VOORWOORD

Cybercriminaliteit is met stip bezig de meest lucratieve vorm van criminaliteit te worden en daarom staat cybersecurity meer dan ooit in de belangstelling. De verdergaande digitalisering en de toenemende afhankelijkheid van IT zijn koren op de molen voor hackers en andere cybercriminelen. Marc Andreessen – bedenker van de internetbrowser en toonaangevend investeerder in Silicon Valley – stelde lang geleden al dat *software is eating the world*. Dat steeds meer apparaten softwarematig worden aangestuurd via internet, maakt het

voor hackers interessant om bekende kwetsbaarheden uit te buiten en aanvallen op te zetten.
De schade van cybercriminaliteit wordt in Nederland geschat op 8,8 miljard euro, ongeveer 1,5 procent van het bruto nationaal product. Wereldwijd wordt de schade geraamd op 325 miljard, zo'n 0,8 procent van de wereldeconomie. Onlangs berekende het CBS dat cybercrime in geld vermogensdelicten overschrijdt. Als oorzaken van cyberschade geldt op dit moment de volgende top drie (in volgorde van schadegrootte):

- schadelijke of criminele aanvallen;
- nalatigheid van personeel;
- verstoring of niet-beschikbaarheid van ICT.

Het wordt voor bedrijven steeds lastiger om weerbaar te blijven tegen cyberrisico's. Het veranderende 'dreigingslandschap' vraagt in combinatie met de verdere digitalisering en strengere wet-

geving om een doortastende, continue en waar mogelijk preventieve aanpak tegen cyberrisico's door particulieren en organisaties, klein en groot. Wat kun je ertegen doen? Verschillende instanties zijn naar aanleiding van onderzoek tot de conclusie gekomen dat preventieve maatregelen alleen niet meer afdoende zijn om weerbaar te blijven tegen cyberrisico's. Gerenommeerde onderzoeksbureaus in het cyberdomein, zoals Gartner en Forrester, stellen zelfs dat je alleen nog weerbaar kunt zijn door informatie te beschermen met actieve monitoring en intelligence.

Dan zijn er ook nog de wet- en regelgevende instanties die van alles van je verlangen. In bijna elke branche die we in Nederland onderscheiden, zijn er wel specifieke normeringen waar een bedrijf aan kan of moet voldoen. En voor iedereen die met persoonsgegevens werkt, is daar sinds 25 mei 2018 de Algemene Verordening Persoonsgegevens (AVG) bij gekomen.

Wat veel organisaties zich nu afvragen, is: hoe zorgen we ervoor dat we continu weerbaar blijven tegen cyberrisico's en dat we tegelijkertijd onze klanten, partners en andere stakeholders het vertrouwen geven dat hun informatie in veilige handen is?

Om deze vraag nu en in de toekomst te kunnen beantwoorden heb je geen keuze: je zult je moeten verdiepen in cybersecurity. Met dit boek willen we je een introductie geven op deze complexe materie en tevens de juiste handvatten bieden om direct aan de slag te kunnen om de beveiliging van je organisatie te verbeteren.

Digitalisering kan niet zonder goede security

Of we nu de krant lezen, nieuwssites bezoeken of naar het journaal kijken, steeds vaker worden we geconfronteerd met nieuws over de toe-

nemende digitalisering van de wereld waarin we leven. Die digitalisering brengt ons fantastische mogelijkheden, bijvoorbeeld de verbondenheid met mensen en de vervaging van de traditionele landsgrenzen. Maar er zijn ook digitale innovaties zoals elektrisch rijden, witgoed op wifi, de enorme rekenkracht in onze smartphones, tablets, en smartwatches. Begin 2018 werd zelfs een Tesla de ruimte in geschoten, waarbij de herbruikbare delen van de raket op de milliseconde nauwkeurig terug op aarde landden. Allemaal mede dankzij de wonderen van ICT.

Deze digitalisering van onze samenleving en onze manier van werken kent echter ook een keerzijde. Bij digitalisering maken we op grote schaal gebruik van systemen en technologieën die worden aangestuurd door software. Software bevat altijd kwetsbaarheden en die kunnen worden misbruikt door kwaadwillenden. En zo worden grote bedrijven aangevallen via internet door tieners

vanaf hun zolderkamer en wordt van nietsvermoedende individuen de digitale identiteit gestolen. Niets lijkt veilig: volledige databases met gevoelige informatie komen op straat te liggen, internetbankieren wordt verstoord, auto's worden gehackt en informatie wordt gekidnapt. En dat zijn zomaar een paar voorbeelden van de keerzijde van de digitalisering.

Niet zelden hoeven cybercriminelen niet eens veel moeite te doen. De soms slechte software van zogenaamde *connected devices* – zoals auto's, medische apparatuur, domotica en zelfs kinderpoppen – geeft hun bijvoorbeeld de kans om makkelijk misbruik van ons te maken. Cybersecurity is dus cruciaal in deze tijd van digitalisering om bedreigingen buiten de deur te houden.

Het doel van dit boek is primair om dit alles begrijpelijk en toepasbaar te maken. We gaan in op risicomanagement, informatiebeveiliging en cybersecurity. We schrijven vanuit onze ervarin-

gen en zijn ook kritisch tegenover ons vak. We beschrijven waar we als *security community* staan en waar we hadden moeten staan. Eén ding is zeker als het om digitalisering gaat: het is niet meer de vraag óf je gehackt wordt, maar wannéér je gehackt wordt. Met deze wetenschap zou je vandaag nog aan de slag moeten gaan met de beveiliging van jouw organisatie.

1

WAT IS CYBERSECURITY?

Als cybersecurity-expert is het onze taak om de ICT-infrastructuur, inclusief de data (bijvoorbeeld privacy-data en bedrijfsgevoelige informatie zoals *intellectual property*), te beveiligen. Wij moeten elke opzettelijke en onopzettelijke verstoring van ICT het hoofd kunnen bieden. Cybersecurity draait om de bescherming van de beschikbaarheid, integriteit en vertrouwelijkheid van data en systemen. In ons vak wordt dat vaak aangeduid met de Engelse term *confidentiality, integrity and availability* (CIA).

cybersecurity

Cybercriminaliteit is de meest lucratieve vorm van criminaliteit geworden. Omdat we zo afhankelijk zijn geworden van digitale informatie is cybersecurity belangrijker dan ooit. Hoe kunnen we onze ondernemingen beveiligen tegen de aanvallen van kwaadwillenden?

Dr. Yuri Bobbert is Chief Information Security Officer bij NN Group NV. Daarnaast is hij verbonden aan de Universiteit van Antwerpen en de Radboud Universiteit. Melvin Broersma is oprichter van VNTRS consulting en is management consultant voor Business Information Security.

Weinig tijd, maar veel ambities? Informeer jezelf snel en grondig met de boeken in de serie *Digitale trends en tools in 60 minuten*.

HAYSTACK

9 789461 263032