de moed zonk hem in de schoenen toen hij zag wat er vervolgens gebeurde.

Hij startte zijn Mac op en werd verwelkomd met een berichtje van de Apple-agenda dat zijn Gmail-wachtwoord onjuist was. Meteen daarop veranderde het fraaie bureaublad van zijn laptop: het werd asgrauw en verdween, alsof het dood was. Op het scherm was alleen een prompt te zien: VUL UW VIERCIJFERIG WACHTWOORD IN. Honan wist zeker dat hij nooit een wachtwoord had ingesteld.

Honan kwam er uiteindelijk achter dat een hacker zijn iCloud-account had gekraakt en toen met behulp van Apple's handige 'zoek mijn telefoon'-functie al zijn elektronische apparaten had opgespoord. Die werden één voor één buiten werking gesteld. De hacker gaf opdracht tot 'remote wipe' en wist zo de data die Honan zijn leven lang had verzameld, op afstand te wissen. Het eerste slachtoffer was zijn iPhone, gevolgd door zijn iPad. En als klap op de vuurpijl moest ook zijn MacBook eraan geloven. Eén tel en al zijn data waren weggevaagd, inclusief alle foto's die hij in het eerste levensjaar van zijn dochtertje had genomen. Ook de onbetaalbare foto's van al lang overleden familieleden waren weg, in de ether gekaapt door onbekenden.

Daarna werd zijn Google-account vernietigd. In een oogwenk was acht jaar aan zorgvuldig beheerde Gmail-berichten verdwenen. Zakelijke berichten, aantekeningen, geheugensteuntjes en herinneringen waren met één muisklik verwijderd. Tot slot richtte de hacker zijn aandacht op zijn uiteindelijke doel, Honans Twitternaam: @Mat. Niet alleen werd zijn account overgenomen, de hacker gebruikte dat ook om in Honans naam racistische en homofobe tirades naar diens duizenden volgers te sturen.

Na de onlineaanval zette Honan zijn journalistieke vaardigheden in om precies te achterhalen wat er was gebeurd. Hij belde naar de technische ondersteuning van Apple om zijn iCloud-account terug te krijgen. Na ruim anderhalf uur aan de telefoon te hebben gezeten, kreeg hij te horen dat 'hij' net een halfuur eerder had gebeld om zijn wachtwoord opnieuw in te stellen. Het bleek dat je alleen zijn factuuradres en de laatste vier cijfers van zijn creditcardnummer moest weten om zijn wachtwoord te wijzigen. Zijn adres was gemakkelijk te achterhalen via zijn domeinnaamregistratie bij WhoIs, waar hij zich had aangemeld toen hij zijn persoonlijke website bouwde. Maar zelfs als het daar niet had gestaan, zouden tientallen onlinediensten als WhitePages.com en Spokeo het gratis hebben verstrekt.

Om achter de laatste vier cijfers van Honans creditcard te komen, nam de hacker aan dat Honan (zoals de meeste Amerikanen) een account bij Amazon.com had. Dat had hij goed geraden. Gewapend met Honans volledige naam en zijn e-mail- en postadres nam de dader contact op met Amazon, en door een medewerker van de klantenservice te bewerken, wist hij achter de laatste vier cijfers van Honans creditcard te komen. Een paar simpele stappen en Honans leven stond op zijn kop. Hoewel dat in dit geval niet gebeurd is, had de hacker met behulp van deze informatie net zo gemakkelijk Honans onlinebank- en -effectenrekeningen kunnen plunderen.

De tiener die uiteindelijk de aanval opeiste, en die in hackerskringen bekendstond als Phobia, beweerde dat het hem erom te doen was de enorme gaten in de beveiliging van internetdiensten die we inmiddels dagelijks gebruiken, aan de kaak te stellen. Dat was hem gelukt. Honan maakte een nieuw Twitteraccount aan om met de hacker te communiceren. Phobia ging ermee akkoord om Honan, via het @Mat-account, op zijn nieuwe account te volgen. Nu konden ze direct berichten uitwisselen. Honan stelde de brandende vraag waar hij al die tijd al mee rondliep: Waarom? Waarom doe je mij dit aan? Het bleek dat de kleine tien jaar aan verloren data en herinneringen slechts een bijkomstigheid was.

Phobia's antwoord was beangstigend: 'Ik had echt niks tegen jou persoonlijk… Ik vond alleen je Twitternaam leuk.' Dat was alles. Daar was het allemaal om begonnen: een aantrekkelijke, drieletterige Twitternaam. Een duizenden kilometers ver weg wonende hacker vond hem leuk en wilde hem zelf hebben.

Het is een absurd idee dat iemand die 'niks tegen jou persoonlijk' heeft je digitale leven met een paar toetsaanslagen kan uitwissen. Toen het verhaal van Honan in december 2012 op de cover van *Wired* verscheen, trok het vrij veel aandacht – eventjes. Er volgde een discussie over betere beveiliging van alledaagse technologie, maar zoals zoveel internetdiscussies bloedde die ook dit keer dood. Sinds Honans beproevingen is er ontzettend weinig veranderd. We zijn nog even kwetsbaar als hij toen, kwetsbaarder zelfs, nu we onszelf steeds afhankelijker maken van mobiele en cloudapplicaties die gehackt kunnen worden.

Net als bij de meeste mensen waren de accounts van Honan met elkaar verbonden in een zelfreferentieel web dat was gebaseerd op vertrouwen: hetzelfde creditcardnummer voor een Apple-profiel en een Amazon-account, een Gmail-adres dat gekoppeld is aan iCloud. Allemaal hadden ze informatie gemeen, zoals inloggegevens, creditcardnummers en wachtwoorden, en alle data samen verwezen naar dezelfde persoon. Honans beveiliging was niet veel meer dan een digitale Maginotlinie, een overlappend allegaartje dat gemakkelijk te omzeilen viel. De informatie die nodig is om zijn, of jouw, digitale leven te verwoesten, is (bijna) allemaal probleemloos online te achterhalen voor iedereen die ook maar een beetje slinks of creatief te werk gaat.

Vooruitgang en gevaar in een verbonden wereld

Google zijn we in een paar jaar tijd, razendsnel en zonder er veel over na te denken, van louter zoekmachine gaan gebruiken als een middel om de weg te vinden, onze agenda en adressenbestanden bij te houden en voor video, vermaak, voicemail en bellen. Een miljard mensen hebben hun meest persoonlijke informatie op Facebook gezet en brengen vrijwillig hun sociale netwerken van familie, vrienden en collega's in kaart. We hebben miljarden keren een app gedownload en we gebruiken ze voor van alles, van het regelen van bankzaken tot koken en het bewaren van babyfoto's. We maken contact met internet via onze laptop, mobiele telefoon, iPad, digitale videorecorder, kabelbox, Playstation3, Blu-ray, Nintendo, HDTV, streamingspeler, Xbox en Apple tv.

De positieve kanten van deze technologische ontwikkeling zijn zonneklaar. In honderd jaar tijd is de levensduur van de mens dankzij de snelle vooruitgang van de medische wetenschap ruim verdubbeld en is de kindersterfte met een factor tien gedaald. Het gemiddelde voor infla-

tie gecorrigeerde inkomen per hoofd van de bevolking is wereldwijd verdrievoudigd. De toegang tot hoogwaardig onderwijs, dat heel lang buiten het bereik van heel veel mensen lag, is via websites als die van de Khan Academy tegenwoordig gratis toegankelijk. En alleen al de mobiele telefoon zou wereldwijd hebben geleid tot vele miljarden dollars aan directe economische ontwikkeling.

Door zijn basisarchitectuur zorgt het internet voor onderlinge verbondenheid en brengt het volkeren over de hele wereld op niet eerder vertoonde wijze met elkaar in contact. Een vrouw uit Chicago kan *Wordfeud* spelen met een willekeurig iemand in Nederland. Een arts uit Bangalore kan op afstand de röntgenfoto's bestuderen van een patiënt uit Boca Raton in Florida en een Zuid-Afrikaanse boer kan op zijn mobiele telefoon dezelfde gewasgegevens opvragen als een promovendus aan MIT in Massachusetts. Deze verbondenheid is een van de belangrijkste voordelen van het internet, en hoe groter het internet wordt, hoe veelzijdiger en nuttiger. Er zijn in onze moderne hightechwereld veel dingen die lof verdienen.

De voordelen van de onlinewereld zijn uitgebreid beschreven en worden door de IT-industrie vaak benadrukt. Maar al die verbondenheid heeft ook nadelen.

Het elektriciteitsnet, de luchtverkeersleiding, de brandweercentrale en zelfs de lift op kantoor zijn in hoge mate afhankelijk van computers. Elke dag vertrouwen we een groter deel van ons leven toe aan het web zonder ons af te vragen wat dat betekent. Mat Honan, en duizenden met hem, hebben op dat punt een harde les geleerd. Maar wat zou er gebeuren als al die uitingen van onze moderne maatschappij – de basistechnologie waarvan we allemaal totaal afhankelijk zijn – volledig zouden verdwijnen? Hoe ziet plan B voor de mensheid eruit? Eigenlijk is dat er niet.

De wereld is plat (en totaal onbeschermd)

De Westfaalse orde van soevereine natiestaten heeft eeuwenlang de wereld bepaald. Die orde hield in dat landen soevereiniteit over hun eigen grondgebied hadden en dat gezag van buiten zich niet in binnenlandse aangelegenheden diende te mengen. De Westfaalse orde werd in stand gehouden door een stelsel van grenzen, legers, bewaking, bewapening en slagbomen. Er konden maatregelen worden genomen om de emigra-

tie vanuit en de immigratie naar het nationale grondgebied te beperken. Bovendien konden er douane- en controlesystemen worden opgezet om de grensoverschrijdende goederenstroom te beheersen. Maar hoe vooruitziend de ondertekenaars van de Vrede van Westfalen in 1648 ook waren, op Snapchat hadden ze niet gerekend.

Hoewel fysieke grenzen nog altijd van belang zijn, zijn grenzen in de onlinewereld een stuk vager geworden. Bits en bytes stromen vrijelijk van het ene land naar het andere en worden niet gehinderd door grenswachten, immigratiebeperkingen en douaneaangiftes. De traditionele landsgrenzen waar boeven, tuig en veroordeelden van eerdere generaties op stuitten, bestaan in de onlinewereld niet meer, wat ongure individuen de vrijheid geeft om virtuele locaties naar believen te betreden en weer te verlaten.

Denk daar eens over na, en over de gevolgen voor onze veiligheid. Als criminelen vroeger op Times Square in New York een bank wilden beroven, dan sprak een aantal dingen voor zich. Om te beginnen kon je ervan uitgaan dat de daders een fysieke locatie waren binnengedrongen binnen de grenzen van het politiedistrict Midtown South. De overval was een misdrijf volgens zowel het federale recht als het recht van de staat New York, en de New Yorkse politie en de FBI waren samen bevoegd om de zaak te onderzoeken. Het slachtoffer (in dit geval de bank) was ook fysiek gevestigd in het rechtsgebied van de betrokken opsporingsinstanties, wat het onderzoek aanzienlijk vergemakkelijkte. Pogingen om de zaak op te lossen werden onderbouwd met fysiek bewijs dat de bankrover op de plaats delict moest hebben achtergelaten, zoals vingerafdrukken op een briefje dat hij aan de kassier had overhandigd of DNA-materiaal op de balie waar hij overheen was gesprongen, mogelijk aangevuld met beelden van de bewakingscamera's van de bank. Bovendien golden voor het misdrijf zelf ook bepaalde fysieke grenzen. Het gestolen geld had een bepaalde omvang en gewicht, en je kon er slechts een beperkte hoeveelheid van meenemen. En misschien waren de stapels bankbiljetten beveiligd met een verfbom, wat de politie een aanwijzing omtrent de dader zou opleveren. Maar zulke beproefde, vaststaande onderzoeksgegevens, zoals fysiek bewijs en een gemeenschappelijke jurisdictie, bestaan in de wereld van vandaag vaak niet meer.

Laten we die denkbeeldige kraak op Times Square eens vergelijken met de beruchte internetbankroof die Vladimir Levin in 1994 pleegde

vanuit zijn woning in Sint-Petersburg. Computerprogrammeur Levin werd ervan beschuldigd de rekeningen van enkele grote zakelijke klanten van Citibank te hebben gehackt en 10,7 miljoen dollar te hebben weggesluisd. Met handlangers over de hele wereld maakte hij grote bedragen over naar rekeningen in Finland, de Verenigde Staten, Nederland, Duitsland en Israël.

Wie was er bevoegd in deze zaak? De politie in de VS, waar het slachtoffer (Citibank) was gevestigd? Of die in Sint-Petersburg, vanwaar de verdachte het misdrijf zou hebben gepleegd? Of toch een instantie in Finland of Israël, waar het gestolen geld elektronisch op valse bankrekeningen werd gestort? Levin heeft het misdrijf gepleegd zonder ooit een voet in de VS te hebben gezet. Hij heeft vingerafdrukken noch DNA-sporen achtergelaten en is nooit met verf besmeurd door een exploderende plofkoffer. Belangrijk is ook dat hij nooit duizenden kilo's aan contanten de bank uit heeft hoeven dragen; meer dan een muis en een toetsenbord heeft hij niet gebruikt. Een bivakmuts of een afgezaagd geweer waren evenmin nodig. Lewin verborg zich simpelweg achter zijn computerscherm en volgde een ingewikkelde virtuele route om zijn digitale sporen te wissen.

Door de aard van het internet leven we steeds meer in een wereld zonder grenzen. Vandaag de dag kan iedereen, met goede of slechte bedoelingen, met de snelheid van het licht virtueel de halve wereld rondreizen. Voor criminelen is deze technologie enorm handig. Zij hoppen van het ene land naar het andere en hacken zich een weg door de virtuele wereld in een poging de politie te slim af te zijn. Ze hebben ook geleerd hoe ze kunnen voorkomen dat ze online gevolgd worden. Een handige hacker zal nooit vanuit zijn eigen huis in Frankrijk een aanval op een bank in Brazilië uitvoeren. Hij zal die aanval laten verlopen via allerlei besmette netwerken: van Frankrijk via Turkije naar Saudi-Arabië en uiteindelijk naar zijn doelwit in Brazilië. Dat je van land naar land kunt springen is een van de grootste voordelen van het internet, maar het bezorgt de politie enorme administratieve en bevoegdheidsproblemen, en het is een van de redenen dat onderzoeken naar cybercrime vaak zo moeizaam en inefficiënt verlopen. De politie in Parijs heeft niet de bevoegdheid om in São Paulo iemand te arresteren.

Bijlage

Alles is met elkaar verbonden, iedereen is kwetsbaar. Dit kun je eraan doen.

In dit boek hebben we de technologische gevaren onderzocht die de maatschappij bedreigen en hebben we diverse manieren bekeken om de risico's systematisch te verminderen. In het update protocol, dat hieronder staat, staan een paar praktische tips die je kunt gebruiken om jezelf, je bedrijf en je naasten te beschermen tegen de meest gangbare technologische gevaren. Volg deze stappen (het digitale equivalent van de huisdeur op slot doen en je autosleutels niet in het contact laten zitten) en je kunt meer dan 85 procent van de digitale bedreigingen voorkomen.

Update regelmatig
Moderne softwareprogramma's zijn vergeven van bugs. Hackers en criminelen gebruiken deze zwaktes om in je computer en andere apparatuur in te breken, je geld te stelen en chaos te veroorzaken. Voorkom deze problemen door de software van je besturingssysteem, computerprogramma's en apps automatisch te updaten. Let vooral op browsers, plug-ins, mediaspelers, Flash en Adobe Acrobat, dat zijn de favoriete doelwitten van slechteriken om jou een poot uit te draaien. Als je niet automatisch updatet is je apparatuur kwetsbaar, wat voorkomen kan worden door je software simpelweg tijdig te updaten.

Wachtwoorden

Wachtwoorden horen lang te zijn (denk aan twintig karakters of meer) en bevatten kleine letters, hoofdletters, symbolen en spaties. We hebben het natuurlijk al duizenden keren gehoord, maar een sterk wachtwoord is de belangrijkste factor bij de bescherming van je accounts en het moet regelmatig worden veranderd. Gebruik nooit hetzelfde wachtwoord voor verschillende sites. Doe je dat wel, dan hebben hackers toegang tot je logingegevens die ze vervolgens voor meerdere domeinen kunnen gebruiken, van je socialemedia-account tot je bankrekening. Maar om voor elke account zo'n lang en uniek wachtwoord te onthouden vraagt meer dan je hersens aankunnen. Gelukkig zijn er talloze wachtwoordmanagers die dit proces betrekkelijk pijnloos van je kunnen overnemen. Het is bekend dat criminelen eigen wachtwoordmanagers hebben gecreëerd om te proberen jou je digitale kroonjuwelen te ontfutselen. Gebruik daarom alleen managers van bekende ondernemingen zoals 1Password, LastPass, KeePass en Dashlane, waarvan de meeste zowel op je computer, smartphone als tablet werken. Daarnaast zijn er veel diensten zoals Google, iCloud, Dropbox, Evernote, PayPal, Facebook, LinkedIn en Twitter die met een dubbele authenticatie werken, waarbij je bij elke login een wachtwoord krijgt toegestuurd, meestal via een sms'je of een appje rechtstreeks op je mobiele telefoon. Zo'n authenticatie met twee factoren houdt in dat je wachtwoord, zelfs als dat gehackt is, niet gebruikt kan worden zonder de tweede factor (de fysieke toegang tot jouw mobiele telefoon).

Downloaden

Download alleen software van officiële sites (zoals de App Store van Apple of rechtstreeks van een geverifieerde eigen website van een bedrijf). Bekijk onofficiële appstores met het nodige wantrouwen, net als sites van derden die 'gratis' software aanbieden. Vermijd daarnaast gestolen media en software die overal verkrijgbaar is op peer-to-peernetwerken; die bevatten vaak malware en virussen. Via de instellingen in zowel het Windows- als Mac-besturingssysteem kun je een 'witte lijst' maken zodat er alleen goedgekeurde software van bekende leveranciers op jouw machine wordt gebruikt. Daarmee ben je niet helemaal veilig wat betreft software, maar de kans op besmetting wordt zo sterk verminderd. Let goed op wat je toestaat bij apps. Ze zijn niet voor niets