CODE ROOD

Tekst: Ramses Sloeserwij
Met dank aan Richard van der Kraan & Maurits van den Heuvel
Foto omslag: Susan Dammingh
Vormgeving: Studio Spade
ISBN: 978-90-825499-6-6

VOORWOORD

7 mei 2021 kwam het bericht naar buiten dat het Texaanse oliebedrijf Colonial Pipeline geraakt was door een ransomware–aanval. De cybercriminelen vroegen losgeld in de vorm van cryptovaluta. Na het betalen van 4,4 miljoen dollar werd de digitale gijzeling op 12 mei opgeheven. Gevolg was wel een totale verstoring van het dagelijkse leven. Grote run op brandstof, ellenlange rijen bij tankstations en verhoogde brandstofprijzen. Kort daarvoor kwam ook het nieuws naar buiten dat Russische cybercriminelen wisten te infiltreren in de beheersoftware van IT– bedrijf SolarWinds om daarmee een zogenaamde supply-chainaanval uit te kunnen voeren. Het gevolg hiervan was ongewenste toegang tot minstens 18.000 overheids- en particuliere netwerken, waaronder zelfs het Pentagon. Dit zijn slechts twee zeer recente voorbeelden, en we kunnen ervan uitgaan dat er meer en nog grotere cyberaanvallen zullen volgen. We moeten cyberaanvallen niet langer beschouwen als incidenten, want op de lange termijn is dat zeer gevaarlijk: cyberaanvallen raken het hart van onze maatschappij. Recent waarschuwde Huib Modderkolk er al voor in zijn boek '*Het is oorlog maar niemand die het ziet*'. En zoals Johan Cruijff het ooit al eens zei: '*Je ziet het pas als je het door hebt*'. Met andere woorden: als je er even meer aandacht aan besteedt, zie je een schrikbarende toename. Een toename waardoor we van lieverlede mogen spreken over een Code Rood-situatie. Het cyberdomein staat wat dat betreft figuurlijk in brand.

Wat is er aan de hand? Waardoor komt dat? Dit boek probeert hierop een antwoord te geven. Wat verzwakt ons cyberdomein en hoe kunnen we dat tegengaan? Welke cyberactoren zijn er, waardoor raken ze gemotiveerd en hoe gaan ze te werk? Om je te kunnen verdedigen, moet je weten wie je vijand is en welke strategie deze hanteert.

Internet heeft echt een volgende stap in de evolutie van de mens veroorzaakt. Naast de fysieke wereld ontstaat een totaal nieuwe wereld, een virtuele wereld: het cyberdomein. Een wereld die langzaam maar zeker een steeds grotere invloed gaat krijgen op de fysieke wereld. Kijk bijvoorbeeld naar de ontwikkelingen in China rond surveillancesystemen en het Social Credit System. Dit klinkt voor de Nederlander ver weg maar onze eigen coronamelder-app heeft al een eerste aanzet hiertoe gegeven. Trek deze lijn maar eens door naar de toekomst.

INHOUD

2. CODE ROOD SAMENVATTING OORZAKEN

Het cyberdomein is nog jong en daarom realiseert niet iedereen zich hoe gevaarlijk dit domein is. Zo is bijvoorbeeld op Hackmageddon.com — een website die alle cyberaanvallen registreert en deze op alle manieren statistisch weergeeft— te zien dat het werkelijke aantal cyberaanvallen nog altijd jaarlijks toeneemt. Van 1337 aanvallen in 2018 naar 2539 in 2021 — haast een verdubbeling in enkele jaren. En deze trend zal zeker verder doorzetten.

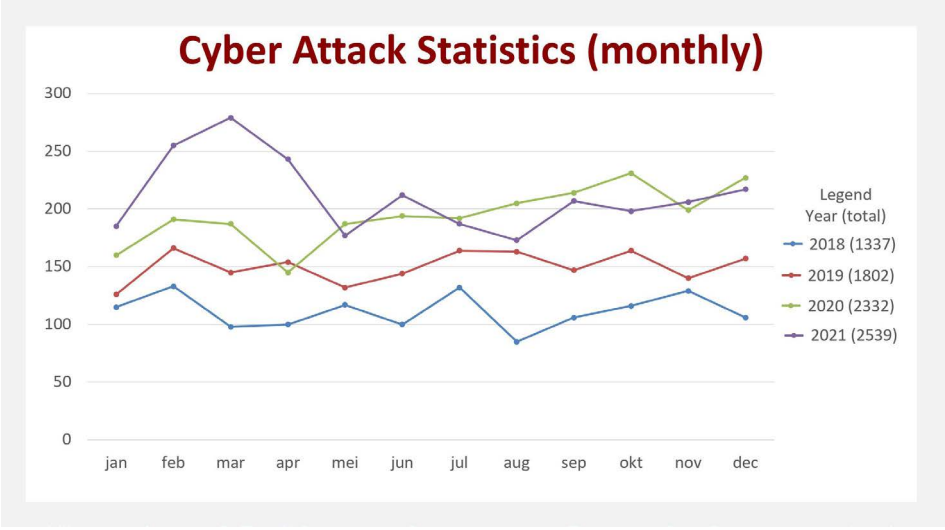

Fig. 2: Aantal cyberaanvallen tussen 2018 en 2021.

Deze toename blijkt niet alleen uit het aantal cyberaanvallen maar ook uit de jaarlijkse financiële schade die het veroorzaakt. Want als we kijken naar de totale schade die in de Verenigde Staten bij het Internet Crime Compliant Center (IC3) is geregistreerd, dan zien we dat het bedrag aan schade van 2001 tot 2020 een nagenoeg identieke verdubbeling toont.

In de laatst gerapporteerde periode bedroeg het verlies aan cybercriminaliteit 4,2 miljard dollar, tegen 1 miljard dollar in 2015. Goed, dit zijn cijfers uit de Verenigde Staten, maar het is aannemelijk dat deze stijging ook in de rest van de wereld te zien zal zijn. Overigens geldt dit niet alleen voor westerse welvarende landen, want cybercriminelen verdienen evengoed aan minder welvarende landen.

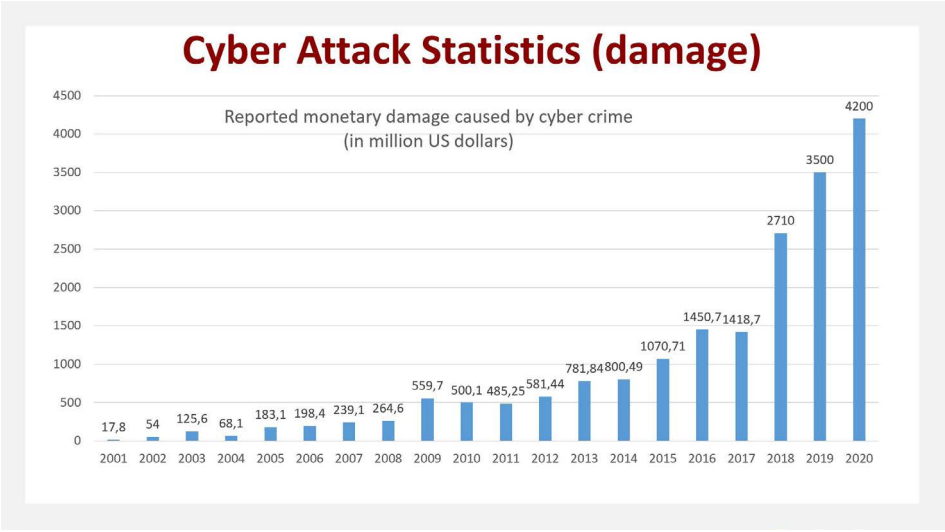

Fig. 3: Financiële schade in de VS door cybercriminaliteit.

Als we naar het aantal buitgemaakte datarecords kijken, gaan helemaal alle alarmbellen af. Zo laat een studie van Selfkey.org zien — dat is een organisatie die zich inzet voor identiteitsbeveiliging — dat er elke twee seconden een nieuw persoon slachtoffer is van identiteitsdiefstal. Ook deze studie richt zich weer alleen op de Verenigde Staten maar de uitkomsten mogen natuurlijk ook de rest van de wereld zorgen baren.

Deze criminaliteitstoename is niet enkel toe te schrijven aan het uitdijende cyberdomein. Er zijn hier meerdere ontwikkelingen debet aan, zoals ontwikkelingen op technologisch, menselijk en maatschappelijk gebied. Denk aan de combinatie van vergrijzing, digibetisme, oude gewoontes, geopolitieke spanningen en de lage pakkans van cybercriminelen. Deze oorzaken versterken elkaar, waardoor er een synergetisch effect ontstaat. Parallel daaraan zie je dat statelijke actoren zich steeds offensiever opstellen en misbruik maken van de nieuwe kansen en mogelijkheden uit het cyberdomein. Daarnaast worden cybercriminelen steeds professioneler en volhardender. Met andere woorden: het geheel wordt groter en kwetsbaarder terwijl aan de andere kant de dreiging groter wordt.

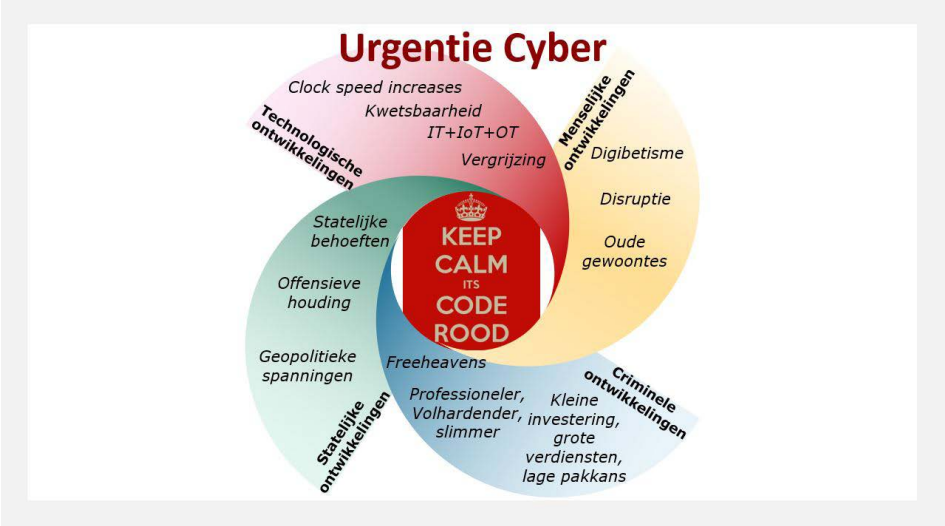

Fig. 4: Synergie tussen verschillende ontwikkelingen leidt tot een versnelde cyberdreiging.

2.1 Technologische ontwikkelingen

Technologische footprint veroudert steeds sneller
Technologische ontwikkelingen gaan steeds sneller — haast exponentieel. Hierdoor ontstaat een Technology Push-markt, waardoor chips steeds sneller werken (de *clock speed increases*) de levenscyclus van producten steeds korter wordt en de veroudering, ook wel vergrijzing genoemd, sneller toeneemt. Als direct logisch gevolg daarvan neemt de kwetsbaarheid ook toe.

Technologische footprint wordt steeds groter (IT + IoT + OT)
Steeds meer productonderdelen worden uitgerust met internettechnologie en deze worden vervolgens op het internet aangesloten. Naast een groeiend Information Technology (IT)-park, groeit ook het Internet-of-Things (IoT), maar worden ook steeds meer Operational Technology (OT)-componenten op het internet aangesloten. Hierdoor groeit onze totale technologische footprint explosief. Daarnaast neemt het aantal onveilige componenten zoals IoT- en OT-componenten ook steeds meer toe. Gevolg hiervan is dat we steeds kwetsbaarder worden, onze *attack surface* wordt vergroot.

Aantal zwakheden (vulnerabilities) neemt jaarlijks toe
Zwakheden of *vulnerabilities* zijn inherent aan geprogrammeerde softwareregels. Ondanks dat gevonden zwakheden worden verholpen — dankzij *security patches* — introduceren we ook steeds weer nieuwe kwetsbaarheden.

Complexiteit van de totale technologische footprint neemt verder toe
Organisaties maken in toenemende mate gebruik van technologische diensten van derden, in diverse uiteenlopende vormen — denk aan O*n-premise, private/public/hybrid Cloud, PaaS/SaaS* — wat de totale technologische footprint diffuus maakt.

2.2 Menselijke ontwikkelingen

Toenemend digibetisme
Naarmate mensen ouder worden, hebben ze steeds meer moeite om met de digitale wereld om te kunnen gaan; er ontstaat digibetisme.

Steeds groter wordende disruptie
Technologie ontwikkelt zich haast exponentieel maar het menselijke aanpassingsvermogen volgt niet eenzelfde ontwikkeling, deze is eerder lineair. Niet alleen individuen, maar zelfs hele organisaties kunnen en zullen dat tempo niet meer bijhouden. Er ontstaat een ontwrichting of disruptie.

Vasthouden aan oude gewoontes/oud denken
Mensen maar ook organisaties houden zich graag vast aan oude gewoontes. Immers: het verleden heeft aangetoond dat deze werken. Het vermogen om zich continu aan te passen is slechts beperkt.

Beperkt lerend vermogen
De wil om te leren van fouten van andere organisaties is maar zeer beperkt. Criminelen hanteren vaak een vast patroon in hun aanval. Verandering is niet noodzakelijk omdat andere organisaties hier toch niet van leren.

Security-fundamentalisme
Security moet business mogelijk maken maar door de tijd heen worden security-functionarissen zodanig geconditioneerd dat zij niet meer denken in mogelijkheden. Elk risico roept weerstand op waardoor ze houvast vinden in 'kan niet, mag niet'.

2.3 Ontwikkelingen statelijke actoren
Het cyberdomein wordt door vrijwel alle krijgsmachten beschouwd als het vijfde operationele domein. Diverse landen, en dan niet alleen de 'usual suspects', maken er maar al te graag handig gebruik van om uiteenlopende redenen. Een aantal daarvan is bovengemiddeld actief in dit domein en haalt geregeld op zeer negatieve wijze het nieuws, waaronder: