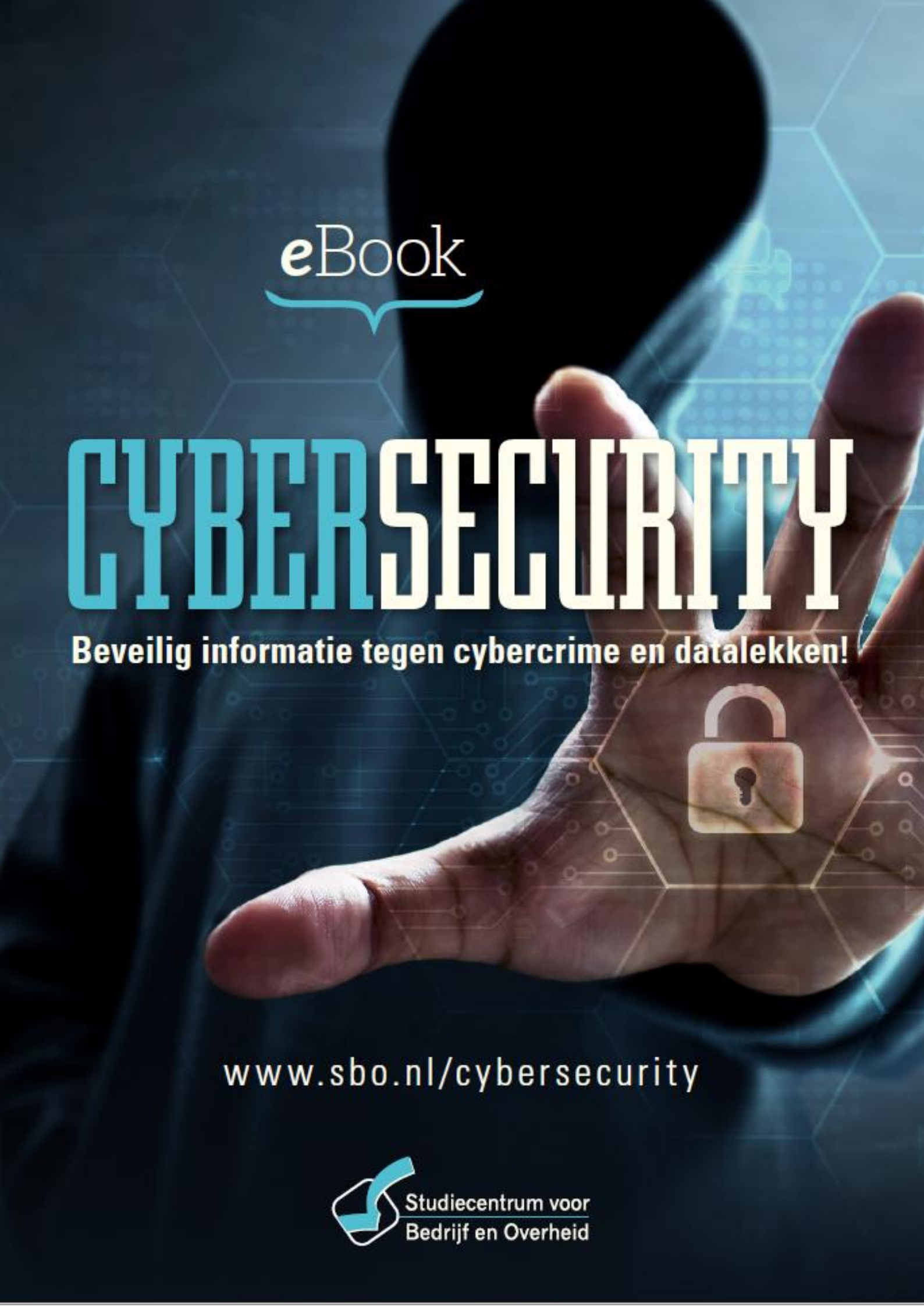
eBook
CYBERSECURITY
Beveilig informatie tegen cybercrime en datalekken!
www.sbo.nl/cybersecurity
Studiecentrum voor
Bedrijf en Overheid

Inhoud

Terreur van de SCADA en het IoT: gecoördineerde aanvallen op kritieke infrastructuur

Met slimme apparaten die met het IoT verbonden zijn, worden steeds meer dingen mogelijk, zoals bijvoorbeeld *Supervisory Control and Data Acquisition* (SCADA). Een SCADA-systeem stelt gebruikers in staat om complexe datastromen te monitoren en de bronnen van die gegevens te reguleren om de efficiëntie te maximaliseren. SCADA-systemen zijn overal. Denk hierbij aan waterkrachtcentrales, waterzuiveringsinstallaties en ziekenhuizen.

Richard van Hooijdonk, Trendwatcher en Futurist bij BNR Nieuwsradio
en Nyenrode University

Met name de *command and control features* maken SCADA-systemen aantrekkelijk voor kritieke infrastructuur. Met deze systemen kun je de waterstroming in een zuiveringsinstallatie meten en deze in real time aanpassen. Ook kun je met SCADA de stroomopwekking in een kerncentrale monitoren en reguleren. SCADA-systemen zijn overal en ze zijn van cruciaal belang. Maar ze zijn ook zeer kwetsbaar. Zoals Tom Simonite zegt in het MIT Security Review, zijn degenen die er het meest vanaf weten ook het meest bezorgd. Experts maken zich zorgen dat de hyperconnectiviteit van SCADA een makkelijk doelwit is voor hackers en kwaadaardige software. Het is dan ook niet onwaarschijnlijk dat we in de toekomst te maken krijgen met gecoördineerde, gelijktijdige aanvallen op kritieke infrastructuur.

Verouderde systemen zijn een security nachtmerrie

In het tijdschrift SecurityWeek schreef Eduard Kovacs dat Verizon in maart 2016 ontdekte dat relatief onervaren hackers de SCADA-systemen van een waterzuiveringsbedrijf waren binnengedrongen. Dankzij de verouderde hardware van het bedrijf dat in 1988 voor het eerst in gebruik genomen was, kwamen de hackers erachter dat het interne IP adres en de inloggegevens van de administrator op de server stonden. Vervolgens kregen zij via de klantgegevens toegang tot betaalgegevens en daarna tot de industriële controlesystemen. Vervolgens waren ze in staat om wijzigingen aan te brengen in de snelheid van de stroming en de chemische behandeling van het water. Gelukkig zagen menselijke toezichthouders op tijd wat er aan de hand was waardoor schade voorkomen kon worden.

Maar Kovacs waarschuwt: “… de aanvallers hadden waarschijnlijk weinig kennis van de werking van de industriële controlesystemen. De aanval zou veel grotere gevolgen hebben gehad als de hackers beter op de hoogte waren geweest.” Als ze meer ervaring hadden gehad en de monitoringssystemen geautomatiseerd en digitaal waren geweest, hadden ze via de zuiveringsinstallatie ongemerkt besmet water kunnen laten verspreiden. Deze verouderde systemen zijn een security nachtmerrie, en terroristen weten dat ze hiermee een verlammende aanval kunnen uitvoeren.

Een recent voorbeeld van dit soort kwetsbaarheid is de energiecentrale in de Oekraïne die in 2015 door een groep hackers werd uitgeschakeld. Hierdoor kwamen 80.000 bewoners in het donker te zitten. Kim Zetter merkt in een artikel voor Wired op dat de aanvallers slim genoeg waren om de computerschermen van de meetstations te bevriezen waardoor de indruk werd gewekt dat alles in orde was. Het zijn dit soort slimme aanvallen waarvan security-experts slapeloze nachten krijgen. De hoge kosten voor het upgraden van deze verouderde systemen hebben ervoor gezorgd dat ze nu, lang na het verstrijken van de ‘houdbaarheidsdatum’, nog steeds in gebruik zijn. Het is voor hightech terroristen een fluitje van een cent om deze systemen te hacken, waardoor het in feite tikkende tijdbommen worden.

Gehackte waterzuiveringsinstallaties kunnen miljoenen mensen infecteren

Als deze moordenaars toegang krijgen tot een waterzuiveringsinstallatie is hun doel niet om informatie te stelen, maar om ervoor te zorgen dat het water zo lang mogelijk ongezuiverd blijft. Dit klinkt misschien onschuldig, maar het is een potentiële ramp van epische proporties. Bedenk bijvoorbeeld dat in Londen 8,7 miljoen mensen afhankelijk zijn van vijf waterzuiveringsinstallaties. Als terroristen het voor elkaar zouden krijgen om de SCADA-systemen in slechts één van deze installaties in gevaar te brengen, waardoor onbehandeld water vermengd wordt met de schone uitstroom, zouden ze miljoenen mensen met ziekten als tyfus, hepatitis A of Giardia lamblia kunnen besmetten. En niet alleen gewone burgers maar natuurlijk ook hulpverleners, artsen en verpleegkundigen zouden worden besmet. Zo'n ramp zou ziekenhuizen overweldigen en duizenden, zo niet tienduizenden mensen zouden kunnen sterven. Dit is geen huis-, tuin- en keukensabotage, dit is geavanceerde biologische oorlogsvoering. Rob Joyce van de National Security Agency zegt: "Door de problematiek rond SCADA-beveiliging doe ik 's nachts geen oog dicht." Zeer vergelijkbaar zijn de gevoelens van Nicholas Weaver van het International Computer Science Institute. Hij zegt: "Ik houd me niet bezig met SCADA-onderzoek want ik hecht teveel waarde aan mijn nachtrust."

Zelfs medische apparaten verbonden met het IoT zijn potentiële wapens

Door de vooruitgang in de medische technologie zijn we gezonder en leven we langer. Zo kunnen we diabetici nu voorzien van een continue glucosemonitor en een insulinepomp die zich aanpast aan schommelingen in de bloedsuikerspiegel, waardoor de werking van een gezonde pancreas wordt nagebootst. Hartpatiënten hebben nu pacemakers, gekoppeld aan Bluetooth-apparaten, die hun hartslag bewaken en reguleren. Net als de command and control systemen voor kritieke infrastructuur, fungeren deze medische apparaten als SCADA voor het lichaam.

In de geavanceerde medische centra van de komende tien jaar, zijn controlesystemen draadloos met een centrale hub verbonden, waardoor verpleegkundigen en artsen real-time toegang hebben tot de vitale functies van hun patiënten en zijn ze zelfs in staat om hen op afstand te behandelen.

De terroristen van de toekomst houden deze ontwikkelingen nauwlettend in de gaten en de potentiële gevolgen zijn haast niet te overzien. Als een arts op afstand een dosis morfine kan toedienen of de toedieningssnelheid van intraveneuze vloeistof kan veranderen, kan een hacker dat straks ook.
Volgens Kim Zetter van Wired, begon een bekende ‘white hat’ hacker en beveiligingsexpert onlangs tijdens een verblijf in het ziekenhuis te twijfelen aan de veiligheid van intraveneuze pompen. Hoewel de hardwaresystemen die toegang geven tot de pomp voor updates gescheiden zijn van de firmware die het apparaat bestuurt, staan ze toch met een seriële kabel met elkaar in verbinding. Zo kan een hacker dus toegang krijgen tot de instellingen van de pomp. Rios ontdekte dat het niet alleen mogelijk is om de hoeveelheid insuline (of antibiotica, chemotherapie, morfine, etc.) te wijzigen, maar dat ook het display van het apparaat gemanipuleerd kan worden waardoor het de oorspronkelijke, juiste dosering blijft weergeven. Al was dit een zeer verontrustende ontdekking, is het tegelijkertijd geen grote verrassing, vooral met het oog op wat we inmiddels weten over andere SCADA kwetsbaarheden en de recente aanval op de Oekraïense energiecentrale.

Hoe meer medische apparaten worden verbonden met het IoT, des te acuter wordt het gevaar

Terroristen nemen in de toekomst niet alleen de controle van SCADA-systemen over, ze zullen ook de displays en controlesystemen zo manipuleren dat niemand iets in de gaten heeft. Hierdoor kunnen ze nóg meer schade aanrichten. Kaspersky Lab bevestigde dat we in ziekenhuizen met dezelfde kwetsbaarheden te maken hebben als die Verizon ontdekte in de waterzuiveringsinstallaties. Verouderde besturingssystemen als Windows XP maken het terroristen wel heel makkelijk om toegang te krijgen tot deze apparaten en vervolgens hoge doses röntgenstraling toe te dienen.

Hoe meer medische apparaten worden verbonden met het IoT, des te acuter wordt het gevaar. Het grootste gevaar dat op de loer ligt is dat terroristen in de toekomst geavanceerde, gelijktijdige aanvallen kunnen uitvoeren op kritieke infrastructuur. Door waterzuiveringsinstallaties, elektriciteitscentrales en ziekenhuizen tegelijkertijd te hacken kunnen miljoenen mensen ziek worden en honderdduizenden sterven.

Schade (digitale) bedrijfsspionage loopt in miljarden

Bron: Nieuwsplatform Securitas

U hebt het goed voor elkaar; de mooiste hardware, de slimste software én een beveiligd bedrijfsnetwerk. Toch bent zelfs u kwetsbaar. Want bij bedrijfsspionage is niet het systeem, maar de mens de zwakste schakel, stelt Mark van den Wijngaard, veiligheidsdeskundige bij Securitas

Gevaren bedrijfsspionage

Het Nederlandse bedrijfsleven is zich volgens Mark van den Wijngaard nauwelijks bewust van de gevaren van bedrijfsspionage. ‘Bedrijven beseffen pas achteraf dat bedrijfsgevoelige informatie is verdwenen. De financiële schade loopt hierdoor in de miljarden en reputatieschade ligt op de loer.’

Cyberrisico’s

Uit een studie van Deloitte naar cyberrisico’s in Nederland van april dit jaar blijkt dat cybercriminaliteit organisaties maar liefst 10 miljard euro per jaar kost. Uitgaande van een worst case scenario kan het verlies voor individuele bedrijven oplopen tot achttien keer meer dan het waardeverlies dat ze mogen verwachten.

Verstoring van operationele continuïteit

Een groot risico op waardeverlies (ruim 40%) komt voort uit het onderbreken van de operationele continuïteit. Dit is het gevolg van gerichte aanvallen door partijen die uit zijn op verstoring, maar ook een bijkomend gevolg van breder gerichte cybercriminaliteit. Verstoring raakt bijna alle organisaties. Een ander groot waardeverlies (bijna 40%) komt voort uit het kwijtraken van intellectueel eigendom, strategische informatie en verminderde betrouwbaarheid van producten en diensten.

Verlies van bedrijfsgevoelige informatie

Bedrijfsgevoelige informatie is volgens Mark van den Wijngaard vaak slecht beveiligd met als gevolg dat concurrenten er met ideeën vandoor gaan of dat data simpelweg kwijtraken. ‘Cyber- en fysieke beveiliging hangen nauw met elkaar samen’, zegt hij. ‘Je kunt alles perfect technisch hebben dichtgetimmerd, maar als er vervolgens via de HR-afdeling een kwaadwillende als sollicitant binnenkomt, dan werkt zelfs de beste beveiligingstechnologie niet meer.’ Een ander voorbeeld is het onbewaakt verrichten van onderhoud aan servers in bijvoorbeeld datacenters. ‘Het kan ronduit gevaarlijk zijn om externen alleen te laten met waardevolle data. Beter is het ‘vier-ogen-principe’ en noodzakelijk onderhoud onder toezicht laten verrichten.’

Social engineering

Voorafgaand aan een (cyber)aanval wordt vaak gebruik gemaakt van social engineering. Daders vergaren gevoelige informatie via lokmails of door onder valse voorwendselen medewerkers te bellen en gebruikersnamen en wachtwoorden te ontfutselen. Daarnaast winnen ze via het internet informatie in over medewerkers van een bedrijf. Mensen delen veel over zichzelf op sociale netwerken als LinkedIn en daar wordt gretig misbruik van gemaakt. ‘Social engineering is een bijzondere tak van sport waartegen maar weinig mensen zijn bestand’, zegt Mark van den Wijngaard. ‘Mensen worden zo gemanipuleerd dat ze toegang geven tot vertrouwelijke gegevens. Daders maken gebruik van psychologische trucs.

Een compliment geven bijvoorbeeld is een veel gebruikte tactiek, dat werkt altijd. Of ze spelen in op je nieuwsgierigheid. Mensen zijn in het begin vaak nog wel alert, dat hebben ze geleerd. Maar zodra ze het gevoel hebben dat iemand vertrouwd is, dan geven ze je alles.'

Informatie prijsgeven

Zo blijken medewerkers van salarisadministraties bereid telefonisch een burgerservicenummer door te geven als ze denken met een medewerker te maken te hebben die het hard nodig heeft, concludeerde Mark van den Wijngaard uit eigen onderzoek. En ook via email geven mensen gemakkelijk informatie prijs, merkte hij. 'In een gecontroleerde bedrijfsomgeving stuurden we als test een Arbo-enquête rond met daarin allerlei vragen over werkomstandigheden. Het thema hadden we expres gekozen. Veel mensen vinden het prettig als het over henzelf gaat. Als ze iets kunnen zeggen over hun eigen omstandigheden.'

Pure misleiding

'In feite was het pure misleiding, een afleidingsmanoeuvre', vervolgt hij. 'Het enige wat wij écht wilden weten was de informatie onder het kopje van de enquête: de naam, functie, standplaats en personeelsnummer. Om te kijken hoe scherp mensen waren schreven we dat de vragenlijst van hun eigen HR personeelsafdeling afkomstig was, maar stuurden we de email en bijlage via een hotmailaccount.'

Met de antwoorden op zak kon een vervolgactie niet uitblijven. Mark van den Wijngaard deed zich voor als medewerker en belde de salarisadministratie met het verhaal dat hij zijn burgerservicenummer nodig had voor het afsluiten van een hypotheek. 'Tot mijn verbazing gaven sommige medewerkers het direct, anderen vroegen naar mijn personeelsnummer en dat had ik natuurlijk. Het bleek kinderlijk eenvoudig om informatie los te peuteren.'

'De nep-enquête werd ondanks de signalen door veel mensen geopend', zegt Van den Wijngaard. 'Dat toont aan hoe naïef we zijn en hoezeer we bereid zijn antwoord te geven op de vragen die ons worden gesteld. Ook al ben je nog zo goed beveiligd, als mens ben je kwetsbaar.'

Informatie is het nieuwe goud

‘Cybercrime, identiteitsfraude en bedrijfsspionage vormen de top drie van huidige dreigingen’, weet de veiligheidsspecialist. ‘Informatie is het nieuwe goud en daarvan komt steeds meer beschikbaar. Tegelijkertijd is bedrijfsspionage gemakkelijker geworden. Voor kwaadwillenden is het slechts een kwestie van de puzzelstukjes verzamelen om een compleet beeld te verkrijgen.’

Volgens Mark van den Wijngaard is het belangrijk dat risico’s beter worden geïnventariseerd en dat medewerkers worden getraind in het herkennen van verdachte mails en telefoontjes. Ook moeten bedrijven ervoor zorgen dat medewerkers afwijkende situaties eenvoudig kunnen melden en dat er duidelijke veiligheidsrichtlijnen zijn.

‘Het veiligheidsbewustzijn binnen een organisatie is pas effectief wanneer dit wordt gewaarborgd in een continu proces’, zegt hij. ‘Dat betekent dat organisaties het risico van bedrijfsspionage en van cybercrime moeten opnemen in hun risicoprofiel. Zij moeten accepteren dat het gebeurt om het vervolgens in securityplannen te kunnen vertalen in maatregelen.’

Need to know of nice to know?

Belangrijke maatregelen zijn volgens hem awareness-programma’s voor medewerkers. Daarnaast moeten organisaties nadenken over de waarde van hun informatie. ‘Informatiebeveiliging is tegenwoordig het belangrijkste wat er is. Je moet dus goed weten wie je toegang geeft tot welke informatie. Is er sprake van need to know, of nice to know? Dat is de vraag die je jezelf moet stellen. Het kan nuttig zijn om informatie te kwalificeren en zo te bepalen tot welk niveau medewerkers toegang krijgen tot bepaalde informatie. Een ander belangrijk thema is een zorgvuldige screening van mensen. Zeker op vertrouwensposities’, zegt Mark van den Wijngaard. ‘Er wordt slecht gescreend, referenties worden vaak nauwelijks gecheckt.’

Awareness-programma’s

Hoewel Securitas niet actief is in ICT Beveiliging, speelt awareness wel een belangrijke rol in awareness-programma’s. ICT komt daarin zeker aan bod. ‘In dit soort programma’s leren we mensen hoe belangrijk het is om zelf na te denken en afwijkingen te signaleren. Daarmee voorkom je narigheid op veel vlakken, fysiek én digitaal. Via bedrijfsspionage kunnen kwaadwillenden sociale interventies uitvoeren op de mensen achter de systemen’, zegt hij. ‘Awareness-programma’s maken mensen bewust. Ze leren bijvoorbeeld dat je bij normafwijkingen nooit privacygevoelige informatie moet prijsgeven. Als je gebeld wordt door de ING bijvoorbeeld, dan moet er een alarmbelletje afgaan. Is een aanbieding te mooi om waar te zijn? Dan klopt het vaak niet.’

De oplossing?

Dat het veiligheidsbewustzijn omhoog moet staat vast. Gemakkelijk is dat echter niet, waarschuwt Mark van den Wijngaard. ‘Het lastige is dat alles wat we denken, doen en uitvoeren gebaseerd is op onze eigen ervaringen. Zolang mensen zelf geen slachtoffer worden is het moeilijk om dit bewustzijn tussen de oren te krijgen. Mensen vormen daardoor de sterkste, maar tegelijkertijd de zwakste schakel.’

Grootschalige, geavanceerde cyberaanvallen: Internetvandalisme of teken aan de wand?

Recent werd er in verschillende delen van de Verenigde Staten melding gemaakt van grootschalige cyberaanvallen waardoor de websites van onder andere Reddit, Amazon, Airbnb, PayPal, Netflix, Twitter, Spotify en de New York Times crashten of urenlang onbereikbaar waren. De storingen werden veroorzaakt door een DDoS-aanval (Distributed Denial of Service) die gericht was op Internet-infrastructuurbedrijf Dyn dat kritieke IT-diensten levert aan grote bedrijven. Tijdens de aanvallen werden de directoryservers van Dyn verstoord. De aanvallen roepen veel vragen op. Zijn het slechte voorbodes?

***Richard van Hooijdonk**, Trendwatcher en Futurist bij BNR Nieuwsradio en Nyenrode University*

Wat is DDoS en wat gebeurt er precies tijdens zo'n cyberaanval?

Dyn is een DNS-provider (Domain Name System), die met haar wereldwijde aanwezigheid meer dan 4 miljoen gebruikers en bedrijven ondersteunt. Als je een bepaald website-adres intikt gaat Dyn op zoek naar de locatie van de server en zorgt er vervolgens voor dat je op de plek van bestemming aankomt. Tijdens DDoS-aanvallen worden servers door miljoenen dataverzoeken dusdanig overweldigd dat reguliere gebruikers van de servers geen respons krijgen. Dit resulteert dan in onbereikbaarheid of vastlopen van websitepagina's en een dramatische daling van websiteverkeer.

Dyn omschreef de aanvallen als ‘complex en zeer geavanceerd’. Niet alleen spraken zij hun bezorgdheid uit over hoe kwetsbaar het Internet is, maar ook over de kracht van degenen die het Internet willen verstoren.

Dit is toch al vaker gebeurd, wat is er nu anders?

Er hebben in het verleden al talloze DDoS-aanvallen plaatsgevonden en dit is op zich geen wereldschokkend nieuws. De aanvallen hebben echter het potentieel om steeds meer problemen te veroorzaken. Het zijn met name de grote bedrijven die de infrastructuur van het Internet leveren die melding maken van een toename van de frequentie, duur, ernst en complexiteit van de DDoS-aanvallen. In vergelijking met eerdere aanvallen, lijken deze nieuwe meer ‘aftastend’, alsof men verschillende servers aan het testen is, op zoek naar het breekpunt, om te zien wat ze aankunnen.

Volgens insiders kan dit erop duiden dat iemand, ergens aan het leren is hoe ze het Internet kunnen platleggen om wijdverbreide verstoring te veroorzaken.

De DDoS-aanvallen werden door middel van gehackte IoT-apparaten uitgevoerd en met name door webcams, CCTV-camera’s en DVR’s, waarvan de onderdelen worden gemaakt door XiongMai Technologies, een Chinees techbedrijf. Het probleem met de onderdelen in deze apparaten is dat hun wachtwoorden hard-gecodeerd in de firmware staan en de gebruiker deze niet kan wijzigen of uitschakelen. Andere *connected* apparaten die gehackt en ingezet kunnen worden bij soortgelijke aanvallen zijn televisies, koelkasten, thermostaten en zelfs babyfoons.

Was het een kwestie van Internetvandalisme of iets sinisters?

Volgens deskundigen is het niet erg waarschijnlijk dat deze aanvallen van criminele aard zijn omdat verstoring criminelen weinig oplevert. Woordvoerders van verschillende inlichtingendiensten vertelden dat het hier slechts ging om een klassiek geval van ‘Internetvandalisme’. Er wordt echter ook gespeculeerd dat landen als Rusland en China zich bezighouden met onderzoek naar wat er mogelijk is met grootschalige DDoS-aanvallen.

De Amerikaanse regering, hoge ambtenaren en cyberspecialisten hebben Rusland er onlangs van beschuldigd cyberaanvallen te hebben uitgevoerd. Volgens hen zijn Russische inlichtingendiensten verantwoordelijk voor het hacken van Hillary Clintons e-mails met de bedoeling de presidentsverkiezingen te beïnvloeden. Niemand heeft de verantwoordelijkheid voor de aanvallen van de 21e echter nog opgeëist.

Een aantal beveiligingsbedrijven hebben gemeld dat de DDoS-aanval waarschijnlijk gepleegd werd door de Mirai-malware die gebruikt wordt om botnet- of zombielegers te creëren en vervolgens op zoek gaat naar IoT-apparaten als digitale videorecorders en IP-camera's met standaardwachtwoorden. De malware kan miljoenen apparaten infecteren en hiermee DDoS-aanvallen uitvoeren met als doel een overbelasting van kritieke infrastructuur te veroorzaken. Een persoon met de naam 'Anna-senpai' heeft de source code voor de malware achter het irai-botnet onlangs online gezet.

Dit wordt vaker gedaan door criminelen om te voorkomen dat zij niet de enigen zijn die over de software beschikken en zo minder eenvoudig door opsporingsdiensten of beveiligingsbedrijven gevonden worden. Soortgelijke botnets worden overigens ook gewoon op het Internet verhandeld. Als je maar genoeg bitcoins hebt kun je ze kopen en gebruiken waar en hoe je maar wilt. De verwachting is dan ook dat het aantal aanvallen door de publicatie van de broncode zal toenemen.

Wat de hackers hebben willen bereiken is nog steeds onduidelijk. Aanvallen in het verleden vonden meestal bij specifieke bedrijven plaats en dan werd er losgeld gevraagd. In dit geval is daar geen sprake van. Het is wel duidelijk dat de aanvallen zeer geavanceerd zijn, wat suggereert dat we niet te maken hebben met een tiener die aan het experimenteren is. Beveiligingsspecialist Bruce Schneier beweert dat iemand probeert uit te zoeken hoe sterk het verdedigingsmechanisme is van de bedrijven die kritieke punten van de Internetinfrastructuur beheren en hoe het Internet platgelegd kan worden.

De beveiligingsproblematiek van het IoT bezorgt de NSA slapeloze nachten

Rob Joyce van de Operations Tailored Access-eenheid van de NSA, leidt een team van hackers dat inlichtingen verzamelt door computernetwerken te hacken. Het team hackt ook Amerikaanse netwerken om te bepalen waar de beveiliging kan worden verbeterd.

Joyce maakte bekend dat het Internet of Things en het gebrek aan adequate beveiliging het zeer eenvoudig maken om bepaalde doelen aan te vallen. De slechte beveiliging van IoT-apparaten zoals controlesystemen maakt het mogelijk om eenvoudig toegang te krijgen tot organisaties. Dit feit wordt door computernetwerkbeheerders vaak over het hoofd gezien.

Ook is het voor organisaties moeilijk om te detecteren wanneer zo'n hack gebeurt. De grootste zorg is dat hackers via deze apparaten ook van binnenuit toegang krijgen tot zakelijke, defensie- en staatsnetwerken, zonder door firewalls en andere intrusion prevention-systemen opgemerkt te worden. Duizenden van deze commerciële en industriële SCADA-systemen, inclusief kritieke infrastructuur zoals elektriciteitscentrales, zijn haast argeloos op het Internet aangesloten. "De problematiek rond SCADA-beveiliging bezorgt me slapeloze nachten," zegt Joyce.

Alles wat verbonden is met het Internet of Things is tot op zekere hoogte te hacken. Denk daarbij aan je Apple Watch, je slimme koelkast, de verbonden auto die je rijdt of de Hello Barbie van je dochter. Bar weinig van deze apparaten zijn afdoende beveiligd en dat is de droom van elke hacker. Ook bij zorginstellingen vervult het Internet of Things een steeds belangrijkere rol, een sector die de afgelopen jaren ook al verschillende keren slachtoffer is geworden van cyberaanvallen. Volgens Chris Sullivan van Core Security zijn de recente DDoS-aanvallen een indicatie dat we in de toekomst met nog geavanceerdere aanvallen te maken krijgen. Denk hierbij aan diefstal van creditcards en wapenontwerpen. Ook is men met deze aanvallen in staat om banken via SWIFT te hacken, het systeem dat het betalingsverkeer tussen alle banken wereldwijd regelt.

Bovendien kan men met de aanvallen ook fysieke schade aanrichten, zoals het geval was met de hack die plaatsvond bij oliegigant Saudi Aramco in 2012. Tijdens de aanval werden 30.000 computers beschadigd en werden daarbij van allerlei systemen gegevens buitgemaakt. Vervolgens werden de computers en servers compleet gewist. Hierdoor moest de grootste olieproducent ter wereld weer schrijfmachines en faxapparaten gebruiken. Pas vijf maanden later slaagde Saudi Aramco erin de schade te herstellen en kon het bedrijf weer online. Uiteraard met een nieuw computernetwerk en een uitgebreid beveiligingssysteem. Volgens beveiligingsexperts heeft het bedrijf geluk gehad dat het Shamoon-virus geen permanente schade aanrichtte aan de oliefaciliteiten, anders waren de gevolgen niet te overzien geweest.

We lijken er helaas weinig aan te kunnen doen

Helaas is het zo dat we bestaande IoT-apparaten niet beter kunnen beveiligen en gebruikers moeten er dan ook zelf voor zorgen dat hun privégegevens veilig zijn. Het grootste probleem is dat veel mensen niet eens weten, of niet geloven, dat hun thermostaat of webcam gehackt kan worden en dat criminelen op die manier toegang kunnen krijgen tot hun persoonlijke informatie. De enige manier om deze problemen te voorkomen is als bedrijven hun producten afdoende beveiligen. Maar zonder product recalls, nieuwe industrienormen, rechtszaken of regelgeving van de overheid zal dit naar alle waarschijnlijkheid niet gebeuren.

Het probleem is dat we de wereld zo razendsnel genetwerkt hebben dat de beveiliging van de miljoenen IoT-apparaten en goedkope sensoren daar geen gelijke tred mee heeft kunnen houden. De techbedrijven moeten de verantwoordelijkheid op zich nemen en de problemen oplossen die ze gecreëerd hebben. De allerbeste manier om een eind te maken aan ransomware en DDoS-aanvallen zou uiteraard zijn om al onze miljoenen IoT-apparaten los te koppelen van het Internet, maar dat is in de huidige tijd geen reële optie. Dan is er ook nog de kwestie van aansprakelijkheid. Wie is er verantwoordelijk als er iets misgaat? De eigenaar van het apparaat? De fabrikant? De hacker? En het gaat niet alleen om cyberaanvallen. Stel je voor dat je slimme apparaat zoals je koelkast gebruikt zou worden voor het verspreiden van kinderporno, bij wie ligt dan de verantwoordelijkheid?

‘Slechts’ een paar dagen zonder Internet zou voor iedereen rampzalige gevolgen hebben

Wat er op de 21e heeft plaatsgevonden heeft geleid tot speculaties over een cyberaanval die het hele Internet langdurig zou platleggen, met enorme schade voor de economie. Een volledige Internetuitval zou waarschijnlijk gevolgd worden door een moment van stilte, en dan een collectieve, wereldwijde schreeuw. Met andere woorden, het zou rampzalig zijn, al zeggen experts dat de kans dat dit gebeurt niet erg groot is.

Het Internet is een uiterst flexibel netwerk van netwerken van nóg meer netwerken. Als een deel ervan uitvalt, werken de resterende delen gewoon door. Maar als er bijvoorbeeld sprake was van een zonnestorm, of iemand sneed de onderzeese glasvezelkabels door, en het hele Internet zou vervolgens een of twee dagen platliggen, wat dan?

Onze eerste reactie zou waarschijnlijk irritatie zijn. Omdat we niet kunnen googlen, geen Whatsapp-berichten kunnen sturen, geen toegang hebben tot social media, niet naar muziek kunnen luisteren of online shoppen en films kijken. Communicatie zou dan erg moeilijk zijn. Ook zouden we geen nieuwsberichten ontvangen. Dan komt de realisatie dat we voor veel meer dan alleen entertainment afhankelijk zijn van het Internet en dat een langdurige storing ernstige chaos kan veroorzaken.

We zouden geen toegang hebben tot ons geld, automatische betalingen zouden niet doorgaan en onze salarissen zouden niet op onze rekening verschijnen. We zouden geen spullen kunnen kopen of kunnen reizen. Dan zijn er de verkeerssystemen die niet werken en de hulpverleningsdiensten die niet bereikbaar zijn. Logistieke systemen zijn ook sterk afhankelijk van het Internet en bedrijven die hun rekeningen niet betalen ontvangen geen goederen van hun leveranciers. Met lege winkels, paniek onder de burgers en zelfs rellen als resultaat.

De recente DDoS-aanvallen waren de grootste ooit vertoond op het Internet en beveiligingsambtenaren van de Amerikaanse overheid hebben aangegeven dat er serieuze pogingen zijn geweest om kritieke onderdelen van de Amerikaanse infrastructuur uit te schakelen. Ook is men bezorgd over gecoördineerde aanvallen op het elektriciteitsnet die hele regio’s in duisternis zouden hullen, en deze zorgen zijn niet ongegrond. Misschien is de kans dat dit binnenkort gebeurt nog niet erg groot, maar hij is wel degelijk aanwezig.

Betere beveiliging mobiele data en apparatuur

Minder dan een op de vijf Nederlanders heeft zijn smartphone, laptop of tablet zodanig beveiligd dat hij zijn mobiele apparatuur bij diefstal onbruikbaar kan maken. Hierdoor loopt ruim 80% van de Nederlanders het risico dat persoonlijke gegevens na diefstal op straat belanden. Daarom roept minister Van der Steur (Veiligheid en Justitie) Nederlanders op hun mobiele apparaat 'Boefproof' te maken. Ook dertien partijen uit de telecom- en ICT-sector, die zijn aangesloten bij brancheverenigingNederland ICT, maken zich sterk voor deze betere beveiliging. Daarom is een actieplan ondertekend om diefstal van mobiele apparatuur en misbruik van mobiele data terug te dringen.

Boefproof

"Vanuit de overheid stimuleren we dat mensen hun mobiele apparatuur Boefproof maken om diefstal terug te dringen," zegt minister Van der Steur. Sinds de start van de Boefproof-campagne in 2014 is het aantal gestolen smartphones met 30% gedaald. "Onze vorige Boefproof-campagnes zijn een fantastisch voorbeeld van samenwerking. Naar aanleiding van dit succes voegen wij dit jaar ook tablets en laptops toe aan deze campagne," vervolgt Van der Steur.

Maatschappelijke verantwoordelijkheid

"Het belang van goede beveiliging van zowel apparatuur als data wordt in de sector breed gedragen. Dat blijkt uit de steun voor het actieplan", aldus Jeannine Peek, voorzitter Nederland ICT en algemeen directeur Dell Technologies. "De sector beseft dat hier sprake is van een maatschappelijke verantwoordelijkheid en werkt daarom graag mee aan de Boefproof-campagne."

Activeren of installeren van een anti-diefstalfunctie

Boefproof maken is het activeren of installeren van een anti-diefstalfunctie op je mobiele apparaat, waardoor je deze op afstand kunt blokkeren. Denk hierbij aan een functie zoals ‘vind mijn smartphone/tablet’ en speciale anti-diefstal software. Hierdoor wordt het gestolen apparaat waardeloos voor dieven en hebben ze geen toegang tot mail, foto’s en vertrouwelijke documenten. Op dit moment is bijna een kwart van de smartphones Boefproof (23,6%), gevolgd door tablets (17,7%) en laptops (12,2%).

Recent onderzoek in opdracht van het ministerie van Veiligheid en Justitie, toont aan dat 43,1% van de Nederlanders niet weet dat zij hun mobiele telefoons en laptops zo kunnen instellen dat deze onbruikbaar worden bij diefstal. Hierbij geeft 40,3% van de Nederlanders aan niet te weten hoe je je mobiele apparaat Boefproof maakt, terwijl dat in de praktijk eenvoudig is.

Actieplan

Minister Van der Steur en dertien partijen uit de telecom- en ICT sector, die zijn aangesloten bij brancheverenigingNederland ICT, ondertekenden een Boefproof-actieplan. Het doel daarvan is het aantal Boefproof gemaakte mobiele apparaten te vergroten en zo het aantal gestolen smartphones, tablets en smartphones verder terug te dringen. De deelnemende bedrijven zijn zowel hardware fabrikanten, als providers. Deelnemende fabrikanten zijn Microsoft Nederland, Samsung Electronics Benelux, Apple Inc., Dell Technologies, HP Netherlands, Sony Mobile Communications, Huawei Technologies (Netherlands) B.V. De deelnemende providers zijn KPN, T-Mobile Netherlands B.V., Ziggo, Simyo, Vodafone Nederland en Tele2.

De private partijen spannen zich zoveel mogelijk in dat klanten hun mobiele apparatuur Boefproof kunnen maken en zullen dit ook nadrukkelijker onder de aandacht brengen bij hun klanten. Het ministerie zet via de landelijke Boefproof campagne in op het breed verspreiden van preventietips via social media, Facebook en abri’s om zo het gebruik van de beveiligingsmogelijkheden extra te stimuleren.

Vitale Infrastructuur, belangrijk doelwit van ‘Nation-State sponsort’ cyber aanvallen

Cyberspace is uitgegroeid tot een volwaardige oorlogsvoeringsdomein als regeringen / overheidsgesponsorde groepen over de hele wereld botsen om de digitale suprematie in een nieuwe, veelal onzichtbare wereld van operaties. Vanuit het militaire perspectief wordt cyberspace reeds het vijfde domein van oorlogsvoering genoemd en hebben reeds vele landen militaire eenheden opgericht om actief te kunnen zijn in dit domein.

***Jaap Schekkerman**, directeur onderzoek bij het Cyber Research Center – Industrial Control Systems*

Cyberaanvallen

Cyberaanvallen zijn niet meer alleen het domein van opportunistische criminelen, maar zijn een steeds belangrijker wapen voor overheden in haar streven om de nationale soevereiniteit te verdedigen en om haar macht / kracht te etaleren. Voorbeelden hiervan zijn strategische cyber spionage campagnes, zoals Moonlight Maze (1998) en Titan Rain, tot aan destructieve acties, zoals cyber aanvallen op Iran (Stuxnet), Georgië, Oekraïne (BlackEnergy3) en vele andere landen. Internationale conflicten komen in een nieuwe fase in hun lange geschiedenis waarbij de nucleaire dreiging vervangen wordt door de cyber dreiging. In deze schimmige wereld worden doelen bevochten met bits en bytes in plaats van kogels, malware in plaats van milities en botnets in plaats van bommen.

Ongezien en geheim

Deze geheime aanvallen vinden grotendeels ongezien plaats voor het publiek. In tegenstelling tot de oorlogen van weleer, produceren deze cyberoorlogen niet direct dramatische beelden van exploderende bommen, verwoeste gebouwen of vluchtende burgers. Maar de lijst van serieuze slachtoffers wordt met de dag groter en bevat reeds een aantal van de grootste namen in de technologie, financiële diensten, defensie, overheid, staalindustrie, olie & gas en elektriciteit. Dit soort type cyberaanvallen kan het best begrepen worden, niet als een doel op zich zelf, maar als een potentieel krachtig middel om een breed scala van politieke, militaire en economische doelen te bereiken.

Impact en bescherming

Maar zijn we ons bewust van deze cyberdreigingen en kennen we de impact? Kunnen we onszelf beschermen tegen deze cyber dreigingen? Of moeten we accepteren dat we worden gecompromiteerd en als dat zo is, zijn we dan voorbereid op een dergelijke situatie? Het Cyber Research Center - Industrial Control Systems / vitale infrastructuur is een onafhankelijke, not for profit, onderzoeks en expertisecentrum dat werkt aan de laatste ontwikkelingen op het gebied van fysieke & cyber bescherming en de daarmee gepaard gaande weerbaarheid. Onze doelstellingen zijn het doen van onderzoek van 'nation-state gesponsort’ cyberaanvallen op industrieën / vitale infrastructuren m.b.t. de snel veranderende dreigingen waarmee zij worden geconfronteerd en de maatregelen, controles en technieken die kunnen worden toegepast om beter voorbereid te zijn, als ook om te gaan met deze cyberdreigingen.

De complexe, gevaarlijke en verontrustende wereld van het Darknet

Het Internet dat we allemaal kennen is eigenlijk een sluier die een moreel en ethisch verontrustende cyberonderwereld verbergt, beter bekend als het Darknet. Het Darknet is niet alleen een toevluchtsoord voor politieke bloggers en revolutionairen; het is ook een duistere, wetteloze plek waar het wemelt van de criminelen.

***Richard van Hooijdonk**, Trendwatcher en Futurist bij BNR Nieuwsradio en Nyenrode University.*

Internet, Deep Web, Darknet – wat is wat?

Het normale Internet is redelijk ‘clean’ en iedereen kan er gebruik van maken. Daar onder bevindt zich het Deep Web, een deel van het Internet dat voor onze gewone zoekmachines te groot en te complex is om te indexeren. Mensen die door censuur beperkte Internettoegang hebben en ook activisten en journalisten die vrezen voor hun leven maken gebruik van het Deep Web. Daarnaast vindt je in het Deep Web talloze privébestanden, grote databases, academische stukken en bibliotheken die niet voor het gewone publiek toegankelijk zijn. Het Deep Web zelf is niet verontrustend, maar dat is het Darknet wel.

Het Darknet: een complexe, gevaarlijke en verontrustende onderwereld

Het Darknet is een niet geïndexeerd, geheim deel van het Deep Web, dat voornamelijk gebruikt wordt voor illegale en criminele praktijken. Het Darknet is niet toegankelijk via onze reguliere browsers. Het bestaat uit websites met .onion domeinen en de browsersoftware die nodig is om deze sites te bezoeken heet Tor, of ‘the Onion Router’. Met Tor heb je toegang tot vele sites zonder je IP-adres kenbaar te maken. Een ander ‘privé netwerk’ op het Darknet dat gestaag aan populariteit wint, is het onzichtbare Internet Project of I2P. I2P biedt verschillende verbeteringen, zoals de opslag en het delen van bestanden, beveiligde mail en blog- en chatfuncties. Het Darknet werd in 2002 ontwikkeld door de Amerikaanse marine, met als doel een platform te creëren voor anonieme communicatie. Dit inspireerde tot de naam ‘anonymous net’. Op dit moment zijn er tussen 7,000 en 60,000 .onion sites op het Darknet.

Wie zijn de gebruikers van het Darknet?

Omdat Tor ontwikkeld is door de Amerikaanse marine, behoren militaire-, politie- en overheidsorganisaties tot belangrijke Darknet gebruikers. Op het ‘normale’ Internet is je locatie en met wie je communiceert makkelijk te vinden, ook bij een versleuteld gebruik en dat is gevaarlijk voor overheidsdiensten. Het Darknet is ook populair in landen waar politieke gevangenschap en censuur de gewoonste zaak van de wereld zijn. Daarom vind je hier veel bloggers, klokkenluiders, activisten en journalisten. De anonimiteit van het Darknet geeft hen de mogelijkheid te communiceren zonder het risico te lopen gepakt te worden. Ook kunnen ze zich organiseren zonder dat hun locatie bekend wordt. Maar op het Darknet wemelt het ook van criminelen en duistere groepen zoals drugsdealers, pornograven, politieke extremisten, huurmoordenaars en hackers. Op de beruchte Darknet markten heb je met een muisklik toegang tot allerlei sinistere diensten en producten. Je kunt betalen met Bitcoins of ander cryptogeld en je bestelling wordt voor je deur afgeleverd.

De opkomst en ondergang van de beruchte Silk Road markt

Een van de bekendste Darknet sites was de beruchte Silk Road Drugs Markt. Het was de grootste op het Internet en alleen toegankelijk via Tor, ver van het gewone publiek. In 2013 werd de site door de FBI opgerold en werd de oprichter van en het brein achter Silk Road, Ross William Ulbricht, gearresteerd. Hij werd veroordeeld voor drugshandel, hacken en witwassen van geld. De FBI nam $ 33.6 miljoen aan Bitcoins in beslag. Velen dachten hiermee een slag te hebben geslagen in de strijd tegen de cybermisdaad, maar de waarheid is anders.
Vele andere sites zagen meteen het licht, zoals Silk Road 2.0 en 3.0 en Evolution. Op deze sites zijn wapenhandel, drugs, kinderpornografie, vervalsing van documenten en zelfs huurmoorden de gewoonste zaak van de wereld.

Drugs: van sigaretten tot Devil’s Breath

Er zijn duizenden drugs verkrijgbaar op Darknet, variërend van ‘onschuldige’ sigaretten tot harddrugs en alles wat zich daar tussen bevindt. Denk aan cannabis, heroïne, geestverruimende middelen, ecstasy en pijnstillers en steroïden. Sommige dealers geven hun klanten zelfs gratis proefmonsters. Tevreden klanten kunnen een beoordeling achterlaten. Een voorbeeld van een marihuana review: “Zeer krachtig en schoon spul. Sensationele geur, 30 gram op schaal ;-)” De meest afschrikwekkende drug ter wereld, Devil’s Breath, is ook te koop op het Darknet. Van deze drug wordt beweerd dat als het in iemands gezicht wordt geblazen, het slachtoffer in een willoze zombie verandert, met alle gevolgen van dien. Denk aan inbraken, leeggehaalde bankrekeningen of gestolen organen. Er zijn honderden misdaden aan de mysterieuze drug toegeschreven, maar in hoeverre de verhalen op waarheid berust zijn, is onbekend.

‘Snuff’ films en ‘crush’ films – geen alledaagse porno

‘Doorsnee’ pornografie is zeer toegankelijk op het Internet. Het soort porno dat je op het duistere Darknet vindt, is echter van een heel ander kaliber. Er is een overvloed aan kinderpornografie en ook verkrachtings- en ‘snuff’ films zijn geliefde koopwaar. ‘Crush’ porno, waarin dieren op brute wijze worden vermoord, zijn er ook te vinden. Dit soort pornografie is het meest verontrustende aspect van het Darknet en omdat deze sites achter die versleutelde sluiers verborgen gaan, is het vrijwel onmogelijk ze te op te sporen en te verwijderen.

Forums die eetstoornissen en zelfs zelfmoord aanmoedigen

Het Darknet biedt ook plaats aan forums waar mensen met eetstoornissen en depressies elkaar ontmoeten. Op deze forums worden tips uitgewisseld over hoe je jezelf het beste kunt uithongeren en leden worden toegejuicht als ze dagenlang niets eten. Op zelfmoordforums worden leden aangemoedigd hun zwarte gedachten te koesteren en zelfmoord-partners te vinden. Door velen wordt dit veroordeeld, anderen vinden het bevrijdend en zelfs therapeutisch, omdat het leden de mogelijkheid geeft om open en eerlijk over hun verontrustende gedachten te praten.

Valse paspoorten, sofinummers en creditcards

Op het Darknet kun je verschillende vervalste documenten kopen, zoals rijbewijzen en sofinummers en digitale paspoorten. ‘Echte’ paspoorten zijn moeilijker te verkrijgen, maar niet onmogelijk. Je kunt er vervalst geld kopen en voor $8 heb je zo een creditcardnummer. Ook kun je er voor een paar dollar een gehackte bankrekening of een PayPal-, Uber- of Netflixaccount kopen.

Wapens en huurmoordenaars

Daarnaast worden er enorm veel wapens aangeboden op het Darknet, varierend van eenvoudige 9mm pistolen tot kalasjnikovs. Ook kun je er elektromagnetische puls devices uit China kopen, waarmee tegoeden van gokkasten bij het casino kunnen worden opgewaardeerd maar je kunt er ook elektrische apparaten mee ‘wissen’. Met een heavy duty device kun je zelfs het elektriciteitsnet van een stad platleggen. En het gaat nog veel verder. Je kunt er ook doe-het-zelf bommen en granaten kopen of bommen uit de Eerste Wereldoorlog. Verder vind je er gebruiksaanwijzingen voor het bouwen van een 3D-geprint wapen en stap-voor-stap instructies voor het hacken van een geldautomaat. Maar de meest sinistere Darknet sites zijn toch wel diegene waar je voor $150.000 een huurmoordenaar inhuurt of sites waar je uraniumerts kunt kopen. Het is niet moeilijk om je voor te stellen wat daarmee allemaal mogelijk is…

Het oprollen van het Darknet: een eindeloos kat-en-muisspel?

Op het moment dat Silk Road werd opgerold, verschenen er honderden andere illegale marktplaatsen als AlphaBay en Agora en de economie van het Darknet verdubbelde. Volgens een recente studie van de universiteit van Carnegie Mellon, gaat er dagelijks meer dan $500.000 om in het Darknet ecosysteem. De FBI doet zijn uiterste best om zoveel mogelijk criminele sites op te rollen, maar het is vechten tegen de bierkaai. Ook is de anonimiteit van het Darknet tweeledig.
Het wordt weliswaar misbruikt voor sinistere, criminele doeleinden, maar er bevinden zich ook mensen en groeperingen die geen kwaad in de zin hebben.

Nederlanders niet voorbereid op cybercrime

Nederlanders weten te weinig over online gevaren en hoe zij zich daartegen kunnen beschermen. Ook onderschatten zij de kans dat zij slachtoffer worden van cybercrime. Dit blijkt uit het onderzoek ‘Cybersecurity awareness en skills in Nederland (2016)' van Alert Online. Ruim de helft van de Nederlanders heeft nog nooit van ransomware gehoord, terwijl dit de snelst groeiende dreiging op internet is.

Ransomware populair geworden onder cybercriminelen

Ransomware is de laatste paar jaar enorm populair geworden onder cybercriminelen. Het virus gijzelt je computer door bestanden ontoegankelijk te maken en geeft deze pas vrij als je losgeld hebt betaald. In 2015 had 65% van de Nederlanders nog nooit van ransomware gehoord. Inmiddels is dit gedaald naar 53%. Dat 15% van de ondervraagden zelf slachtoffer is geworden van gijzelsoftware of iemand kent die ermee te kampen heeft gehad, lijkt mede oorzaak te zijn van deze daling. Hoewel de helft van de Nederlanders dit soort online risico’s kent, gedraagt lang niet iedereen zich daarnaar. Zo verzuimen veel Nederlanders automatische updates aan te zetten (52%) of regelmatig back-ups te maken (eveneens 52%), terwijl deze maatregelen cruciaal zijn om je bijvoorbeeld tegen ransomware te beschermen en schade bij besmetting te beperken.

Nederlanders onderschatten kans dat zij slachtoffer worden

De meerderheid van de Nederlanders (69%) maakt zich weinig zorgen over zijn digitale veiligheid. Zij schatten de kans dat zij slachtoffer worden van de grootste dreigingen op internet, zoals ransomware, phishing en malafide advertenties, veel lager in dan in werkelijkheid het geval is. Staatssecretaris Dijkhoff van Veiligheid en Justitie: “Internetcriminelen weten steeds weer nieuwe vormen te vinden ons te verleiden om bijvoorbeeld hun vervalste mails te openen, in te gaan op verzoeken of om op malafide advertenties te klikken. Wij moeten daarom ook steeds slimmer worden door onze cyberskills te verbeteren. Dit onderzoek laat zien dat we hier nog flinke stappen moeten zetten.

Tips ter bescherming

Voor wie zich tegen ransomware wil beschermen of schade wil voorkomen hieronder drie belangrijke tips:

- Maak regelmatig een back-up van bestanden.
- Update software direct. Het helpt om automatisch updaten in te stellen.
- Klik niet zomaar op bijlagen of links in e-mails. Het kan een valse e-mail zijn.

De toekomst van biometrische datacollectie en identificatie in relatie tot cyber security

We zijn altijd al gefascineerd geweest door biometrische technologie. Elk individu is uniek en kan worden geïdentificeerd door middel van zijn of haar intrinsieke gedrag en fysieke eigenschappen. Veel sci-fi films van begin 21e eeuw bevestigen onze fascinatie met biometrie. Denk bijvoorbeeld aan iRobot, Minority Report en Skyfall, de film waarin het Walter PPK pistool van James Bond alleen afgeschoten kan worden als hij het wapen zelf vasthoudt. Deze waren stuk voor stuk een blik in een toekomst waarin ons DNA onlosmakelijk verbonden is met onze digitale identiteit.

Biometrische identificatiemethoden

We gebruiken biometrische technologie al om onze smartphones te ontgrendelen en bijvoorbeeld om toegang te krijgen tot een gebouw. Onze fitnesstrackers verzamelen biometrische gegevens om onze vitale statistieken te monitoren en ons te vertellen hoe goed we hebben geslapen. Ze weten waar we zijn en wat we doen. In ons streven om biometrische technologie en de toepassingen ervan te verbeteren, tasten we voortdurend nieuwe gebieden af. Een aantal biometrische identificatiemethoden die al gebruikt worden zijn vingerafdrukken, DNA, netvlies, hand en gezicht. Maar wist je dat er methoden ontwikkeld en getest worden waarbij gebruik gemaakt wordt van je oren, geur, toetsaanslagen, hersensignalen, ‘wachtwoord-pillen’ en zelfs selfies? Een van de meest interessante is wel de elektronische tatoeage. Laten we daarmee beginnen.

Tech Tatt, de elektronische tatoeage van Chaotic Moon

Chaotic Moon is een Amerikaans bedrijf uit Texas dat mobiele apps ontwikkelt. Het is met name bekend als de maker van vuurspuwende drones en fitnesstrackers waarmee je bitcoins kunt verdienen. Volgens Chaotic Moon's CEO, Ben Lamm, is het Tech Tatt biowearables project een van de meest opwindende Chaotic Moon projecten ooit. In het project wordt geleidende verf met verschillende elektronische componenten gecombineerd om tatoeages te maken die direct communiceren met je huid. Door middel van de elektronische schakelingen in de tatoeages kun je gegevens verzenden, ontvangen, verzamelen en opslaan. Tech Tatts bieden volledige integratie en een betaalbaar alternatief voor de duurdere, dikkere apparaten zoals de huidige fitnesstrackers. Omdat de Tech Tatts direct contact maken met je huid zijn de biometrische gegevens die ze verzamelen en uploaden via Bluetooth ook veel nauwkeuriger. Je kunt de tattoo's gewoon opplakken en je hebt er verder geen omkijken naar.

Net als fitnesstrackers die je vitale statistieken meten, kan de Tech Tatt dat ook. In plaats van jezelf elk jaar medisch te laten doorlichten kun je met deze biowearables op je huid je vitale statistieken zoals hartslag en bloeddruk zelf meten. En als er gezondheidsproblemen zijn, dan stuurt Tech Tatt een signaal naar je arts. De Tech Tatts kunnen ook ingezet worden (of eigenlijk, opgeplakt worden) om soldaten te monitoren tijdens missies. Zo detecteert de tattoo gifstoffen en ziektekiemen in het lichaam en meet de biowearable de hartslag en transpiratie- en adrenalineniveaus om te zien of de soldaat gewond of gestrest is. De locatie-tracking features in de tattoo zijn ook zeer geschikt om kinderen in de gaten te houden bij een bezoek aan een drukke dierentuin of een overvol strand. De mogelijkheden zijn vrijwel ongelimiteerd.

Er kan ook allerlei persoonlijke informatie worden verwerkt in de printplaat van de Tech Tatt. Op die manier hoef je je ID kaart of je pinpas niet meer bij je te dragen. Je kunt met de Tech Tatt ook geld opnemen of bij de supermarkt betalen voor je boodschappen. Identificatiedata en pincodes worden opgeslagen op de controller op de huid. Deze data wordt vervolgens met je vingerafdruk of met een handgebaar naar een 'tap-to-pay' apparaat overgebracht.

MasterCard introduceert biometrische beveiliging en identificatie

Tot nu toe hadden klanten wachtwoorden of pincodes nodig als ze online of in een winkel willen betalen. Maar deze informatie kan gestolen, vergeten of gemanipuleerd worden. Een recent onderzoek heeft uitgewezen dat meer dan de helft van de online shoppers minstens eens per week één of meerdere wachtwoorden vergeet. De introductie van ApplePay heeft bewezen dat men er over het algemeen geen probleem mee heeft om zichzelf met behulp van biometrische gegevens – zoals de iPhone vingerafdruk-scanner – te identificeren. En banken en andere financiële instellingen zoals MasterCard gaan hier nu ook mee aan de slag. In een poging om fraude te bestrijden, is deze wereldwijde betaalgigant een pilot gestart met een biometrische betaalservice waar 500 klanten aan deelnemen.

In deze pilot – de MasterCard Identity Check – worden experimenten gedaan met vingerafdrukken en technologie als gezichts- en stemherkenning. Gebruikers kunnen met dit nieuwe systeem niet alleen met hun stem of vingerafdruk online betalen, maar ook door middel van een selfie die gemaakt wordt door met je ogen te knipperen. Omdat de hele wereld ‘selfie-crazy’ is, denkt MasterCard dat met name deze specifieke identificatiemethode echt zal aanslaan. Overigens wordt er niet letterlijk een foto gemaakt, maar een scan die het gezicht of de vinger van de gebruiker ‘in kaart’ brengt en omzet in binaire code van enen en nullen. MasterCard bevestigde dat persoonlijke klantgegevens beveiligd verzonden en opgeslagen worden op de servers van het bedrijf. Cybersecurity-deskundigen geven echter aan dat het veiliger is als de gegevens op de telefoon van de gebruiker worden opgeslagen. Eén centrale locatie met miljoenen klantgegevens is voor hackers natuurlijk een zeer aantrekkelijk doelwit.

Zodra de pilot succesvol blijkt en alle alle kinderziektes overwonnen zijn, wordt deze innovatieve beveiligingsoplossing aan het publiek geïntroduceerd. Er zijn inmiddels al partnerships gevormd met bedrijven als Samsung, Google, Apple, Microsoft en BlackBerry. MasterCard heeft aangegeven dat hun biometrische identificatiemethoden binnen vijf jaar voorgoed met pincodes en wachtwoorden afrekenen.

Biometrische technologie als identificatiemethode is straks niet meer weg te denken

Het lijkt erop dat biometrische technologie inmiddels een internationaal fenomeen is dat op miljoenen smartphones, op de meeste grote luchthavens en bij een aantal van de grootste banken al wordt gebruikt. Ook wordt het door het publiek in toenemende mate als identificatiemethode geaccepteerd.

Uit diverse onderzoeken en enquêtes door bedrijven als Visa is gebleken dat de meeste Europese burgers tussen de 17 en 25 jaar geen problemen hebben met biometrische identificatiemethoden in plaats van wachtwoorden. Onderzoek van WorldPay toonde aan dat bijna de helft van de Europese consumenten biometrische betaling als alternatieve methode zou verwelkomen. Een meer specifiek voorbeeld van het gebruik van biometrische technologie is Barclays Bank in het Verenigd Koninkrijk. Zij bieden hun klanten bijvoorbeeld identificatiemethoden als spraakherkenning.

In Zweden en Polen zijn diverse geldautomaten al uitgerust met aderherkenningstechnologie. Hiermee kunnen consumenten in plaats van met een PIN nu ook geld opnemen door hun aderen te scannen.

Bedenkingen cybersecurity experts bij deze nieuwe ontwikkelingen

De introductie van biometrie ter vervanging van de huidige identiteitscontroles zoals wachtwoorden, pincodes en ID cards brengt ongetwijfeld ook minpunten met zich mee. Een uitdaging is bijvoorbeeld de verschuiving van fysieke misdaad naar cyber- of informatiecriminaliteit.

Het gebruik van biometrie kan gerichte aanvallen in de hand werken. Beveiligingssystemen die vingerafdrukken gebruiken zijn in het verleden al diverse keren gehackt. Met residuele vingerafdrukken op voorwerpen zoals een glas kunnen met gemak nep-afdrukken gemaakt worden. Met een digitale camera en goedkope huishoudproducten als gelatine maakte cryptograaf Tsutomu Matsumoto een paar jaar geleden al een ‘gummi’ kopie van een echte vinger.

Ook hebben een aantal gebruikers van vingerafdruk-beveiligingssystemen al melding gemaakt van verschillende ‘valse’ positieve identificaties. Aan de hand van deze uitdagingen, gecombineerd met mogelijke diefstal van biometrische gegevens en daaruit voortvloeiende identiteitsdiefstal, kunnen we concluderen dat biometrische betalingssystemen voorlopig niet op grote schaal toegepast zullen worden.

Beroepscriminelen steeds groter gevaar voor digitale veiligheid in Nederland

Beroepscriminelen organiseren zich steeds beter en maken gebruik van geavanceerde digitale aanvalsmethoden. Het afgelopen jaar vonden verschillende grootschalige aanvallen plaats met een hoge organisatiegraad, gericht op diefstal van geld en kostbare informatie. Naast de overheid waren bedrijven en burgers hiervan in toenemende mate het slachtoffer. Beroepscriminelen vormen daarmee een steeds grotere bedreiging voor de digitale veiligheid in Nederland. Dat blijkt uit het Cybersecuritybeeld Nederland 2016 (CSBN 2016) dat staatssecretaris Dijkhoff aanbood aan de Tweede Kamer.

Actuele cyberdreigingen

Afgelopen jaar was sprake van toenemende reële cyberdreigingen. Volgens Dijkhoff zijn de bevindingen uit het CSBN 2016 zorgelijk: ‘Deze ontwikkelingen hebben consequenties voor heel Nederland. Digitale veiligheid is een randvoorwaarde voor het veilig functioneren van onze samenleving en belangrijk voor het vertrouwen in de economie. Via het Nationaal Detectie Netwerk informeren overheid en bedrijven elkaar over actuele dreigingen. Op deze digitale dijkbewaking ga ik de komende tijd extra inzetten. We moeten realistisch zijn: niemand kan op elk moment alles overzien. Daarom moeten overheid en samenleving samenwerken om onze online wereld veilig te houden. De basis is weten waar kwetsbaarheden zijn, die informatie delen en dan de boel dichten.'

Digitale spionage

Daarnaast is digitale spionage het afgelopen jaar toegenomen. Deze spionage is gericht op politieke en economische informatie. Dit vormt een belangrijke bedreiging voor de nationale veiligheid en concurrentiepositie van Nederland. De Nederlandse inlichtingen- en veiligheidsdiensten hebben bijvoorbeeld spionage waargenomen bij Nederlandse bedrijven binnen de defensie-industrie en de topsectoren.

Maatregelen om digitale veiligheid te versterken

Het kabinet heeft eerder al diverse maatregelen genomen om de digitale veiligheid van Nederland te versterken. Via het actieprogramma van de tweede Nationale Cyber Security Strategie zijn grote stappen gezet. Zo wordt de aanschaf van veilige software gestimuleerd. Publiekscampagnes zoals Alert Online vergroten het bewustzijn. Ook wordt geïnvesteerd in innovatie en onderwijs. Bovendien heeft Nederland het voortouw genomen tijdens het EU-voorzitterschap om cybersecurity internationaal op de agenda te zetten.

Dijkhoff: ‘Nederland heeft de kennis, kunde en capaciteiten om op dit moment op topniveau in het digitale domein te kunnen acteren. Toch zijn extra inspanningen noodzakelijk. Om de bedreigingen het hoofd te blijven bieden, moet Nederland de volgende stap zetten om in het digitale tijdperk mee te komen. Dat kan alleen als overheid en het bedrijfsleven samen optrekken. De samenleving verwacht dat ook.’

Hoe cybercrime de fysieke misdaad inhaalt

De grenzen tussen ‘gewone’ misdaad en cybercrime vervagen steeds meer. Sterker nog, over tien-twintig jaar zijn deze grenzen volledig verdwenen. Volgens recente statistieken zijn er nu 15 miljard aangesloten devices en dat worden er in 2020 maar liefst 200 miljard. Dat is een ongelooflijk grote hoeveelheid apparaten die gehackt kan worden en dit maakt ons steeds kwetsbaarder. Onze moderne wereld lijkt op een digitaal kaartenhuis, dat ieder moment in elkaar kan storten als we niet snel de juiste voorzorgsmaatregelen treffen. We hebben nu te maken met bedreigingen die tien jaar geleden volledig ondenkbaar waren. Ze vormen een gevaar voor het voortbestaan van de huidige maatschappij.

***Richard van Hooijdonk**, Trendwatcher en Futurist bij BNR Nieuwsradio en Nyenrode University*

Internet of Things wordt nu al onder vuur genomen

Je bent vast verbaasd hoe weinig mensen weten dat elk aangesloten apparaat te hacken is. De gamingconsole van je zoontje lijkt misschien een onschuldig apparaat, maar consoles zijn al eerder gehackt voor spionagedoeleinden. Ook DVR’s en koelkasten zijn in het verleden al gesaboteerd voor Bitcoin-mining, het installeren van spam en zelfs voor DDoS-aanvallen; allemaal via malware. Cybercriminelen richten zich op specifieke devices en ze gebruiken de kracht van het Internet of Things om deze misdaden makkelijk te kunnen plegen.

Cyberafpersing met ransomware

Afpersing is al zo oud als de wereld en het is nog steeds even effectief. Alle aspecten van ons leven zijn nu verbonden met online platforms. We hebben overal accounts; thuis en op het werk. Of het nu gaat om accounts op social media of online banking; we zijn kwetsbaarder voor afpersing dan ooit tevoren. Afpersing gaat allang niet meer alleen via griezelige telefoontjes waarin men losgeld eist. Iedereen kan tegenwoordig toegang krijgen tot jouw rekeningen en je afpersen. Deze cyberaanvallen worden ook wel ‘ransomware’ genoemd en vinden al plaats in Europa en de VS. Het virus dat gebruikt wordt voor deze aanvallen heet het ‘cryptolocker‘ virus. Cyberafpersing komt nog niet vaak voor, maar over tien tot vijftien jaar hebben we er net zo vaak mee te maken als met spam in onze mailbox. Omdat preventie niet altijd 100% effectief is, moeten bedrijven en organisaties ervoor zorgen dat ze een waterdicht actieplan hebben om cyberafpersing op te sporen en er korte metten mee te maken.

‘Brick attacks’ kunnen je hele bestaan uitwissen

We hebben allemaal weleens gehoord van gestolen creditcardgegevens, bankrekening-overnames en andere financiële fraude. Mischien ben je er zelf weleens slachtoffer van geweest. Dit zijn helaas niet de enige vormen van cybermisdaad waar je je zorgen over moet maken. Stel je voor dat je bankrekeningen volledig zouden worden gewist. Dit kan met de zogenaamde ‘brick attacks’. In plaats van dat je geld ‘gewoon’ gestolen wordt, laten hackers met een brick attack al jouw gegevens verdwijnen. Dit doen ze door de computers waarop jouw informatie is opgeslagen volledig te crashen. Hackers kunnen je firewall uitschakelen en je antivirusprogramma’s uitzetten door instellingen te veranderen. In 2012 werd ’s werelds grootste oliemaatschappij, Saudi Aramco, slachtoffer van een brick attack, waarbij maar liefst 3.000 computers uitgeschakeld werden. Soortgelijke aanvallen zijn al vaker voorgekomen. Stel je voor wat er gebeurt als hackers grote banken aanvallen met brick attacks en alle gegevens van hun cliënten uitwissen…

Het menselijk lichaam als doelwit voor cyberaanvallen

Niet alleen dingen worden gehackt – wij mensen worden ook steeds gemakkelijker het slachtoffer van cyberaanvallen. Je kunt je wel voorstellen wat er kan gebeuren met de honderdduizenden medische apparaten die op het Internet of Things zijn aangesloten. Denk aan insulinepompen, hartbewakingsapparatuur en infuussystemen. Als artsen online toegang hebben tot je hart, heeft je buurman dat in principe ook. Hackers kunnen deze apparaten helemaal overnemen en de medische privacy, fysieke integriteit en veiligheid van de patiënt in gevaar brengen. In de toekomst houden implantaten chronische aandoeningen in de gaten. Deze apparaten meten je vitale statistieken en de informatie wordt aan de arts doorgegeven. Omdat het gebruik van draadloze technologie voor medische hulpmiddelen steeds populairder wordt, kan elk medisch systeem of implantaat makkelijk gehackt worden. Uit een onderzoek van de Universiteit van Liverpool is gebleken dat het mogelijk is om computervirussen via wifi-routers te verspreiden. Dit vormt natuurlijk een groot risico voor patiënten met medische implantaten. Als een computervirus via een onbeveiligd draadloos netwerk verspreid kan worden, kan dat ook gebeuren met medische virussen. Alhoewel het risico van dit soort menselijke cyberaanvallen momenteel niet erg hoog is, moeten ziekenhuizen er wel voor zorgen dat ze een actief beveiligingsbeleid implementeren.

Met cyberkaping kun je een vliegtuig van de radar laten verdwijnen

Criminelen of terroristen die van plan zijn om een vliegtuig te kapen, kunnen dit op afstand doen door het vliegtuig te ‘cyberkapen’. Ze hoeven niet meer fysiek in het vliegtuig aanwezig te zijn om de piloot zijn koers te laten wijzigen en passagiers te gijzelen. Er wordt zelfs gespeculeerd dat vlucht 370 van Malaysian Airlines door cyberkaping is verdwenen. Cyberkapingen variëren van het wijzigen van vliegplannen tussen het vliegtuig en grondstations tot infiltratie van het vluchtmanagementsysteem. Een aanvaller kan ook een vals weeralarm afgeven of het systeem infecteren met een zogenaamd spookvliegtuig. Deze vervangt het eigenlijke vliegtuig zodat het letterlijk van de radar verdwijnt.

Wanneer cyberkapers de computer van het vliegtuig kapen, kunnen ze de besturing van het vliegtuig manipuleren en de koers veranderen. Ook kunnen ze het vliegtuig laten crashen door een ramkoers met een ander vliegtuig in te stellen.

Identiteitsdiefstal en het hacken van genetische data

Denk je dat identiteitsdiefstal een probleem is? Het kan nog veel erger. Biometrische beveiligingsmethoden als iris- en vingerafdrukscans en spraakherkenning worden nog niet veel toegepast. Zodra deze technieken op grotere schaal geïmplementeerd worden – om bijvoorbeeld online profielen als bankrekeningen te authenticeren, worden biometrische gegevens erg waardevol voor cybercriminelen. En dan hebben we het nog niet eens over genetische gegevens. Genetische testen worden om verschillende redenen gedaan; om genetische ziekten uit te sluiten of te bevestigen, om pasgeboren baby's te screenen of om te bepalen of je een goede spermadonor bent. Deze gegevens kunnen makkelijk door cybercriminelen gehackt worden en voor marketingdoeleinden gebruikt worden. Stel je voor dat aan jou gevraagd wordt of je een spermadonor wilt worden omdat je zulke goede genetische eigenschappen hebt. Of misschien vragen ze je of je wilt overwegen om bloeddonor te worden omdat je een zeldzame bloedgroep hebt. Bedrijven kunnen zelfs DNA-databanken kopen die tienduizenden genomen bevatten.

Conclusie

We worden steeds afhankelijker van de technologie en daardoor zijn we ook steeds kwetsbaarder voor cybercriminaliteit. Cybercriminelen kunnen op allerlei manieren toegang krijgen tot en gebruikmaken van onze persoonlijke informatie. Criminelen hoeven niet meer fysiek 'ter plaatse' te zijn of over wapens te beschikken. We moeten in de toekomst steeds waakzamer zijn en wel twee keer nadenken voordat we persoonlijke gegevens vrijgeven.

Cyber Security Event

Beveilig informatie tegen cybercrime en datalekken!

Voorkom imago- en reputatieschade!

Cybercrime en datalekken kost de Nederlandse overheid en het bedrijfsleven jaarlijks meer dan 10 miljard euro. Naast de financiële consequenties kan verlies, diefstal en misbruik van persoonlijke data, intellectueel eigendom en vertrouwelijke bedrijfsinformatie ook ernstige gevolgen hebben voor het imago en de reputatie van een organisatie.

Uit recente incidenten binnen de overheid en het bedrijfsleven blijkt keer op keer dat de bescherming van informatie, systemen en de productieomgeving tekortschiet. Uit onderzoek blijkt dat slechts één op de vijf organisaties haar beveiliging op orde heeft.

Bent u wel goed voorbereid?

Bekijk het programma