Een continue stroom van cyberaanvallen

Het Duitse parlement bleek deze week slachtoffer van een hack, een digitale inbraak. Cyberaanvallen vinden continu plaats en chaos creëren is simpel. Zijn we wel gewapend tegen deze digitale dreiging?

TEKST **Kristel van Teeffelen**

Gekleurde lijnen verschijnen op de wereldkaart als raketten die kort na elkaar worden afgevuurd. Vanuit Rusland naar Europa, van Azië naar Afrika en van Europa naar de Verenigde Staten: ze vertrekken vanuit alle delen van de wereld en richten zich op hun doelen ergens anders op de kaart. Soms worden ze dikker, dan weer nemen ze in hevigheid af.

De lijnen vertegenwoordigen verdacht internetverkeer. Cyberaanvallen dus. Waargenomen door het systeem van Norse, een Amerikaans bedrijf dat met allerlei sensoren het internet monitort (zie kader). De informatie is bedoeld voor cyberspecialisten van bedrijven en overheden die met die aanvallen te maken krijgen.

Naar de constante stroom gekleurde lijnen op de kaart kijken, is even fascinerend als beangstigend. Het drukt je met de neus op het feit dat cyberaanvallen aan de orde van de dag zijn. Een continue stroom gevaarlijk internetverkeer, met uiteenlopende doelen.

Voor de gemiddelde burger blijven veel van de incidenten onbekend. Maar specialisten waarschuwen al jaren voor de maatschappelijke gevolgen van cyberaanvallen. Vooral nu het leven zich steeds meer op internet afspeelt en bijna alles met het web is verbonden. Dat erkent ook verantwoordelijk staatssecretaris Klaas Dijkhoff: de dreiging van cyberaanvallen die de 'maatschappelijke orde verstoren' is hoog.

Natuurlijk laat de kaart van Norse niet zien of de aanvallen ook succesvol zijn. Misschien zit je te kijken naar een verwoede poging van hackers om een bedrijfsnetwerk plat te leggen. Toch zijn ook die pogingen relevant, zegt Jaap Schekkerman, hoofd van de afdeling cybersecurity bij IT-dienstverlener CGI. Het is een manier voor hackers om af te tasten: is een systeem te kraken? En als ik eenmaal binnen ben: wat gebeurt er dan? "Daarna volgen dan vaak de meer gerichte aanvallen, waarbij gebruik wordt gemaakt van de zwakke plekken die ze bij het aftasten hebben gevonden."

Poen of politiek

Of de criminelen succesvol zijn met hun cyberaanval, hangt ook af van hun doel. Dat kan redelijk basaal zijn: geld verdienen. In 2013 bleek dat de Antwerpse haven was gehackt door criminelen die zo grote hoeveelheden harddrugs Europa binnensmokkelden.

Het begon met een simpele *phishing-mail*, zoals iedereen die wel eens binnenkrijgt: een e-mail, zogenaamd afkomstig van de bank of een zakenpartner, maar die in werkelijkheid een computer besmet met een virus. Uiteindelijk konden de criminelen via de netwerken van een havenbedrijf precies volgen waar hun containers met drugs waren en zo als eerste bij de haven klaarstaan om de lading op te pikken.

Criminelen hackten de haven van Antwerpen en konden via de netwerken van de haven volgen waar hun containers met drugs waren

Maar het gaat hackers niet altijd om geld. Het kan ook zijn dat ze willen ontregelen of shockeren, al dan niet om politieke redenen. Deze week nog werd de website van het Amerikaanse minister van defensie gehackt door een groep die zichzelf het 'Syrische Elektronische Leger' noemt. In april was de Franse tv-zender TV5Monde aan de beurt, die zelfs even helemaal op zwart ging.

Ook niet te onderschatten zijn de hoeveelheid aanvallen vanwege spionage. Daar lijkt het Duitse parlement slachtoffer van. Experts zijn al een maand bezig om *malware* van de computers af te krijgen die zich diep in de systemen heeft genesteld.

Hoewel nog niet is bevestigd dat een staat achter de aanval zit, ligt dat vanwege de complexiteit van de malware wel voor de hand, zegt Albert Kramer, technisch expert bij beveiligingsbedrijf Trend Micro. Zulke aanvallen kosten veel tijd en geld.

Ook Nederland heeft met spionage te maken. Het Nationaal Cyber Security Centrum (NCSC) in Den Haag constateerde in het laatste rapport over de cyberdreiging dat het gevaar van digitale spionage onverminderd groot is, dat het groter wordt en toeneemt in complexiteit en impact.

De tijd dat het gewoon lollig was om iets te hacken is echt voorbij, zegt Raimund Genes, hoofd technologie van Trend Micro. "Nu steeds meer systemen zijn aangesloten op het internet, van bruggen tot dammen, van elektriciteitscentrales tot de spoorwegen, kun je mensen echt pijn doen. Ik vrees alleen dat dat besef pas komt als er bloed op straat ligt."

Genes doelt op onze kritieke infrastructuur: de bedrijven die zich bezighouden met energie, olie, gas, defensie, water, transport, telecom en financiën. Als die geraakt worden kan dat serieuze schade opleveren voor de samenleving en voor de economie.

Hoe vaak zulke doelen in Nederland aangevallen worden via internet, weten we niet precies. Bij de NCSC komen wel meldingen binnen: in 2014 ging het om 713 gevallen. Maar bedrijven zijn niet verplicht om bij problemen naar het cybersecuritycentrum van de overheid te stappen. Nog niet, want als het aan het ministerie van veiligheid en justitie ligt, komt zo'n meldplicht er wel. Een wetsvoorstel daartoe gaat nog voor de zomer naar de Raad van State voor advies, zegt een woordvoerder.

Kwetsbare stroom

De incidenten die worden gerapporteerd, zijn het topje van de ijsberg, denkt Jaap Schekkerman. Hij is bij CGI onder meer gespecialiseerd in het digitaal beschermen van elektriciteitscentrales. Dat is de sector die volgens hem het meeste wordt aangevallen. Schekkerman gaat er vanuit dat er dagelijks wel ergens een probleem is, ernstig of minder ernstig.

Raimund Genes bevestigt dat beeld. "Afgelopen jaar zag mijn team bij Trend Micro wel 8000 incidenten rond zwakke plekken in systemen. De meeste komen niet in de publiciteit. Als wij zwakke plekken tegenkomen, waarschuwen we organisaties. Pas als ze er na drie maanden niets aan hebben gedaan, maken we het openbaar. Ik vind het namelijk geen grap als het om de kritieke infrastructuur gaat. Dat moet worden opgelost."

Zo nu en dan haalt een gebeurtenis wel de publiciteit. Zoals malware die in 2012 actief werd op duizenden werkplekken van oliegigant Saudi Aramco. De aanval was goed gepland: niemand was op kantoor vanwege een nationale feestdag. Bijna driekwart van de documenten, e-mails en files werd van de computers gewist, het bedrijf in grote problemen achterlatend.

Nog een voorbeeld: in Turkije explodeerde in 2008 een olieleiding, met grote schade tot gevolg. Onlangs werd bekend dat dat hoogstwaarschijnlijk het gevolg was van een cyberaanval.

Er zijn niet eens explosies nodig om effect te hebben, zegt Genes. Ook op het oog onschuldige aanvallen kunnen grote gevolgen hebben. "Toen het Twitter-account van persbureau Reuters was gehackt en er berichten verschenen over een bomaanslag in het Witte Huis, daalden de koersen op de beurzen. Hackers kunnen met zulke acties veel geld verdienen."

Maar wat moet de burger daarmee? Moeten we ons zorgen maken? Dat zou vooral de overheid moeten doen, vindt Genes. Hoewel het niet alle problemen zal oplossen, pleit hij op zijn minst voor een minimale standaard voor de bescherming van belangrijke systemen, opgelegd door de overheid.

Genes: "De eindgebruiker zal altijd voor gemak kiezen. Een bedrijf zal altijd voor de winst gaan. Daarom moeten overheden het doen. Laat ze reguleren hoe kritieke infrastructuren minimaal beschermd moeten worden. Als Europa zouden we dat samen moeten regelen. Eén Europa kun je niet negeren als bedrijf."

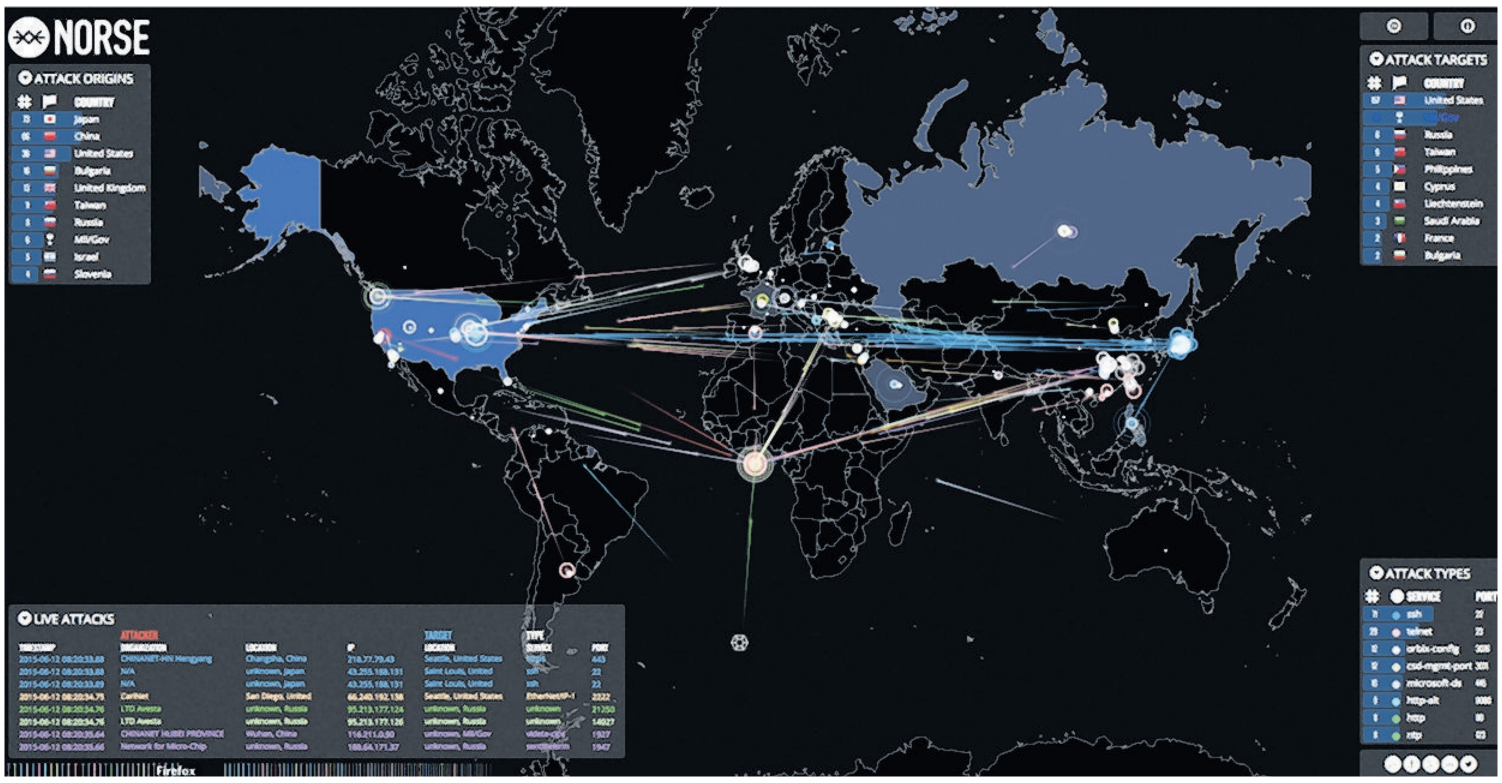
Genes ergert zich aan overheden die bezig zijn het tegenovergestelde te doen: ze verzwakken systemen. Zo doen regeringen volgens

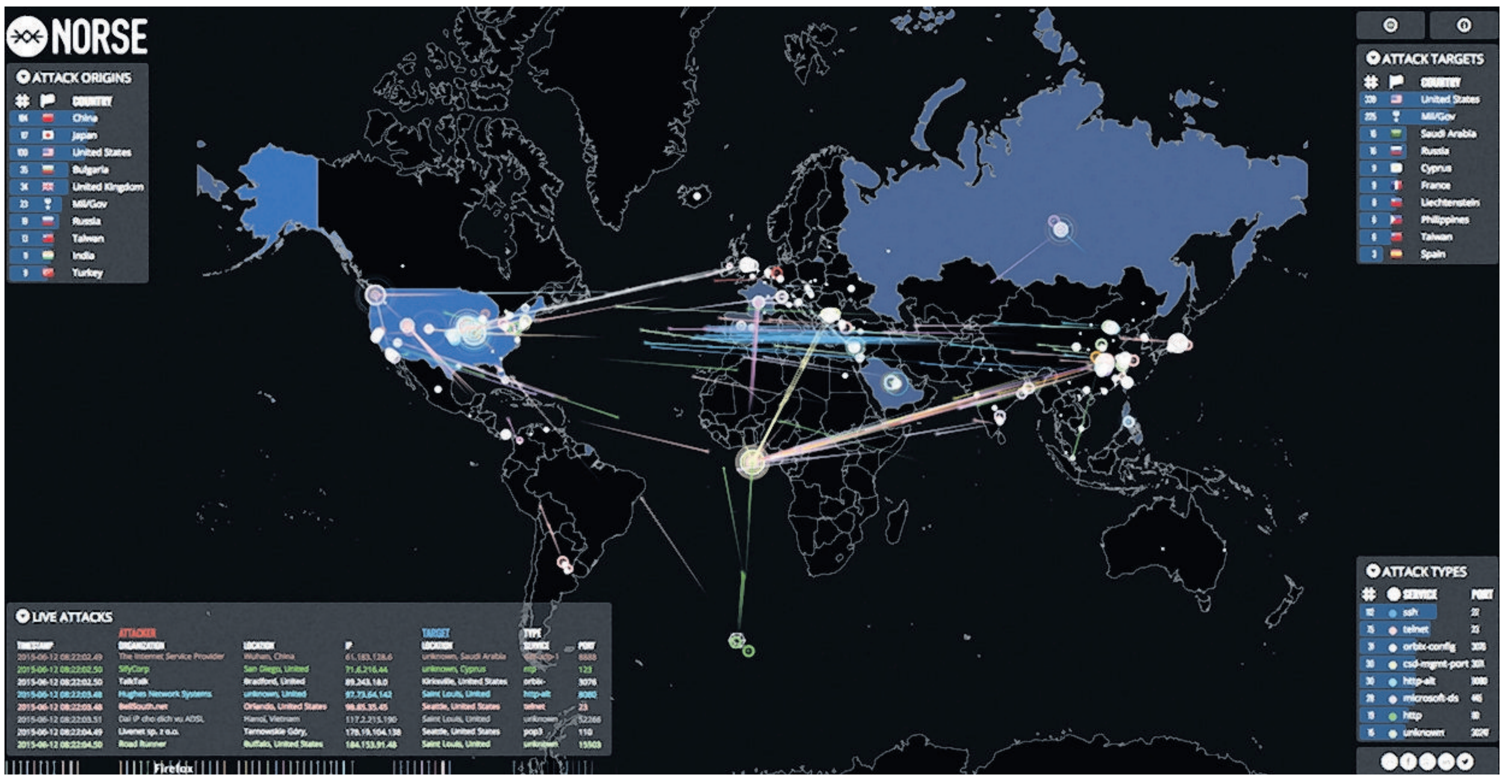
Hoe werkt Norse?

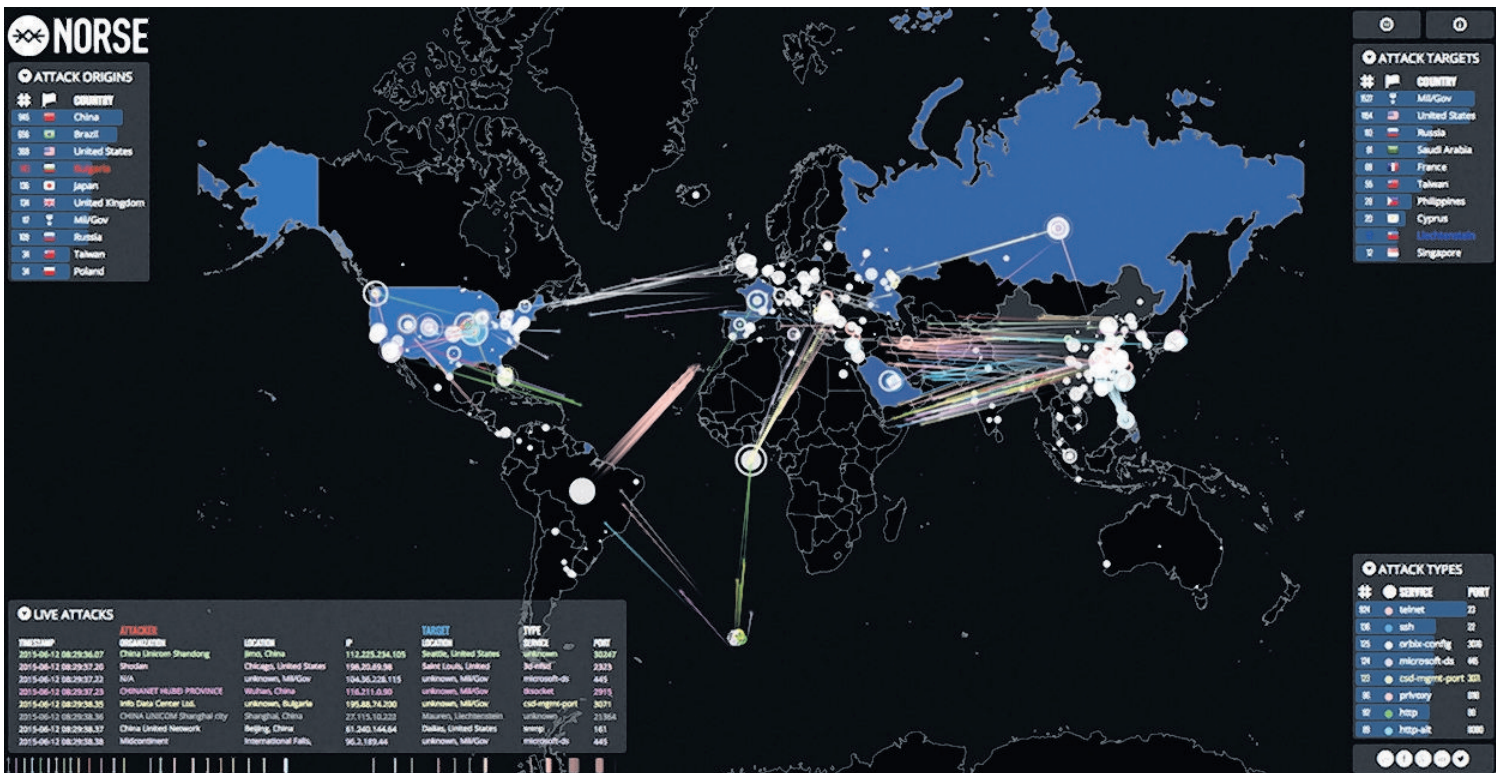
Norse heeft op honderden locaties in zo'n vijftig landen sensoren op het internet geplaatst. Die verzamelen en analyseren continu informatie, ook over de methode die hackers gebruiken bij de cyberaanval. Vooral *darknets* zijn interessant voor Norse. Dat is het deel van het internet dat niet via zoekmachines te doorzoeken is en waar de gemiddelde internetter niet zal komen. Cybercriminelen maken er daarentegen graag gebruik van.

De aanvallen die worden getoond op de wereldkaart op de website van Norse, zijn gebaseerd op het internetverkeer tegen onder meer de zogeheten *honeypots* die Norse gebruikt. Honeypots zijn te vergelijken met een lokfiets tegen fietsdiefstallen. De cyberaanvallen op die loksystemen worden gemeten en geven volgens Norse een representatief beeld van de actuele wereldwijde aanvallen. "Het ziet er misschien eng uit", zegt een woordvoerder van het bedrijf. "Maar het is eigenlijk erger. Om de visualisatie te versimpelen, zie je op de wereldkaart maar 1 op de 1000 hits op ons netwerk."

> *‘Steeds meer systemen zijn aangesloten op internet. Hackers kunnen mensen echt pijn doen.’*







Drie momentopnames van verdacht internetverkeer, waargenomen door het bedrijf Norse op vrijdagochtend (Nederlandse tijd) 12 juni. De lichtlijnen geven het verkeer weer, de rondjes zijn de doelen. Zelf meekijken naar het verkeer: zie map.ipviking.com

hem mee aan de handel in *zero days*. Dat zijn tot dan toe onbekende zwakke plekken in computersystemen die misbruikt kunnen worden. Overheden gebruiken die achterdeurtjes om zelf te spioneren, zonder melding te maken van het bestaan ervan, aldus Genes.

Ook Jaap Schekkerman benadrukt het belang van een minimale standaard. “Neem de energiesector. Als de stroom eruit ligt, zijn de gevolgen groot. Maar de kosten voor een goede online bescherming zijn hoog. Mag je van partijen verwachten dat ze er in investeren? Of vindt de overheid het zo belangrijk dat de energiemaatschappij die kosten mag doorberekenen in de energieprijs?”

Als de impact na een hack zo groot is, waarom zijn al die belangrijke systemen dan verbonden aan het internet? Dat heeft vooral met gemak te maken, zeggen de specialisten. Zo kunnen bruggen of sluizen van een afstandje worden bediend en hoeven ze niet meer te worden bemand. Of het functioneren van een systeem kan op afstand worden gecontroleerd.

Schijnveiligheid

Vorig jaar liet de Nederlandse regering nog onderzoeken of het mogelijk is om belangrijke bedrijven of overheidsdiensten niet aan het ‘gewone’ internet te verbinden, maar aan een speciaal beveiligd gescheiden netwerk. Onrealistisch, was de conclusie van consultant PWC. Zo is een gescheiden netwerk niet alleen duur, maar creëert het ook een schijnveiligheid. Zo’n speciaal netwerk waar allerlei belangrijke systemen op draaien kan juist een aantrekkelijk doelwit zijn van gerichte cyberaanvallen.

Bovendien draait het niet alleen om digitale beveiliging. Want hoe goed je de digitale weg ook dichttimmert, indringers kun je nooit helemaal buitensluiten. Schekkerman: “Menselijk gedrag is bijna altijd de zwakke schakel. Mensen zijn makkelijk te verleiden tot handelingen die ze eigenlijk niet moeten uitvoeren. Het is vaak de eerste stap voor een kwaadwillende om binnen te komen. Zoals via een usbstick die besmet is met malware en in een computer wordt gestopt. Of via een phishingmail.”

Het Duitse parlement heeft het geweten. Maar de lijnen op de wereldkaart van Norse lijken tot nu toe in Nederland nog weinig écht grote problemen te hebben veroorzaakt. Tenminste, voor zover we weten. Is het wachten tot één van die cyberaanvallen de samenleving wel ernstig weet te ontwrichten?

“Dat is moeilijk te voorspellen”, zegt Schekkerman. “Maar chaos is niet zo moeilijk te veroorzaken. Schakel een elektriciteitscentrale uit en het is al zover.”