Cybersecurity voor dummies®

SPIEKBRIEF

Bescherm jezelf en je gezin op internet

Om jezelf en je gezin in de cyberwereld te beschermen, moet je ervoor zorgen dat iedereen bij jou thuis snapt dat jullie een doelwit zijn. Neem de volgende tips ter harte om de gegevens van jou en je gezin beter te beschermen, ook tegen oplichters op internet:

- **Bescherm jullie apparaten.** Laat op zijn minst beveiligingssoftware draaien op elk apparaat dat jullie gebruiken om toegang te krijgen tot gevoelige gegevens. Stel jullie apparaten zo in, dat ze automatisch worden vergrendeld en zorg ervoor dat jullie ze met een sterk wachtwoord ontgrendelen. Laat jullie apparaten niet op een onveilige plek rondslingeren en installeer alleen software van betrouwbare leveranciers, zoals officiële appwinkels en officiële websites van de fabrikant en leverancier.
- **Bescherm jullie gegevens.** Versleutel alle gevoelige gegevens en maak geregeld een back-up. Als je niet zeker weet of iets moet worden versleuteld, dan moet dat waarschijnlijk wel gebeuren. Als je niet zeker weet of je wel vaak genoeg een back-up maakt, dan doe je dat waarschijnlijk te weinig; net als de meeste mensen trouwens.
- **Gebruik een veilige verbinding.** Open nooit gevoelige gegevens via een gratis, openbare wifiverbinding. Zo'n verbinding kun je maar beter helemaal niet gebruiken voor apparaten waarop je vertrouwelijke informatie moet verwerken of waarmee je toegang hebt tot gevoelige gegevens. De verbinding die je internetprovider biedt, is waarschijnlijk veel veiliger dan een openbare wifiverbinding.
- **Gebruik fatsoenlijke authenticatie en wachtwoorden.** Ieder die toegang heeft tot een belangrijk systeem moet zijn of haar eigen inloggegevens hebben. Zeg niet tegen je partner en kinderen wat je wachtwoorden zijn voor internetbankieren, e-mailen, social media enzovoort. Gebruik voor je gevoeligste systemen in elk geval sterke, unieke wachtwoorden.
- **Deel niet te veel.** Deel niet te veel informatie over jezelf op social media of andere platforms. Oplichters zoeken op deze platforms naar dat soort informatie, die ze gebruiken om mensen te misleiden en te manipuleren. Door te veel over jezelf en je naasten te vertellen, loop je een groter risico dat oplichters jou als doelwit uitkiezen.

Vermijd de gebruikelijke cybersecurityfouten

Hier zijn enkele van de meest voorkomende fouten die mensen maken als het om hun cybersecurity gaat. Door deze fouten wordt hacken een eitje en maak je het criminelen heel makkelijk om cybercriminaliteit te plegen.

- **Denken dat het jou niet overkomt.** Individuen, bedrijven, organisaties of overheidsinstanties zijn allemaal een potentieel doelwit voor hackers. Mensen die denken dat ze geen waardevolle dingen hebben ('waarom zouden hackers mij willen aanvallen?'), handelen vaak wat al te onbezorgd. Meestal komen ze er vrij snel achter dat ze het verkeerd hadden ingeschat.

Cybersecurity voor dummies®

SPIEKBRIEF

- **Zwakke wachtwoorden gebruiken.** Ondanks de overbekende waarschuwing dat je geen zwakke wachtwoorden moet gebruiken, zijn wachtwoorden als '123456' of 'wachtwoord' nog steeds erg populair. Dat blijkt uit lijsten met gekraakte wachtwoorden die na verschillende hacks op internet zijn gepubliceerd. Als je een zwak wachtwoord gebruikt of op een gevoelige website hetzelfde wachtwoord gebruikt als voor andere websites, dan loop je een aanzienlijk groter risico dat je account wordt gehackt.
- **Geen multifactorauthenticatie gebruiken hoewel dat mogelijk is.** Alle grote socialmediaplatforms, Google, Amazon en de meeste grote financiële instellingen bieden de mogelijkheid om een vorm van multifactorauthenticatie te gebruiken. Multifactorauthenticatie kan, als een wachtwoord wordt gekraakt, het verschil uitmaken tussen een account dat wordt gehackt of goed beveiligd blijft. In 2019 benutte nog altijd slechts een minderheid van de gebruikers dergelijke mogelijkheden.
- **Niet de juiste beveiligingssoftware gebruiken.** Met de moderne beveiligingssoftware heb je een aanzienlijk grotere kans om je goed te verdedigen tegen een hele reeks potentiële cybersecurityproblemen, zoals malware, hacks, grote hoeveelheden spam en dergelijke. Toch gebruiken veel mensen die software nog steeds niet op hun computers (waaronder laptops, tablets en smartphones). Ook zijn er mensen die de software wel geïnstalleerd hebben maar niet up-to-date houden. Dan biedt die software geen bescherming meer tegen de nieuwste (en vaak gevaarlijkste) bedreigingen.
- **Software niet up-to-date houden.** Veel updates van het besturingssysteem en de software bestaan uit oplossingen voor beveiligingsproblemen die onderzoekers (of hackers) in eerdere versies hebben ontdekt. Als je je software niet up-to-date houdt, zijn je apparaten kwetsbaarder voor aanvallen. Erger nog, als de fabrikant van de software bekendmaakt welke kwetsbare plekken zijn verholpen, dan proberen criminelen soms via zogenoemde exploit scripts computers te zoeken zonder zo'n reparatiepatch, zodat ze die kunnen aanvallen.
- **Niet je gezond verstand gebruiken.** Bijna altijd is de mens de zwakste schakel in de cybersecurityketen. Of het nu gaat om klikken op een link waarop niet geklikt had moeten worden, geld sturen naar een fraudeur die zich met een nep-e-mailtje voor jouw baas heeft uitgegeven, een malwareapp installeren, een film illegaal downloaden of om een andere onvoorzichtige handeling, menselijke fouten openen vaak de cyberdeur voor criminelen. Hierdoor krijgen ze de mogelijkheid om nog veel meer schade aan te richten dan hun zonder die fouten was gelukt.
- **Geen basiskennis willen opdoen.** Mensen die een ziekte hebben of van wie een naaste ziek is, verdiepen zich meestal in die ziekte. Ze willen immers de juiste behandeling krijgen en niet onnodig gevaar lopen. Maar als het om hun cybersecurity gaat, dan kiezen veel mensen ervoor om onwetend te blijven. Ze denken dat als ze maar doen alsof ze geen gevaar lopen, dat ook zo is.
- **Geen professional inhuren.** Bij ernstige incidenten op cybersecuritygebied proberen mensen (veelal particulieren en kleine bedrijven) de problemen vaak zelf op te lossen. Dat is eigenlijk hetzelfde als dat je probeert een ernstige ziekte te behandelen zonder naar de dokter te gaan of je voor de strafrechter te verdedigen zonder advocaat. Hackers, ontwikkelaars van malware en andere cybercriminelen bezitten een flinke dosis kennis. Kom je vast te zitten in een gevecht tegen hen, dan is het goed dat er ook een professional aan jouw kant staat.

Inhoud in vogelvlucht

1 Aan de slag met cybersecurity

IN DIT DEEL . . .

Ontdek je wat cybersecurity inhoudt en waarom het nog niet zo makkelijk is om de term nauwkeurig te omschrijven.

Lees je waarom cyberaanvallen zo vaak lijken voor te komen en waarom technologie alleen ze niet lijkt te stoppen.

Kijk je welke verschillende soorten veelvoorkomende cybergevaren er zijn en met welke bekende instrumenten je de cybersecurity kunt waarborgen.

Krijg je inzicht in het wie, hoe en waarom van verschillende soorten aanvallers en figuren die een bedreiging vormen, maar niet als kwaadwillend te boek staan.

IN DIT HOOFDSTUK

- **Het verschil tussen cybersecurity en informatiebeveiliging**
- **Waarom cybersecurity een doel is dat je nooit echt bereikt**
- **Waarom je aan cybersecurity moet doen**
- **Welke risico's je met cybersecurity kunt verkleinen**

Hoofdstuk 1

Wat betekent cybersecurity nu eigenlijk?

Om jezelf en je naasten beter beveiligd te houden moet je begrijpen wat cybersecurity betekent, wat je cybersecuritydoelen zijn en waar je je nu eigenlijk tegen beveiligt.

Hoewel de antwoorden op deze vragen op het eerste gezicht eenvoudig en logisch lijken, zijn ze dat niet. Zoals je in dit hoofdstuk ziet, verschillen de antwoorden enorm tussen mensen, afdelingen van bedrijven, organisaties en zelfs voor dezelfde persoon of organisatie op verschillende momenten.

Cybersecurity betekent verschillende dingen voor verschillende mensen

Hoewel *cybersecurity* misschien klinkt als een term die eenvoudig te omschrijven is, betekent hij in feite heel verschillende dingen voor verschillende mensen in verschillende situaties. Daardoor zijn er enorm uit-

eenlopende beleidsmaatregelen, procedures en praktijken ontstaan. Zo wordt het steeds onwaarschijnlijker dat iemand die haar socialmedia-accounts tegen hackers wil beschermen methoden en technieken gaat inzetten die de AIVD gebruikt om zijn geheime netwerken te beveiligen.

Cybersecurity betekent meestal:

- voor **individuen**, dat hun persoonsgegevens voor niemand anders toegankelijk zijn dan voor henzelf en voor degenen die ze daartoe gemachtigd hebben, en dat hun computerapparatuur fatsoenlijk werkt en er geen malware op staat;
- voor **eigenaren van kleine bedrijven**, dat bijvoorbeeld hun creditcardgegevens fatsoenlijk worden beschermd en dat in winkels en bij kassa's de geldende normen voor gegevensbeveiliging worden nageleefd;
- voor **bedrijven die online zakendoen**, dat ze bijvoorbeeld hun servers beschermen waarop mensen van buiten werken die niet (op voorhand) te vertrouwen zijn;
- voor **providers van gedeelde diensten**, dat ze hun vele datacenters met vele servers beschermen die op hun beurt weer vele virtuele servers van vele verschillende organisaties hosten;
- voor de **overheid**, dat ze bijvoorbeeld gegevens in verschillende klassen indeelt, elk met hun eigen stel regels, beleidsmaatregelen, procedures en technologieën.


BELANGRIJK

Kortom, het is niet zo moeilijk om het woord cybersecurity te omschrijven, maar mensen hebben nogal uiteenlopende verwachtingen voor de praktijk als ze het woord cybersecurity horen.

Technisch gesproken is cybersecurity het onderdeel van de informatiebeveiliging dat gaat over informatie en informatiesystemen die gegevens in elektronische vorm opslaan en verwerken, terwijl *informatiebeveiliging* over de beveiliging van alle vormen van gegevens gaat (bijvoorbeeld de beveiliging van een papieren dossier of een archiefkast).

Toch halen veel mensen de termen tegenwoordig door elkaar en hebben het dan vaak over bepaalde aspecten van de informatiebeveiliging die technisch gezien niet tot de cybersecurity behoren. Die verwarring komt ook doordat de twee aspecten zich in veel situaties met elkaar vermengen. Zo heeft technisch gesproken iemand die een wachtwoord op een papiertje schrijft en dat papiertje duidelijk zichtbaar op zijn bureau laat liggen in plaats van het op te bergen in een veilig kluisje, een basisregel geschonden van de informatiebeveiliging en niet van de cybersecurity, ook al kan zijn gedrag grote gevolgen hebben voor de cybersecurity.

Cybersecurity is een doel dat je nooit echt bereikt

Hoewel het uiteindelijke doel van cybersecurity in de loop van de tijd niet echt veranderd is, zijn de beleidsmaatregelen, procedures en technologieën die worden gebruikt om dat doel te bereiken in de loop van de jaren enorm veranderd. Zo zijn veel methoden en technologieën die in 1980 meer dan voldoende waren om de digitale gegevens van de consument te beschermen tegenwoordig ronduit waardeloos. Dat komt doordat het gebruik ervan niet meer praktisch is, of omdat ze door de technologische vooruitgang verouderd of niet meer afdoende zijn.

Het is onmogelijk om een volledige lijst te geven van elke stap vooruit die de wereld de afgelopen decennia heeft gezet en hoe die veranderingen van invloed zijn op de cybersecurity. Toch belichten we hier enkele belangrijke ontwikkelgebieden en de invloed ervan op de alsmaar veranderende aard van de cybersecurity: technologische veranderingen, nieuwe economische modellen en het uitbesteden van werk.

Technologische veranderingen

Technologische veranderingen hebben een enorme impact op de cybersecurity. De nieuwe mogelijkheden en gemakken van de nieuwe producten brengen ook nieuwe risico's met zich mee. Het tempo van de technologische vooruitgang ligt weliswaar steeds hoger, maar dat geldt ook voor het tempo van de nieuwe cybersecurityrisico's. Terwijl er door de nieuwe producten in de afgelopen decennia verbazingwekkend hoge aantallen van dat soort risico's zijn ontstaan, hebben enkele terreinen onevenredig veel impact gehad op de cybersecurity. Hierna bespreek ik ze.

Digitale gegevens

In de afgelopen decennia zijn de bestaande technologieën enorm veranderd. Dat geldt ook voor degenen die de technologieën gebruiken, hoe ze dat doen en waarom. Al deze factoren zijn van invloed op de cybersecurity.

Bedenk eens hoe eenvoudig het vroeger allemaal was. Toen veel volwassenen van nu nog kinderen waren, betekende de toegang tot gegevens in een bedrijf bewaken simpelweg dat de eigenaar van de gegevens een tastbaar bestand met informatie in een kast legde die werd afgesloten; de sleutel ervan ging alleen naar de mensen die gemachtigd waren, en ze konden alleen tijdens kantooruren om die sleutel vragen. Om de gegevens extra te beveiligen stond de kast in een ruimte die na kantoortijd werd

afgesloten en in een gebouw dat ook kon worden afgesloten en met een alarminstallatie beveiligd was.

Met de digitale opslag van informatie van tegenwoordig zijn de eenvoudige regels voor het bewaren en beschermen van informatie vervangen door ingewikkelde technologieën: ze moeten een geautomatiseerde authenticatie uitvoeren van de gebruikers, die van waar ook en wanneer dan ook met de gegevens willen werken, en vaststellen of die gebruikers bevoegd zijn om met (een bepaald) deel van die gegevens te werken, en dan de juiste gegevens veilig bezorgen. En tegelijkertijd moet worden voorkomen dat het systeem dat zich bezighoudt met die gegevensaanvragen wordt aangevallen of dat de gegevens tijdens het overbrengen worden aangevallen, of dat de beveiligingsmechanismen die beide aspecten beschermen worden aangevallen.

Verder heeft de overgang van communicatie op papier naar e-mails en chatgesprekken enorme hoeveelheden gevoelige informatie op servers gezet die met internet verbonden zijn. En de cybersecurity is ook veel urgenter geworden nu we massaal zijn overgestapt van filmrolletjes naar digitale fotografie en filmpjes. Bijna elke foto of filmpje dat tegenwoordig wordt (op)genomen wordt elektronisch opgeslagen. Daardoor kunnen criminelen van over de hele wereld foto's van mensen stelen en lekken, of kunnen ze waardevolle beelden van mensen gijzelen met gijzelsoftware. En doordat films en tv-programma's nu elektronisch worden opgeslagen en uitgezonden, kunnen ze illegaal worden gekopieerd en aan een massapubliek worden aangeboden, soms via websites die met malware zijn geïnfecteerd.

Internet

De belangrijkste technologische stap vooruit wat betreft de impact van de cybersecurity is de komst van internettijdperk. Nog maar enkele tientallen jaren geleden was het onvoorstelbaar dat hackers van over de hele wereld een bedrijf konden ontwrichten, verkiezingen konden manipuleren of een miljard euro konden stelen. Tegenwoordig sluit niemand die ook maar een beetje kennis van zaken heeft dat soort dingen nog uit.

Vóór het internettijdperk was het voor de gemiddelde hacker bijzonder moeilijk om met hacken geld te verdienen. Door de komst van internetbankieren en de online handel in de jaren negentig konden hackers echter rechtstreeks geld of goederen en diensten gaan stelen. Dat betekende niet alleen dat ze eenvoudig en snel munt konden slaan uit hun activiteiten, maar dat mensen die geen last hadden van hun geweten een sterke prikkel hadden om de cybercriminaliteit in te gaan.

Cryptovaluta

Die prikkel is de afgelopen 10 jaar nog eens flink versterkt door de komst en verspreiding van cryptovaluta en de nieuwe ontwikkelingen die het potentiële rendement van de investering in cybercriminaliteit enorm hebben vergroot. De mogelijkheden van criminelen om via cybercriminaliteit geld te verdienen, plus de mogelijkheden om zich daarbij te verschuilen, zijn tegenwoordig flink toegenomen. Vroeger was het voor criminelen lastig om betalingen te ontvangen, omdat de rekening waarop het geld werd gestort vaak met hen in verband te brengen was. Met cryptovaluta bestaan dat soort risico's in feite niet meer.

Mobiele arbeidskrachten en overal toegang

Nog niet zo lang geleden, in het pre-internettijdperk, was het voor hackers niet mogelijk om op afstand de systemen van grote bedrijven binnen te dringen. Immers, de netwerken van grote bedrijven waren niet verbonden met openbare netwerken en vaak kon je er niet op inbellen. Directeuren die op weg naar een klant waren, belden vaak met hun secretaresse om te kijken of er een boodschap voor hen was binnengekomen of om bepaalde gegevens te verkrijgen.

Door de verbinding met internet ontstonden er risico's, maar firewalls weerden aanvankelijk mensen van buiten de organisatie. Afgezien van verkeerd geconfigureerde firewalls en/of softwarefouten, bleven de meeste interne systemen dus relatief op zichzelf staan. De opkomst van de elektronische handel en internetbankieren betekende uiteraard dat bepaalde productiesystemen bereikbaar en vanuit de buitenwereld toegankelijk moesten zijn, al bleef bijvoorbeeld intranet voor het personeel meestal geïsoleerd bestaan.

De komst van de zogenoemde remote access-technologieën (met toegang op afstand), bijvoorbeeld Outlook Web Access en pcAnywhere, die zich hebben ontwikkeld tot systemen met VPN- of VPN-achtige toegang, heeft het spel totaal veranderd.

Slimme apparaten

Zo betekent de komst van slimme apparaten en *internet der Dingen* (IoT, *internet of things*), het geheel aan apparaten dat niet door traditionele computers wordt gevormd maar dat met internet verbonden is (waarvan de verspreiding en uitbreiding momenteel razendsnel plaatsvindt) dat de oude, niet te hacken en tastbare computers nu snel worden vervangen door apparaten die hackers in feite vanaf de andere kant van de wereld kunnen besturen.

Big data

Hoewel big data leidt tot de ontwikkeling van vele nieuwe cybersecurity-technologieën, biedt ze aanvallers ook nieuwe kansen. Door bijvoorbeeld grote hoeveelheden informatie te correleren over de werknemers van een organisatie, is het voor een crimineel makkelijker dan vroeger te achterhalen wat ideale methoden zijn om met social engineering in een organisatie binnen te komen, of om zwakke plekken in de infrastructuur van de organisatie te vinden en te benutten. Daardoor hebben allerlei organisaties zich genoodzaakt gevoeld om allerlei soorten controlemechanismen in te voeren om informatielekken te voorkomen.

Er zijn hele boeken volgeschreven over de impact van de technologische vooruitgang. Wat je vooral moet onthouden is dat de technologische vooruitgang een flinke impact heeft op de cybersecurity. Enerzijds is het moeilijker geworden om cybersecurity voor elkaar te krijgen. Anderzijds staat er nu meer op het spel als het personen of organisaties niet lukt om hun kapitaal fatsoenlijk te beschermen.

Sociale veranderingen

Mensen zijn zich door internet (deels) anders gaan gedragen en gaan nu anders met elkaar om. Ook dat heeft een grote impact gehad op de cybersecurity. Door internet kunnen mensen van over de hele wereld bijvoorbeeld in realtime met elkaar communiceren. Uiteraard kunnen criminelen van over de hele wereld ook in realtime hun misdrijven op afstand plegen. Maar burgers uit dictaturen en democratische landen kunnen nu met elkaar communiceren; dat biedt mogelijkheden om de eeuwige propaganda door te prikken die totalitaire staten als excuus gebruiken voor het feit dat ze er niet in slagen om hun burgers dezelfde levenskwaliteit te bieden als in de vrije wereld. Tegelijkertijd hebben de ‘cyberkrijgers’ van regeringen die tegenover elkaar staan de mogelijkheid om via hetzelfde netwerk aanvallen te lanceren.

De omzetting van diverse informatiebeheersystemen van papier naar computer, van op zichzelf staand naar met internet verbonden en van alleen-op-kantoor-toegankelijk tot vanaf elke smartphone of computer toegankelijk, heeft radicaal veranderd welke informatie hackers kunnen stelen. In veel gevallen waarin zo’n overstap om veiligheidsredenen eerst niet plaatsvond, hebben mensen afgedwongen dat die overstap wel plaatsvindt; tegenwoordig verwachten mensen immers dat alle gegevens te allen tijde beschikbaar voor hen zijn, waar ze zich ook bevinden. Dit biedt nieuwe kansen voor criminelen. Hackers zien tot hun grote genoegen dat veel organisaties die in het verleden zo wijs waren om gevoelige informatie offline te houden, zich dat nu niet meer kunnen veroorloven als ze niet failliet willen gaan.

Ook de social media hebben de wereld van de informatie ingrijpend veranderd. Mensen raken eraan gewend om veel meer over zichzelf te vertellen dan ooit tevoren, vaak aan een publiek dat ook veel groter is dan vroeger. Vanwege deze gedragsverandering is het voor kwaadwillenden van overal ter wereld een koud kunstje geworden om een lijst op te stellen van vrienden, collega's en familieleden van een doelwit en om met die mensen te communiceren. Zo is het ook makkelijker dan ooit tevoren om te achterhalen welke technologieën een bepaald bedrijf gebruikt en voor welke doeleinden, wat het reisschema van mensen is, en welke mening ze hebben over diverse onderwerpen of welke muziek en films ze leuk vinden. De trend om steeds meer informatie te delen zet zich verder door. De meeste mensen zijn zich er nog steeds totaal niet van bewust hoeveel informatie er over hen op met internet verbonden apparaten staat en hoeveel andere informatie er over hen af te leiden is uit de hiervoor genoemde gegevens.

Al die veranderingen hebben tot een griezelige werkelijkheid geleid: door de maatschappelijke veranderingen kunnen kwaadwillenden tegenwoordig makkelijk een veel grotere, geavanceerdere social-engineeringaanval lanceren dan nog geen 10 jaar geleden mogelijk was.

Nieuwe economische modellen

Doordat internet bijna de hele wereld met elkaar verbindt, heeft het nieuwe trends voortgebracht die enorme gevolgen hebben voor de cybersecurity. Methoden van bedrijfsvoering die ooit ondenkbaar waren, bijvoorbeeld een Europees bedrijf dat gebruikmaakt van een callcenter in India en een afdeling softwareontwikkeling op de Filippijnen, zijn nu de normaalste zaak voor veel grote bedrijven. Deze veranderingen hebben echter allerlei soorten cybersecurityrisico's voortgebracht.

De afgelopen 20 jaar hebben we een enorme groei gezien in het uitbesteden van allerlei werkzaamheden van locaties waar het duurder produceren is naar regio's waar dat tegen veel lagere kosten wordt gedaan. De gedachte dat een bedrijf in Europa voornamelijk zou werken met computerprogrammeurs uit India of de Filippijnen, of dat iemand uit Amsterdam die een logo voor haar bedrijf wil laten maken, vlak voor het slapen gaan iemand aan de andere kant van de wereld 5 euro betaalt voor het ontwerpen van dat logo en het de volgende ochtend in haar e-mailbox vindt, zou een generatie geleden als economische sciencefiction hebben geklonken. Tegenwoordig is zoiets niet alleen gebruikelijk; het is vaak gebruikelijker dan alle andere methoden om vergelijkbare resultaten te behalen.

Uiteraard heeft dat grote gevolgen voor de cybersecurity. De overgebrachte gegevens moeten worden beschermd tegen vernietiging, wijziging of diefstal, en er zijn meer garanties nodig dat er niet bewust of per ongeluk met de code wordt geknoeid. Er is meer bescherming nodig tegen diefstal van intellectueel eigendom en andere vormen van bedrijfsspionage. Hackers hoeven niet langer direct in te breken in de organisatie die ze proberen te hacken; ze hoeven alleen maar een of meerdere van diens internetproviders aan te vallen. Die providers gaan misschien veel minder zorgvuldig om met de beveiliging van hun gegevens en de gedragscode van hun medewerkers dan het uiteindelijke doelwit.

Politieke veranderingen

Net als de technologische vooruitgang hebben politieke veranderingen enorme gevolgen voor de cybersecurity. Enkele daarvan lijken niet uit het nieuws weg te slaan. Al vaker is gebleken dat een combinatie van regeringsmacht en sterke technologie de burger duur komt te staan. Als de huidige trends zich voortzetten, dan wordt de impact van cybersecurity op een aantal politieke veranderingen alleen nog maar groter in de nabije toekomst.

Data verzamelen

Door de enorme verspreiding van informatie via internet en het feit dat computers en apparaten nu van over de hele wereld kunnen worden aangevallen, zijn regeringen in staat om de burgers van hun eigen land en de inwoners van andere landen tegenwoordig in ongekende mate te bespioneren.

Nu steeds meer zakelijke, persoonlijke en maatschappelijke activiteiten een digitale voetafdruk achterlaten, hebben regeringen een veel grotere hoeveelheid informatie over hun inlichtingendoelwitten binnen hun bereik dan enkele jaren geleden, tegen veel hogere kosten, het geval was. Door de relatief lage kosten van digitale gegevensopslag, geavanceerde bigdatatechnologieën en de verwachting dat vele huidige versleutelingstechnologieën uiteindelijk gekraakt worden, hebben regeringen een sterke prikkel om zo veel mogelijk gegevens over zo veel mogelijk mensen te verzamelen en op te slaan, voor het geval dat later van pas zou komen. Het is wel duidelijk dat enkele regeringen hier nu al mee bezig zijn.

De langetermijngevolgen zijn uiteraard nu nog niet bekend. Maar één ding is duidelijk: als bedrijven gegevens niet fatsoenlijk beschermen, dan proberen landen waarmee we op niet zo'n goede voet staan die gegevens waarschijnlijk te verkrijgen en op te slaan, om ze op de korte en/of lange termijn te gebruiken.

Inmenging in verkiezingen

Een generatie geleden was het geen onbeduidende zaak als een land zich mengde in de verkiezingen van een ander land. Uiteraard bestond dat soort inmenging wel (net zo lang als er verkiezingen zijn), maar grote inmengingscampagnes waren duur, arbeidsintensief en riskant.

Om onjuiste informatie en andere propaganda te verspreiden moest informatie worden afgedrukt en fysiek worden verspreid of worden opgenomen en via de radio worden uitgezonden. Dat betekende dat die losse campagnes meestal maar een klein publiek bereikten. De inspanningen leverden meestal maar weinig op en de partij die de campagne runde, liep een relatief groot risico om ontmaskerd te worden.

Het was buitengewoon moeilijk om databanken met stemgerechtigden of geregistreerde kiezers te manipuleren; bijvoorbeeld om te voorkomen dat stemgerechtigden gingen stemmen en/of om nepkiezers te laten stemmen. Ook was dat enorme risicovol; de verrader moest algauw iemand zijn die 'van binnenuit werkte'. In een land als de Verenigde Staten, waar de databanken met geregistreerde kiezers zijn gedecentraliseerd en op regionaal niveau worden beheerd, zou het rekruteren van voldoende saboteurs om de verkiezingsuitslag daadwerkelijk te beïnvloeden vrijwel onmogelijk zijn geweest. Ook was de kans waarschijnlijk heel groot om daarbij betrapt te worden. In het tijdperk van de papieren stembiljetten en het handmatig tellen van de stemmen was het voor buitenlandse mogendheden praktisch onmogelijk om de verkiezingsuitslag grootschalig te manipuleren.

Maar het spel is veranderd. Een regering kan via social media heel makkelijk en tegen zeer lage kosten onjuiste informatie verspreiden. Als ze een uitgekiende campagne in elkaar zet, laat ze andere mensen die informatie gewoon verspreiden; iets wat niet massaal mogelijk was in het tijdperk van de radio-opnamen en gestencilde pamfletten. Nu veel meer mensen te bereiken zijn tegen veel lagere kosten dan ooit tevoren, mengen meer partijen zich in politieke campagnes. Dat levert ook nog eens meer op dan in het verleden. Zo verspreiden regeringen tegenwoordig soms ook onjuiste informatie om de ontevredenheid onder de bevolking van vijandige naties aan te wakkeren, of om de vijandige houding tussen etnische en religieuze groepen in andere landen te versterken.

Nu de databanken van stemgerechtigde of geregistreerde kiezers in elektronische vorm worden opgeslagen (soms op servers die op zijn minst indirect met internet zijn verbonden), kunnen er vanaf de andere kant van de wereld ongemerkt kiezersbestanden toegevoegd, gewijzigd of verwijderd worden. Ook al is die vorm van hacken in feite onmogelijk, veel burgers geloven tegenwoordig wel dat dit mogelijk is. Dat heeft het vertrouwen in verkiezingen ondermijnd, wat we de afgelopen jaren in de

Verenigde Staten hebben gezien en daar in alle lagen van de maatschappij is doorgedrongen. Zelfs Jimmy Carter, oud-president van de Verenigde Staten, heeft gezegd dat hij meent dat uit een volledig onderzoek naar de presidentsverkiezingen van 2016 zou blijken dat Donald Trump de verkiezingen heeft verloren. Er is totaal geen bewijs voor die conclusie, zelfs niet na een grondig onderzoek hiernaar van de FBI.

Ook is het niet moeilijk voor te stellen dat als er ooit in landen via internet gestemd gaat worden, het potentieel astronomisch toeneemt dat buitenlandse regeringen, criminelen en zelfs politieke partijen van het land dat naar de stembus gaat, de stembusuitslag gaan manipuleren.

Nog geen 10 jaar geleden vonden de Verenigde Staten computersystemen die met de verkiezingen te maken hadden nog geen kritieke infrastructuur en gaf de federale overheid nog geen geld voor de beveiliging van die systemen. Tegenwoordig begrijpen de meeste mensen dat cybersecurity op dat gebied van het allergrootste belang is; het beleid van slechts enkele jaren geleden lijkt nu pure waanzin.

In Nederland zijn bij de verkiezingen tussen 1991 en 2007 stemcomputers gebruikt, al had de overheid ze niet eerst getest op fraudegevoeligheid. De Nederlandse overheid had alle vertrouwen in de techniek, maar wist tegelijkertijd nauwelijks hoe alles werkte. Wetenschappers en IT-specialisten hebben voortdurend op de gevaren gewezen, en mede dankzij de actiegroep Wij vertrouwen stemcomputers niet wordt er sinds 2008 in Nederland weer met potlood en papier gestemd.

In België ligt de situatie weer anders: in de gemeenten van Brussel is digitaal stemmen algemeen, in Vlaanderen stemt iets meer dan de helft van de gemeenten digitaal en in Wallonië is het digitaal stemmen juist afgeschaft.

Hacktivisme

De verspreiding van de democratie sinds de ineenstorting van de Sovjet-Unie een generatie geleden en internetcontact tussen mensen van over de hele wereld heeft het tijdperk ingeluid van het hacktivisme. Mensen weten beter dan ooit wat er allemaal loos is in de wereld. Hackers die het niet eens zijn met bepaald beleid of activiteiten van de regering in een land, kunnen zich vanaf de andere kant van de wereld op die regering of de burgers van dat land richten.

Grotere vrijheid

Tegelijkertijd zijn onderdrukte volkeren nu beter op de hoogte van de levensstijl van de mensen in landen die vrijer en welvarender zijn. Daar-

door hebben sommige regeringen zich genoodzaakt gezien om wat meer economische en politieke vrijheid te geven. Andere regeringen hebben juist cybersecurityachtige controlemechanismen ingevoerd om te voorkomen dat hun bevolking gebruikmaakt van internetdiensten.

Sancties

Een ander politiek gevolg van cybersecurity heeft te maken met internationale sancties: schurkenstaten die dat soort sancties opgelegd hebben gekregen, zijn erin geslaagd om die sancties te omzeilen via verschillende vormen van cybercriminaliteit.

Zo wordt aangenomen dat Noord-Korea malware heeft verspreid die voor deze totalitaire staat cryptovaluta genereert op computers van over de hele wereld. Hierdoor verkrijgt het land contant geld dat het overal ter wereld kan uitgeven.

Dat mensen anno nu hun pc niet afdoende beveiligen, kan dus directe gevolgen hebben voor de politieke onderhandelingen tussen landen.

Een nieuw machtsevenwicht

Hoewel de legers van bepaalde landen sinds mensenheugenis veel machtiger zijn dan die van hun tegenstanders (zowel de kwaliteit als de kwantiteit van het wapenarsenaal verschilt enorm van land tot land), ligt het machtsevenwicht totaal anders als het om de cybersecurity gaat.

Hoewel de kwaliteit van de cyberwapens verschilt van land tot land, betekent het feit dat het weinig kost om een cyberaanval te lanceren, dat alle legers feitelijk een onbegrensde voorraad wapens tot hun beschikking hebben. Sterker nog, het lanceren van miljoenen cyberaanvallen kost vaak weinig meer dan het lanceren van slechts één aanval.

In tegenstelling tot de fysieke wereld waarin een land flinke represailles kan verwachten als het op het grondgebied van zijn tegenstander huizen van de burgerbevolking bombardeert, hacken de regeringen van schurkenstaten mensen in andere landen regelmatig en straffeloos. De slachtoffers zijn zich er vaak totaal niet van bewust dat zo'n hack heeft plaatsgevonden, doen er zelden aangifte van bij de politie en weten zeker niet wie ze er de schuld van moeten geven.

Zelfs als de slachtoffers beseffen dat hun computer is gehackt en zelfs als technisch deskundigen de aanvallers als de schuldigen aanwijzen, komen de staten die achter die aanvallen zitten vaak met een plausibele ontkenning, zodat geen enkele regering een openlijke vergeldingsactie uitvoert. Sterker nog, omdat het zo moeilijk is om vast te stellen wie de aanval

heeft gepleegd en vanwege de plausibele ontkenningen, hebben regeringen een sterke prikkel om cyberaanvallen te gebruiken als mechanisme om als eerste een tegenstander aan te vallen. Zo brengen ze allerlei schade toe zonder bang te hoeven zijn voor flinke represailles.

Ook heeft de wereld van de cybersecurity tot een enorme onevenwichtigheid geleid tussen aanvallers en verdedigers, waarvan de minder machtige landen nu profiteren.

Regeringen die het zich nooit hebben kunnen veroorloven om in de fysieke wereld een tegenstander flink aan te vallen, kunnen dat in de cyberwereld makkelijk doen; het kost in de cyberwereld immers zo ongeveer niets om een aanval te lanceren. Daardoor kunnen aanvallers blijven aanvallen tot ze succes hebben; en ze hoeven maar één keer in een systeem in te breken om 'succes te hebben'. Daardoor zadelen ze de verdedigende partij met een enorm probleem op, omdat die haar kapitaal tegen alle aanvallen moeten afschermen. Door deze onbalans hebben de aanvallers een belangrijk voordeel ten opzichte van de verdedigers. Het betekent dat zelfs onbeduidende machten met succes kunnen inbreken op de systemen van de supermachten.

Sterker nog, die onbalans is een van de redenen waarom de cybersecurity zo vaak lijkt te wordt geschonden: veel hackers blijven maar aanvallen tot ze succes hebben. Als een organisatie zich met succes verdedigt tegen tien miljoen aanvallen, maar de tien miljoen en eenste aanval niet weet te stoppen, kan ze flink in de problemen komen en het nieuws halen. In de berichtgeving over die hack wordt waarschijnlijk niet vermeld dat de organisatie een succespercentage van 99,999999 procent heeft in het beschermen van haar gegevens en dat ze met succes 1 miljoen aanvallen op rij heeft gestopt. Zo geldt ook dat als een bedrijf 99,999 procent van zijn beveiligingspatches heeft geïnstalleerd maar één bekende kwetsbare plek heeft vergeten af te dekken, de kans op een hack groot is omdat criminelen het maar blijven proberen. De media zeggen natuurlijk dat de organisatie haar zaakjes niet op orde had, maar vergeten voor het gemak dat de organisatie tot dan toe bijna perfect had gepresteerd op beveiligingsgebied.

Ook heeft het cybertijdperk het machtsevenwicht veranderd tussen criminelen en politie en justitie.

Criminelen weten dat de kans dat ze worden gepakt en vervolgd voor cybercriminaliteit gigantisch veel kleiner is dan voor de meeste andere misdrijven. Ook weten ze dat herhaalde pogingen om een cybercrime te plegen niet vrijwel zeker tot arrestatie leiden, wat wel het geval is bij de meeste andere misdrijven. Ze weten ook dat politie en justitie de middelen niet hebben om de overgrote meerderheid van de cybercriminelen te vervolgen. Zo moet je, wil je iemand met succes op het spoor komen, in

hechtenis nemen en vervolgen (bijvoorbeeld iemand die gegevens steelt vanuit de andere kant van de wereld via talrijke 'hops' in allerlei landen en een netwerk van computers dat eigendom is van mensen die zich netjes aan de wet houden), heel wat meer middelen inzetten dan je nodig hebt om een dief te vangen die op de bewakingscamera's van een winkel in een bepaalde politieregio wordt vastgelegd.

Door de lage kosten van het lanceren van herhaaldelijke aanvallen, de kans om uiteindelijk prijs te schieten, de uiterst kleine kans om gepakt en gestraft te worden en de potentiële beloning die groter wordt door de toegenomen digitalisering weten criminelen maar al te goed dat cybercriminaliteit loont. Dat benadrukt nog eens hoe belangrijk het is dat je je beschermt.

Kijken welke risico's kleiner worden met cybersecurity

Mensen zeggen weleens dat cybersecurity belangrijk is 'omdat je daarmee voorkomt dat hackers in een systeem inbreken en gegevens en geld stelen'. Maar zo'n antwoord is een enorme onderschatting van de rol die cybersecurity speelt bij het draaiende houden van moderne huishoudens, bedrijven en zelfs de wereld.

Je kunt dan ook vanuit een aantal verschillende standpunten naar de rol van cybersecurity kijken, waarbij steeds een ander stel doelen centraal staat. De volgende lijstjes zijn uiteraard niet volledig, maar moeten je wel aan het denken zetten. Ze laten in elk geval zien hoe belangrijk het is dat je begrijpt hoe je jezelf en je naasten moet beveiligen in de cyberwereld.

Het doel van cybersecurity: de CIA-trits

Mensen die in de cybersecuritywereld werken, zeggen vaak dat het doel van cybersecurity drieledig is, namelijk om de *Confidentiality, Integrity en Availability* (CIA) van de gegevens te waarborgen. Dit wordt ook wel de CIA-trits genoemd, en de woordspeling is uiteraard niet toevallig.

» **Confidentiality** of **vertrouwelijkheid** wil zeggen dat ervoor wordt gezorgd dat informatie niet bekend wordt gemaakt of op een andere manier ter beschikking wordt gesteld aan derden die daartoe niet gemachtigd zijn (dat kunnen mensen, organisaties of computerprocessen zijn).

PAS OP

Verwar vertrouwelijkheid niet met privacy: vertrouwelijkheid is een onderdeel van de privacy. Het gaat specifiek over het zodanig beschermen van gegevens dat onbevoegden ze niet kunnen inkijken; privacy gaat meestal over veel meer aspecten.

Hackers die gegevens stelen ondermijnen de vertrouwelijkheid.

» **Integrity** of **integriteit** wil zeggen dat de gegevens nauwkeurig en volledig zijn.

Nauwkeurig betekent bijvoorbeeld dat de gegevens nooit op welke wijze dan ook worden gewijzigd door een onbevoegde partij of door een technische uitglijder. *Volledig* betekent bijvoorbeeld dat geen deel van de gegevens wordt gewijzigd door onbevoegden of vanwege een technische fout.

Onder integriteit valt ook het begrip onweerlegbaarheid; dat is de verzekering dat de gegevens op zo'n manier zijn gemaakt en verwerkt dat niemand kan beweren of hardmaken dat de gegevens niet authentiek of onnauwkeurig zijn.

Cyberaanvallen die gegevens onderscheppen en wijzigen voordat ze worden doorgegeven aan hun bestemming, ook wel man-in-the-middle-aanvallen genoemd, tasten dus de integriteit aan.

» **Availability** of **beschikbaarheid** wil zeggen dat ervoor wordt gezorgd dat de informatie, de gebruikte systemen om die informatie op te slaan en te verwerken, de gebruikte communicatiemechanismen om toegang te krijgen tot die informatie en ze door te geven, en alle veiligheidsmechanismen eromheen, zo functioneren dat ze aan een specifieke norm voldoen (bijvoorbeeld de website moet 99,99 procent van de tijd bereikbaar zijn). Mensen van buiten de cybersecurity vinden beschikbaarheid soms minder belangrijk dan vertrouwelijkheid en integriteit als het om de beveiliging van gegevens gaat. Maar garanderen dat de gegevens beschikbaar zijn, is onlosmakelijk verbonden met cybersecurity. Al is dat vaak lastiger voor elkaar te krijgen dan vertrouwelijkheid of integriteit. Een van de redenen is dat voor de instandhouding van de beschikbaarheid vaak nog andere professionals nodig zijn van buiten de cybersecurity. Daardoor ontstaat het probleem van 'te veel kapiteins op één schip', vooral in grotere organisaties. Met zogenoemde DDoS-aanvallen (zie hoofdstuk 4) proberen hackers de beschikbaarheid te ondermijnen. Bedenk ook dat er, om die DDoS-aanvallen te lanceren, vaak grote hoeveelheden gestolen processorkracht en bandbreedte wordt gebruikt, terwijl de mensen die de beschikbaarheid proberen te waarborgen slechts een relatief kleine hoeveelheid hulpmiddelen kunnen inzetten omdat het anders te duur wordt.

Vanuit de mens bekeken

De risico's waaraan cybersecurity iets wil doen, zijn ook te schetsen vanuit het perspectief van de mens en zijn leefwereld:

- **Privacyrisico's.** Dit zijn de risico's die voortvloeien uit het feit dat mensen niet meer voldoende controle hebben over of misbruik wordt gemaakt van persoonlijke of andere vertrouwelijke informatie.
- **Financiële risico's.** Denk aan het risico om geld te verliezen door een hackaanval. Bij financiële verliezen gaat het om directe verliezen, bijvoorbeeld het stelen van geld van iemands bankrekening doordat een rekening is gehackt, en om indirecte verliezen, bijvoorbeeld een klein bedrijf dat klanten verliest die zijn opgestapt nadat er iets mis is gegaan met de beveiliging.
- **Beroepsrisico's.** Hierbij gaat het om risico's voor iemands loopbaan die voortvloeien uit een hackaanval. Uiteraard lopen professionals in de cybersecurity het risico op loopbaanschade als er onder hun verantwoordelijkheid een geslaagde hack plaatsvindt. Zeker als die het gevolg blijkt te zijn van nalatigheid. Maar ook andere soorten werknemers kunnen tijdens hun loopbaan schade oplopen door een datalek. Leidinggevenden kunnen worden ontslagen, leden van de raad van bestuur kunnen voor de rechter worden gedaagd enzovoort. Beroepsschade kan ook optreden als hackers privémails of privé-informatie publiceren die iemand in een kwaad daglicht stellen, bijvoorbeeld als uit een dossier blijkt dat een werknemer is berispt vanwege ongepast gedrag, een e-mail heeft verstuurd met een aanstootgevende bijlage enzovoort.
- **Bedrijfsrisico's.** Dit zijn risico's voor een bedrijf die vergelijkbaar zijn met de beroepsrisico's voor een individuele werknemer. Uit interne documenten die na een hack bij Sony Pictures werden gelekt, kwam een negatief beeld van het bedrijf naar voren wat betreft zijn salarispraktijken.
- **Persoonlijke risico's.** Veel mensen slaan privé-informatie op hun elektronische apparaten op, van naaktfoto's tot bewijzen van deelname aan activiteiten die in hun naaste omgeving misschien niet als fatsoenlijk worden beschouwd. Dergelijke gegevens zijn soms funest voor de persoonlijke verhoudingen als ze worden gelekt. En met gestolen persoonsgegevens wordt het voor criminelen makkelijker om de identiteit van mensen te stelen, wat tot ook allerlei persoonlijke problemen kan leiden.