Ministerie van Veiligheid en Justitie

Cybersecuritybeeld Nederland

December 2011

< GOVCERT.NL >

GOVCERT.NL

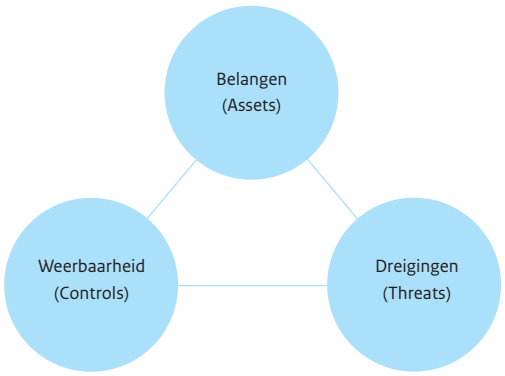
hét Cyber Security en Incident Response Team van de Nederlandse overheid, werkt aan de digitale veiligheid van Nederland door het voorkomen en afhandelen van ICT-veiligheidsincidenten.
Dagelijks geeft GOVCERT.NL waarschuwingen en adviezen aan overheidsorganisaties en organisaties met een publieke taak. GOVCERT.NL werkt daarbij nauw samen met nationale én internationale partners in het publieke en private domein.

Inhoudsopgave

Samenvatting

ICT is doorgedrongen tot in de haarvaten van onze maatschappij en haar functioneren is ervan afhankelijk geworden. ICT is echter feilbaar en kwetsbaar en de opgeslagen of uitgewisselde informatie, al dan niet in gemanipuleerde vorm, is waardevol. Er zijn tal van partijen die misbruik willen maken van die kwetsbaarheden of toegang willen krijgen tot informatie, eventueel met het doel om die te manipuleren of te publiceren. De beveiliging van informatie, systemen en netwerken – kortweg cybersecurity – is om die reden een onderwerp om serieus te nemen.

Vanwege het grote belang van cybersecurity is in 2011 een Nationale Cybersecuritystrategie geformuleerd. Een van de actielijnen die de strategie beschrijft, is de realisatie van adequate en actuele dreigings- en risicoanalyses. Het voor u liggende Cybersecuritybeeld Nederland is de eerste stap in de uitvoering van die actielijn.



Figuur 1. Componenten van een risico-analyse

Dit eerste Cybersecuritybeeld is primair gericht op het beschrijven van dreigingen in het ICT-domein voor de Nederlandse situatie. De nadruk ligt daarbij op moedwillig handelen en dus niet op dreigingen als gevolg van bijvoorbeeld menselijk falen. Het cybersecuritybeeld is geen volledige risico-analyse (zie figuur 1), omdat te beschermen belangen grotendeels buiten beschouwing blijven en weerbaarheid slechts in algemene zin wordt beschreven. Secundair in het beeld is de beschrijving van relevante actoren, hulpmiddelen en kwetsbaarheden. Het Cybersecuritybeeld Nederland is primair de basis voor het overwegen en nemen van maatregelen en is met nadruk niet bedoeld als uitputtende incidentrapportage.

Actoren

Een dreiging kan uitgaan van diverse typen actoren: statelijke actoren, private organisaties, terroristen, hacktivisten, scriptkiddies en beroepscriminelen. De grootste dreiging gaat in potentie uit van statelijke actoren. Zij beschikken het best over noodzakelijke capaciteiten. Ook van beroepscriminelen gaat een grote dreiging uit. Beroepscriminelen kunnen verschillende digitale aanvallen uitvoeren en veroorzaken het merendeel van alle cyberincidenten. Dit laat onverlet dat ook hacktivisten en scriptkiddies zich bezighouden met verstoring en misbruik van ICT. Terroristen gebruiken ICT vooral instrumenteel voor realisatie van hun doeleinden, zoals propaganda bedrijven en zieltjes winnen. Statelijke actoren, private organisaties en burgers vormen potentiële doelwitten voor dreigingen.

Dreigingen

De dreigingen zijn onderverdeeld in drie hoofdcategorieën: informatiegerelateerde dreigingen, systeemgerelateerde dreigingen en indirecte dreigingen. Binnen deze drie categorieën komt een aantal prominente dreigingen naar voren die grotendeels zijn ontleend aan ontwikkelingen en incidenten die tijdens de rapportageperiode (eind 2010 - 15 september 2010) hebben plaatsgevonden.

In tabel 1 wordt inzichtelijk welke dreigingen momenteel het ernstigst zijn, wie daarbij doelwit is, en dreigersgroep. Deze tabel is nadrukkelijk niet bedoeld om voor individuele gevallen te bepalen welke dreigersgroep verantwoordelijk is voor een incident. Daarvoor is uiteraard gericht onderzoek nodig.

Dreigersgroepen	Doelwitten		
	Overheid	Private organisaties	Burgers
Staten	Digitale Spionage en sabotage	Digitale spionage en sabotage	
Private organisaties		Digitale spionage	
Hacktivisten	Publicatie van vertrouwelijke gegevens en digitale verstoring	Publicatie van vertrouwelijke gegevens en digitale verstoring	Publicatie van vertrouwelijke gegevens
Terroristen	Sabotage	Sabotage	
Beroepscriminelen	Cybercrime (waaronder digitale (identiteits-) fraude) Neveneffect: verstoring door malwarebesmetting	Cybercrime (waaronder digitale (identiteits-) fraude) Neveneffect: verstoring door malwarebesmetting	Cybercrime (waaronder digitale (identiteits-) fraude)
Scriptkiddies	Digitale verstoring	Digitale verstoring	

(legenda bij tabel)

Kleur	Betekenis
	Hoog
	Middel
	Laag
	N.v.t of onbekend

Tabel 1. Dreigingsoverzicht naar dreigersgroep en doelwit

De dreiging van vreemde mogendheden gaat voornamelijk uit naar de Nederlandse overheid en multinationals en momenteel in mindere mate naar organisaties in de vitale infrastructuur. Relevant, maar qua omvang zeer klein is de dreiging die van vreemde mogendheden uitgaat naar onderdanen die zich in Nederland bevinden. Over de dreiging die direct uitgaat van private organisaties is weinig bekend. Overlap met de dreiging vanuit staten is hier mogelijk, omdat moeilijk is vast te stellen wie achter een aanval zit.

Beroepscriminelen richtten zich traditioneel voornamelijk op het bedrijfsleven, en dan veelal op de financiële sector. Daarbij wordt veelal diefstal gepleegd door middel van identiteitsfraude, waarbij bestaande identiteiten van burgers in het spel zijn. Er zijn daarnaast aanwijzingen dat nu, met de groei van e-overheidsdiensten, ook de overheid een interessanter doelwit vormt voor beroepscriminelen. De hulpmiddelen die beroepscriminelen gebruiken, met name malware, zijn gemaakt om zichzelf op grote schaal te verspreiden en besmetting te veroorzaken, wat zowel voor overheid als bedrijfsleven een belangrijke indirecte dreiging is. Tenslotte is de dreiging die vanuit beroepscriminelen uitgaat naar burgers aanzienlijk. Het gaat om onder andere identiteits-fraude en om andere typen van fraude, die weliswaar in individuele gevallen vaak relatief beperkt zijn van omvang, maar waar het wel om een aanzienlijk aantal gevallen gaat.
De dreiging die uitgaat van de groep hacktivisten is klein, maar groeiend. Hacktivisten kiezen hun doelwitten vrij onvoorspelbaar en ongeacht of het doelwit publiek of privaat is, zijn daarbij vrijwel altijd persoonsgegevens in het spel.
Terroristen hebben weliswaar de intentie om grootschalige verstoring of ontwrichting te veroorzaken, maar vooralsnog zijn er geen aanwijzingen dat zij de capaciteiten hebben, en dat deze dreiging heel groot is.
Scriptkiddies, ten slotte, vormen nauwelijks een serieuze bedreiging voor de drie genoemde doelwitten, maar richten zich, met hun beperkte middelen, voornamelijk op overheid en private organisaties.

Informatiegerelateerde dreigingen

Informatiegerelateerde dreigingen ontstaan als dreigersgroepen de intentie hebben om informatie te verzamelen, te manipuleren, te publiceren of te misbruiken.

Digitale spionage

Zowel overheden als private organisaties kunnen doelwit zijn voor digitale spionage. Tijdens de afgelopen periode is gebleken dat sprake is van een toenemende dreiging van digitale spionage. Overheden zijn namelijk regelmatig doelwit van digitale spionage geweest, ook in Nederland. Deze cyberaanvallen zijn gericht op het verkrijgen van vertrouwelijke informatie van economische of politieke waarde, of op direct geldelijk gewin.

Een opvallende vorm van digitale spionage in de private sector uit de rapportageperiode is spionage toegespitst op beveiligingsbedrijven, met aanvallen die als een *stepping stone* fungeerden. Daarbij is informatie buit gemaakt die kan worden ingezet bij latere aanvallen op derde partijen. DigiNotar is hier een voorbeeld van geweest. Vervolgaanvallen hebben ook daadwerkelijk plaatsgevonden.
Beveiligingsproducten zijn hiermee niet langer slechts een middel ter verdediging, maar ook een aanvals-instrument. Omdat deze producten juist gebruikt worden voor beveiliging van vertrouwelijke informatie, kunnen de gevolgen hiervan groot zijn.

Publicatie van persoonsgegevens en gevoelige informatie
Tijdens de rapportageperiode zijn tal van incidenten bekend geworden waarbij op illegale wijze toegang is verkregen tot digitale persoonsgerelateerde en/of gevoelige informatie. In sommige gevallen is die informatie gepubliceerd, waardoor deze gegevens op straat zijn gekomen. Zo is HBGary, het bedrijf dat Anonymous wilde ontmaskeren, slachtoffer geworden van een gerichte aanval, waarbij veel vertrouwelijke bedrijfsinformatie is buit gemaakt en vervolgens geopenbaard. Organisaties die zich inzetten voor bestrijding van cybercrime, blijken hiermee meer en meer zelf een doelwit te worden. Daarnaast worden ook burgers getroffen aangezien hun persoonsgegevens geopenbaard worden. Voorbeelden hiervan uit de afgelopen periode zijn het lekken van alle e-mailadressen en wachtwoorden van leden van datingsite Pepper.nl en van abonnees van het Sony Playstation Network.

Digitale identiteitsfraude
Digitale identiteitsfraude is een toenemende dreiging. Door het versturen van phishing e-mailberichten uit naam van publieke en private instellingen, en het inbreken in databanken van bedrijven – zoals het Sony Playstation Network en marketing firma Epsilon – vergaren aanvallers waardevolle persoonsgegevens. Hiermee zijn zij vervolgens in staat om zich voor te doen als een ander om daarmee financieel gewin te behalen. Zwakke authenticatiemiddelen, kwetsbaarheden in websites en het gsm-protocol, en de ontwikkeling van malware voor mobiele platformen zorgen voor een toename van de kwetsbaarheid voor deze dreiging.

Systeemgerelateerde dreigingen
Systeemgerelateerde dreigingen ontstaan als dreigersgroepen de intentie hebben om de dienstverlening of de bedrijfsvoering van een organisatie te verstoren of te onderbreken.

Gerichte verstoring van vitale infrastructuur
Hoewel ook onderdelen van de vitale infrastructuur al langer last hadden van algemene en ongerichte aanvallen op de eigen systemen, werd in 2010 de eerste gerichte aanval met behulp van malware op industriële controlesystemen (ICS) bekend: Stuxnet. Doordat Stuxnet beschikbaar is op het internet en wordt nagebouwd, kunnen uiteindelijk kwaadwillenden op Stuxnet gebaseerde varianten ontwikkelen om ook ICS van andere (vitale) processen te manipuleren. Daarvoor is overigens wel diepgaande kennis nodig van het proces dat men wil beïnvloeden. In combinatie met de toename van gepubliceerde kwetsbaarheden in ICS en de wijze waarop de kwetsbaarheden worden gepubliceerd, vergroot Stuxnet de waarschijnlijkheid van gerichte cyberaanvallen op ICS en daarmee de vitale infrastructuur die daarmee bestuurd wordt. Voor de ontwikkeling van Stuxnet waren aanzienlijke kennis en middelen nodig. Hoewel Stuxnet geen directe dreiging is voor Nederland, kan inmiddels bekendgemaakte software en kennis daarover wel misbruikt of gebruikt worden om soortgelijke aanvallen op andere ICS uit te voeren.

Verstoring van (online)dienstverlening
Uiteenlopende instanties en bedrijven zijn de afgelopen periode het slachtoffer geworden van digitale aanvallen, waarbij de aanvallers handelden uit ideologische motivatie. Dit was het geval tijdens de WikiLeaks-affaire. Sympathisanten van WikiLeaks (Anonymous) hebben toen bijvoorbeeld de websites van Paypal en Mastercard, bedrijven die stopten betalingstransacties van WikiLeaks te verwerken, met een DoS-aanval onder vuur genomen.

Indirecte dreigingen
Deze categorie bevat dreigingen voor cybersecurity, die feitelijk neveneffecten zijn van de hierboven beschreven directe dreigingen.

Verstoring van bedrijfsvoering door malwarebesmetting

Verstoring van de bedrijfsvoering als gevolg van malwarebesmetting is een van de belangrijkste dreigingen voor zowel overheid als bedrijfsleven op dit moment. Het gaat om 'ongerichte' malware, die zichzelf zo veel mogelijk wil verspreiden. Besmettingen kunnen in sommige gevallen zelfs (delen van) een bedrijfsnetwerk onderuithalen. Het opschonen van malwarebesmettingen kan erg kostbaar zijn voor een organisatie, zowel in directe kosten voor het schoonmaken als in indirecte kosten als gevolg van verloren productiviteit.

Verstoring van bedrijfsvoering door aanval bij een derde partij

Een geslaagde aanval op beveiligingsbedrijven kan ingrijpende gevolgen hebben voor de bedrijfsvoering van derden waartegen de aanval niet gericht is. Deze dreiging is vooral in het afgelopen jaar gegroeid. De aanvallen op DigiNotar en RSA, een beveiligingsbedrijf dat onder andere authenticatietokens levert, hebben laten zien wat de effecten kunnen zijn: partijen die gebruikmaakten van de producten van deze leveranciers hebben deze producten, als gevolg van de aanvallen, binnen hun eigen organisatie moeten vervangen.

Verstoring van dienstverlening door aanval bij een derde partij

Verstoring van online dienstverlening is een concrete dreiging voor partijen in Nederland. Aanvallen die bedoeld zijn om verstoring te veroorzaken (DoS-aanvallen), zijn vaak grove aanvallen, waarbij niet alleen de dienst van het primaire doelwit wordt geraakt maar ook diensten van derden die toevallig 'in de buurt staan', bijvoorbeeld ondergebracht bij dezelfde partij.

Hulpmiddelen

De belangrijkste technische hulpmiddelen die actoren inzetten, zijn exploits, malware en botnets. Exploits zijn manieren om misbruik te maken van een kwetsbaarheid. Kwetsbaarheden in standaardsoftware zijn door voor-uitgang in de informatiebeveiliging steeds moeilijker te misbruiken, waardoor het ontwikkelen van exploits een expertise is geworden. Malware, ofwel kwaadaardige software, ligt vaak ten grondslag aan een aanval. Dit komt grotendeels doordat malware voor diverse doeleinden ingezet kan worden, waardoor het een toepasselijk aanvalsinstrument is voor verschillende actoren. Daarnaast onderhouden kwaadwillenden al jarenlang botnets – netwerken van gekaapte computers – om cyberaanvallen te plegen of te faciliteren. Met een gewijzigde aanpak zijn recent met succes enkele botnets ontmanteld, waarbij Nederland een voortrekkersrol heeft vervuld zoals in het geval van het Bredolab-botnet. Desondanks blijft het bestrijden van botnets erg lastig. Botnets hebben en houden een spilfunctie bij het uitvoeren van cyberaanvallen.

Kwetsbaarheden

Menselijke en organisatorische factoren

Onvoldoende aandacht voor beveiliging

Goede beveiliging van informatie is voor vrijwel elke organisatie van direct belang voor de bedrijfsvoering. Het beeld dat nu vooral ontstaat, is dat sommige organisaties, zowel dienstaanbieders als afnemers, pas actie ondernemen als gesignaleerde kwetsbaarheden media-aandacht ontvangen. Voorbeelden hiervan zijn de beveiliging van voicemailboxen tegen caller-ID spoofing en lekke websites waarover geschreven werd in het kader van Lektober. Dit geeft over het geheel een beeld weer van onvoldoende aandacht voor informatiebeveiliging. Dit beeld is in sommige gevallen herkenbaar, maar zeker niet algemeen van toepassing – organisaties die het wel goed doen, en incidenten die niet gebeuren, halen nooit het nieuws.

Onvoldoende herijking van verouderde versleutelingstechnieken

Versleutelingstechnieken, zoals die in de ov-chipkaart en gsm, spelen een belangrijke rol bij het garanderen van de integriteit en vertrouwelijkheid van waardevolle informatie en financiële transacties. Organisaties die deze technieken inzetten, houden vaak onvoldoende rekening met de veroudering ervan. Als gevolg van die veroudering moeten de technieken na verloop van tijd vervangen worden om misbruik, zoals manipulatie van gegevens, te voorkomen. De versleuteling in het huidige gsm-protocol is sterk verouderd en daar een voorbeeld van.

Gedetailleerde vastlegging en verwerking van privacygevoelige informatie

De overheid en het bedrijfsleven registreren veel persoonsgegevens en burgers delen vrijwillig veel persoonlijke informatie via onder andere sociale netwerken. Steeds meer privacygevoelige informatie wordt op gedetailleerde wijze vastgelegd in profielen, maar ook gekoppeld aan andere gegevens. Die gedetailleerde vastlegging maakt degene van wie de informatie is, kwetsbaar voor kwaadwillig of ongewenst gebruik of ongewenste publicatie van de informatie.

Technische factoren

Kwetsbaarheden in websites en standaardsoftware

Websites blijken vaak slecht beveiligd te zijn en best practices worden vaak niet gevolgd: 80% is vatbaar voor een of meer van de tien grootste beveiligingsrisico's. Doordat overheden, burgers en bedrijven via websites meer en meer gegevens uitwisselen en websites een steeds grotere rol spelen bij uiteenlopende soorten transacties, zijn deze kwetsbaarheden voor kwaadwillenden steeds aantrekkelijker (zie verder onder dreigingen).
De beveiliging van websites blijkt regelmatig niet op het niveau te zijn dat past bij het belang van de informatie die erop wordt verwerkt. In oktober 2011 werd dit nogmaals op indringende wijze duidelijk met de publicatie van meerdere lekken in websites, in het kader van 'Lektober'.

Onthullingen van kwetsbaarheden in industriële systemen

In de eerste helft van 2011 is een aanzienlijk aantal kwetsbaarheden bekendgemaakt in software voor ICS, veelal in gebruik in vitale sectoren. In sommige gevallen is ook bekendgemaakt hoe die kwetsbaarheden misbruikt kunnen worden. In meerdere gevallen gebeurde de onthulling zonder afstemming met de leverancier van het betreffende product, waardoor oplossingen nog niet beschikbaar waren op het moment van bekendmaking. Dergelijke onthullingen bieden aanvallers meer mogelijkheden om ICS aan te vallen.

Kwetsbaarheden in het PKI-stelsel

De effecten van het DigiNotar-incident in Nederland en in de rest van de wereld zijn een gevolg van de wijze waarop het wereldwijde certificatensysteem werkt. Het certificatensysteem is bedoeld om (onder andere) de identiteit van websites te kunnen vaststellen en elektronische handtekeningen te kunnen zetten.
Alle certificaatuitgevers krijgen echter evenveel vertrouwen en elke certificaatuitgever kan voor elk willekeurig domein certificaten uitgeven. Als een certificaatuitgever onbetrouwbaar of slecht beveiligd is, kan dit grote gevolgen hebben. Communicatie kan gemanipuleerd of afgeluisterd worden, waarvoor overigens nog wel manipulatie van de communicatiestromen nodig is. Structureel verhelpen van deze kwetsbaarheid is niet eenvoudig en vereist wereldwijd een wijziging van het certificatensysteem. Een alternatief is om tekortkomingen van het systeem te accepteren en op andere wijze de impact van incidenten te verkleinen.

Kwetsbaarheden in routeringprotocollen

De afgelopen jaren is er veel aandacht geweest voor kwetsbaarheden in protocollen (de talen die computers met elkaar spreken), die van fundamenteel belang zijn voor een goede werking van het internet: DNS en BGP. Deze protocollen (BGP en DNS) zorgen ervoor dat computers elkaar op internet op een zo efficiënt mogelijke manier weten te vinden. Succesvolle uitbuiting van de daarin ontdekte kwetsbaarheden zou ertoe kunnen leiden dat het netwerkverkeer tussen computers wordt omgeleid, afgeluisterd of gemanipuleerd. De kwetsbaarheden zijn ernstig, vooral omdat ze door het fundamentele karakter van de protocollen raken aan de basis van het internet. De gevolgen ervan kunnen dan ook groot zijn.

Kwetsbaarheden gerelateerd aan het nieuwe internetprotocol IPv6

De noodzaak voor migratie naar het nieuwe internetprotocol IPv6 neemt steeds verder toe. Dit nieuwe protocol lost een aantal problemen op, waaronder het tekort aan IP-adressen. Maar het brengt ook nieuwe kwetsbaarheden met zich mee. Zo bevat software die hiervan gebruikmaakt, net als alle andere software, fouten. Veel organisaties hebben nog onvoldoende kennis om een IPv6-infrastructuur goed te ontwerpen en te configureren, waardoor systemen ongewenst kunnen worden blootgesteld aan aanvallen van buitenaf. Veel organisaties zijn dus nog niet klaar voor IPv6 en de bijbehorende beveiligingsrisico's.

Nieuwe ontwikkelingen

Vermindering van beheersbaarheid bij uitbesteding van diensten in de cloud

Het uitbesteden of het 'naar de cloud brengen' van bedrijfsprocessen of -informatie introduceert nieuwe risico's bij een organisatie. Bij uitbesteding van diensten of taken kan de verantwoordelijkheid voor informatiebeveiliging nooit uitbesteed worden. Toch heeft de klant bij cloudcomputing vrijwel geen controle over of kennis van de exacte locatie van de ICT, die zich soms in het buitenland bevindt of met anderen wordt gedeeld. Het is daardoor moeilijk te overzien of voor de bedrijfsinformatie wordt voldaan aan de privacy- en vertrouwelijkheidseisen en welk juridisch regime geldt voor incidenten of voor terbeschikkingstelling van data aan overheidsdiensten ter plaatse. Specifieke eisen aan beveiliging en beheer van standaard clouddiensten zijn, door de grote mate van generalisatie, nauwelijks te stellen. De mate van besturing is dan voor de individuele opdrachtgever minder groot.

Groei van mobiliteit maakt misbruik aantrekkelijker

De penetratiegraad van mobiele apparatuur is hoog en blijft toenemen. Mobiele apparatuur is een aantrekkelijk doelwit voor aanvallers: ze zijn vrijwel altijd online, bieden toegang tot een schat aan persoonlijke informatie, bieden mogelijkheden tot het afnemen van diensten en uitvoeren van financiële transacties en zijn vaak slechts in beperkte mate beveiligd. Hoewel het aantal bekende malware-varianten toeneemt, zijn er momenteel slechts enkele honderden stuks malware voor mobiele platformen ten opzichte van honderdduizenden voor desktopplatformen. De verwachting is wel dat serieuze aanvallen gericht op mobiele apparatuur de komende jaren sterk zullen toenemen, zeker als financiële instellingen met nieuwe diensten hiervoor komen.

1

> Inleiding

> 1.1 Context

ICT is doorgedrongen tot in de haarvaten van onze maatschappij en haar functioneren is ervan afhankelijk geworden. Onze maatschappij in de breedste zin van het woord drijft immers op ICT. Steeds meer gebruiksvoorwerpen bevatten elektronica en software, en steeds vaker zijn ze verbonden met het internet en daarmee onderdeel van cyberspace. Die digitalisering en verbinding is zo doorgevoerd, dat we het ons vaak niet eens meer realiseren. Kantoren, huishoudens, fabrieken en winkels zijn allemaal onderdeel van deze ontwikkeling. ICT is een belangrijke drijfveer voor innovatie en vernieuwing, en in veel gevallen een voorwaarde voor succesvol ondernemen. De positieve invloed van ICT op ons leven is over het algemeen duidelijk: voorbeelden te over van manieren waarop ICT het leven gemakkelijker maakt. Maar de keerzijde is niet altijd even duidelijk: ICT is immers feilbaar en kwetsbaar, en de opgeslagen of uitgewisselde informatie, al dan niet in gemanipuleerde vorm, is waardevol. Er zijn tal van partijen die misbruik willen maken van die kwetsbaarheden of toegang willen krijgen tot informatie, soms met als doel die te manipuleren of te publiceren. De beveiliging van informatie, systemen en netwerken is om die reden een onderwerp om serieus te nemen.

Een recent incident met DigiNotar is in het bijzonder voor Nederland een indringend voorbeeld geweest dat ICT kwetsbaar is, dat van ICT misbruik kan worden gemaakt en dat onze samenleving inmiddels heel afhankelijk is van goed functionerende ICT. Eind augustus werd bekend dat er een hack bij beveiligingscertificatenuitgever DigiNotar had plaatsgevonden. Bij de inbraak waren frauduleuze certificaten aangemaakt. Er is geconstateerd dat een van de frauduleuze certificaten, het certificaat voor google.com, in Iran in omloop was en daar mogelijk gebruikt is om vertrouwelijke communicatie van bezoekers van Google af te luisteren. Als gevolg van de inbraak werd het vertrouwen in alle certificaten, uitgegeven door DigiNotar, opgezegd. Verschillende partijen, waaronder overheidsinstanties, werden hierdoor geraakt en hun elektronische dienstverlening en bedrijfsvoering verstoord. In sommige gevallen was het zelfs noodzakelijk om volledig terug te vallen op niet-digitale middelen, zoals papier en fax. Inmiddels zijn de certificaten met grote inspanning van velen vervangen.

Vanwege het grote belang van cybersecurity is in 2011 een Nationale Cybersecuritystrategie geformuleerd. Deze strategie heeft het belang van cybersecurity voor de Nederlandse samenleving verankerd. Cybersecurity is daarin als volgt gedefinieerd:

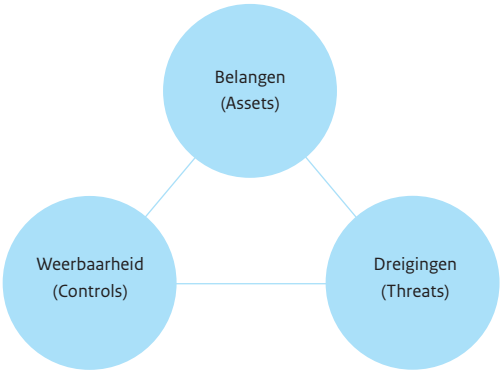
> *Cybersecurity is het vrij zijn van gevaar of schade veroorzaakt door verstoring of uitval van ICT of door misbruik van ICT. Het gevaar of de schade door misbruik, verstoring of uitval kan bestaan uit beperking van de beschikbaarheid en betrouwbaarheid van de ICT, schending van de vertrouwelijkheid van in ICT opgeslagen informatie of schade aan de integriteit van die informatie.*[1]

De Cybersecuritystrategie heeft tot doel: 'het versterken van de veiligheid van de digitale samenleving om daarmee het vertrouwen in het gebruik van ICT door burger, bedrijfsleven en overheid te verhogen'. Een van de actielijnen die de strategie beschrijft, is de realisatie van adequate en actuele dreigings- en risicoanalyses. Preventie en bestrijding van cyberaanvallen vereisen namelijk een overzicht van en inzicht in ontwikkelingen en incidenten die zich voordoen. Dat is nodig om de juiste koers te bepalen voor (nieuwe) maatregelen. Het voor u liggende Cybersecuritybeeld Nederland is de eerste stap in de uitvoering van die actielijn middels het geven van een periodiek overzicht van en inzicht in dreigingen.

[1] Nationale Cyber Security Strategie (2011).

> 1.2 Cybersecuritybeeld Nederland

Dit Cybersecuritybeeld is primair gericht op het beschrijven van dreigingen in het ICT-domein voor de Nederlandse situatie. De nadruk ligt daarbij op moedwillig handelen en dus niet op dreigingen als gevolg van bijvoor-beeld menselijk falen. Het is geen volledige risico-analyse (zie figuur 2), omdat te beschermen belangen grotendeels buiten beschouwing blijven en weerbaarheid slechts in algemene zin wordt beschreven. Secundair in het beeld is de beschrijving van relevante actoren, hulpmiddelen en kwetsbaar-heden. Het Cybersecuritybeeld Nederland is primair de basis voor het overwegen en nemen van maatregelen.



Figuur 2. Componenten van een risico-analyse

Het Cybersecuritybeeld Nederland heeft een rapportageperiode die aansluit bij het Nationaal Trendrapport Cybercrime en Digitale Veiligheid 2010 (hierna: trendrapport) dat in november 2010 is gepubliceerd.[2] Het Cybersecuritybeeld Nederland beslaat in principe de periode eind 2010 tot 15 september 2011. Gebeurtenissen tot en met 30 september 2011 zijn, waar relevant, meegenomen in de analyse. Het Cybersecuritybeeld is met nadruk niet bedoeld als uitputtende incidentrapportage.

Het Cybersecuritybeeld Nederland bouwt voort op eerdere publicaties zoals het trendrapport en de trendpublicaties van GOVCERT.NL en het KLPD van voorgaande jaren. Het Cybersecuritybeeld Nederland geeft inzicht in de problematiek van cyber security en maakt daarbij onderscheid tussen verschillende vormen van dreigingen op het terrein van cyber security. Het doet dit door het bundelen van de inzichten waarover AIVD, MIVD, KLPD, KPN, NCTb en GOVCERT.NL op basis van hun taak beschikken en met de kennis die met hen is gedeeld door de private partijen waarmee zij samenwerken. Het Cybersecuritybeeld Nederland is opgesteld door GOVCERT.NL, het Cyber Security & Incident Response Team van de Nederlandse overheid.

Onderzoek naar de omvang van digitale criminaliteit en digitale aanvallen staat internationaal nog in de kinderschoenen. Het is van belang om meer zicht te krijgen op risico's en incidenten in het digitale domein. Hoewel er binnen de vertrouwde publiek-private netwerken dreigingsinformatie wordt gedeeld, zijn de getroffen organisaties en bedrijven in Nederland, maar ook in andere landen, nog terughoudend met het delen van informatie over incidenten. Een soortgelijke uitdaging is er voor de internationale samenwerkingsverbanden, bijvoorbeeld binnen de Europese Unie, waarin het delen van informatie van essentieel belang is, gezien het internationale karakter van cybercrime.

> 1.3 Opbouw

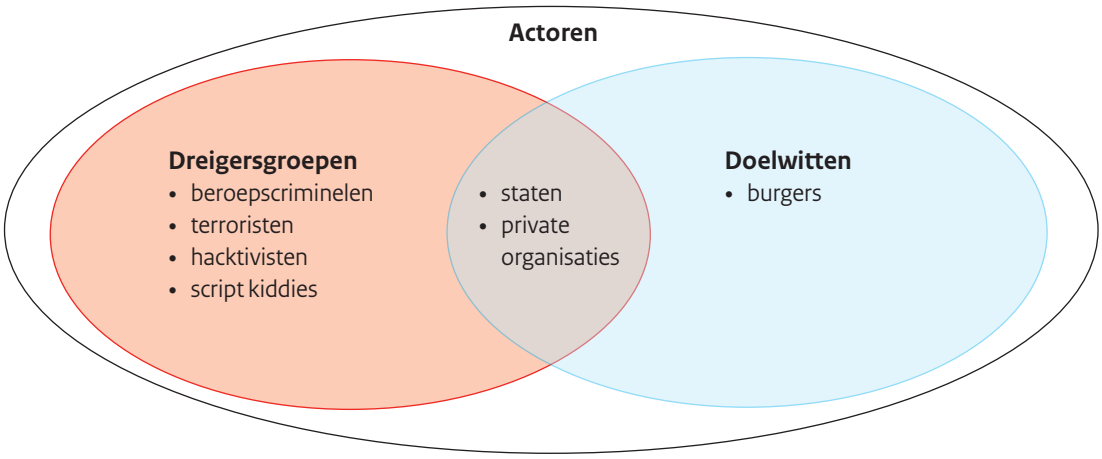
Het Cybersecuritybeeld begint in hoofdstuk 2 met een verkenning van het speelveld door een beschrijving te geven van alle relevante actoren en hun onderlinge verhoudingen. Hoofdstuk 3 beschrijft de meest relevante dreigingen van dit moment, onderverdeeld in drie hoofdcategorieën: informatiegerelateerde dreigingen, systeemgerelateerde dreigingen en indirecte dreigingen. Vervolgens geeft hoofdstuk 4 inzicht in de belangrijkste technische hulmiddelen die dreigersgroepen inzetten en beschrijft hoofdstuk 5 relevante factoren die ertoe bijdragen dat overheid, bedrijfsleven, vitale sectoren of burgers kwetsbaar zijn voor de drie typen dreigingen.

[2] GOVCERT.NL (2010a).

2

> Actoren

Dit hoofdstuk bevat een beschrijving van de actoren op het gebied van cybersecurity. Voor het cybersecuritybeeld worden zeven actoren beschreven. De term actor is in het kader van het document neutraal; actoren kunnen kwaadaardige intenties hebben, maar kunnen ook doelwitten zijn. Drie doelwitten zijn voor dit document van belang: de staat, private organisaties en burgers. Staten, private organisaties en burgers kunnen ook als dreigersgroepen zijn, waarbij we burgers verder onderverdelen naar veronderstelde intentie. In figuur 3 is te zien hoe de actoren zich tot elkaar verhouden.



Figuur 3. Relatie tussen actoren

Het ontwikkelen van een model dat alle actoren goed weergeeft, blijft een uitdaging. Omdat de dreigersgroepen op intentie zijn ingedeeld, is het goed denkbaar dat een persoon of groep in meerdere dreigersgroepen past. Terroristen hebben bijvoorbeeld de intentie om angst te zaaien. Zij zouden hierbij, hoewel we dit nog niet hebben gezien, het internet als wapen kunnen inzetten. Tegelijkertijd kunnen terroristen het internet gebruiken voor het uitdragen van een ideologie. Bepaalde gedragingen zouden in dat kader onder de noemer 'hacktivisten' kunnen vallen. Een tweede aandachtspunt is dat verschillende dreigersgroepen kunnen samenwerken of elkaar kunnen beïnvloeden. Een voorbeeld waarbij een gezamenlijke dreiging uitgaat van hacktivisten en scriptkiddies, wordt beschreven in paragraaf 2.4.

Er zijn regelmatig beveiligingsonderzoekers die, met veronderstelde goede intentie, lekken publiceren in software, in websites of in de beveiliging van organisaties. In de security community is de consensus dat dit de beveiliging van de betreffende software of organisatie ten goede kan komen, mits de onderzoekers de lekken op een verantwoorde wijze onthullen. Deze manier van werken wordt in de security gemeenschap responsible disclosure genoemd. Voorwaarden hiervoor zijn het aantonen van het lek in concept zonder dat daarbij daadwerkelijk inzage van gegevens plaatsvindt, en het inlichten van de verantwoordelijke organisatie voorafgaand aan het publiceren van het lek. De organisatie hoort daarbij een realistische termijn te krijgen om zelf maatregelen te nemen, voordat tot publicatie wordt overgegaan.

Dergelijke beveiligingsonderzoekers (ook wel ethical hackers of white hat hackers genoemd) en academische onderzoekers maken niet deel uit van het model in figuur 1 omdat zij noch dreigersgroep, noch doelwit zijn. Relevant zijn ze wel: de informatie die ze leveren kan een belangrijke bijdrage zijn voor de verbetering van informatiebeveiliging.

> 2.1 Staten

Als actor binnen het digitale speelveld kunnen staten zowel dader als doelwit zijn. Wanneer zij optreden als dader, kan dit zijn met de intentie om hun geopolitieke of economische positie te verbeteren of om bijvoorbeeld burgers af te luisteren. Hiervoor hebben zij ruime toegang tot benodigde capaciteiten. Zij houden zich van alle actoren dan ook bezig met het breedste palet van digitale aanvallen. De grootste dreiging die voor Nederland momenteel van vreemde mogendheden uitgaat, is de dreiging van digitale spionage, vooral gericht op de overheid, het bedrijfsleven en de academische sector in Nederland.

Advanced Persistent Threat (APT) is een term die de afgelopen jaren in zwang is geraakt. De dreiging is echter niet nieuw: het gaat om een voortdurende, geavanceerde en gerichte dreiging. Dat de dreiging geavanceerd wordt genoemd betekent dat de aanvaller de mogelijkheid heeft om geavanceerde aanvallen uit te voeren, maar betekent niet dat ook elke aanval op zichzelf geavanceerd is. De aanvaller heeft een specifiek doel en dat doel kan te bereiken zijn met een simpele aanval. Mocht dat niet het geval zijn, dan zal de vasthoudende aanvaller geavanceerdere aanvallen inzetten. De term APT zegt dus iets over de karakteristieken van een aanvaller, maar niks over wie de aanvaller precies is. Gezien de kenmerken van de aanvaller wordt over het algemeen gedacht aan statelijke actoren.

> 2.2 Private organisaties

Private organisaties gebruiken we in het kader van dit document als overkoepelende term voor onder andere bedrijven en NGO's. Net zoals bij staten, kunnen ook private organisaties zowel dreigersgroep als doelwit zijn. Zo kunnen private organisaties digitale spionage plegen om vertrouwelijke informatie te bemachtigen, terwijl zij tegelijkertijd daar ook doelwit van kunnen worden. Hier kunnen grote organisaties de middelen voor hebben, maar waarschijnlijker is dat ze kennis inhuren uit de groep beroepscriminelen. Daarnaast heeft deze gehele groep er belang bij inzicht te hebben in hun klanten en/of markt. Dit kan leiden tot privacyinbreuken.

> 2.3 Burgers

Burgers kunnen zowel de rol van doelwit als de rol van dreigersgroep vervullen, bijvoorbeeld als hacktivist. In deze rapportage gaat het om de rol als doelwit.

> 2.4 Hacktivisten

Hacktivisten zijn personen die een bepaalde ideologie aanhangen en digitale middelen inzetten voor hun 'zaak'. Een bekend voorbeeld zijn de groeperingen die op grote schaal de inhoud van websites aanpasten met religieuze boodschappen. De kunde van hacktivisten hoeft niet per se heel groot te zijn, maar de effecten van hun daden kunnen aanzienlijk zijn.
De dreigersgroep hacktivisten is recent behoorlijk in beweging geweest, als gevolg van de opkomst van Anonymous en LulzSec. Zo was Anonymous eind 2010 heel actief met DoS-aanvallen tegen organisaties die door hen als 'fout' werden gezien als gevolg van hun rol in de Wikileaks-affaire. Hierbij is op te merken dat de DoS-aanvallen in het kader van Wikileaks toe te schrijven zijn aan een combinatie van hacktivisten en scriptkiddies, waarbij de hacktivisten vooral doelwit en middelen kozen, en de scriptkiddies (sympathisanten) hun computer beschikbaar stelden om de aanvallen mee te helpen uitvoeren. De huidige trend is dat men vooral kwetsbare webservers aanvalt, gegevens buit maakt en deze vervolgens publiek maakt via sites als pastebin.com.
LulzSec is een hackersgroepering die in tegenstelling tot Anonymous minder politiek gemotiveerd is en zich meer lijkt te richten op spraakmakende hacks. In sommige gevallen trekken beide groeperingen gelijk op, bijvoorbeeld tijdens hacks in het kader van 'antisec': een golf van aanvallen tegen beveiligingsbedrijven, opsporings- en andere overheidsinstanties. Slachtoffers waren onder meer Scotland Yard, verschillende Amerikaanse politiekorpsen, de NATO en de Italiaanse High Tech Crime Unit.

De acties van Anonymous en LulzSec lijken andere hackers en hackersgroeperingen te inspireren of juist tegen de borst te stuiten. Een hackersgroepering die ook actief werd, was antisec_nl. Deze groep was verantwoordelijk voor het hacken van de Nederlandse datingsite Pepper.nl en het lekken van grote hoeveelheden abonnee-gegevens. Het Team High Tech Crime van het KLPD heeft in het kader van deze hack enkele arrestaties verricht.

> 2.5 Scriptkiddies

Scriptkiddies handelen vooral vanuit een baldadige motivatie en een behoefte aan een kick. Het zijn personen die met een minimum aan kennis maar enige interesse voor hacken en malware voor schade kunnen zorgen. Door gebrekkige kennis zijn scriptkiddies grotendeels afhankelijk van bestaande hulpmiddelen om hun activiteiten uit te voeren. Deze groep vormt op zichzelf geen grote dreiging. Deze groep is mogelijk wel te mobiliseren door hacktivisten en eventueel ook in te zetten door andere partijen.

> 2.6 Beroepscriminelen

Voor beroepscriminelen is financieel gewin het primaire doel van hun activiteiten. Hiermee onderscheiden zij zich van andere aanvallers, zoals hacktivisten en scriptkiddies, die ook illegale activiteiten uitvoeren. Criminelen als dreigersgroep vertegenwoordigen een divers geheel omdat het een spectrum bekleedt van kruimeldieven tot innovators, die zich meer bezighouden met hightechcrime op basis van innovatieve methoden. De potentie van professionele criminelen moet op veel vlakken (bijna) gelijk aan die van statelijke actoren geacht worden.

> 2.7 Terroristen

Terroristen lijken vooral de digitale arena te kunnen (en willen) misbruiken voor propaganda, communicatie en informatievergaring (bijvoorbeeld over middelen om een aanslag te plegen). In deze zijn digitale mogelijkheden een ondersteuning voor het voorbereiden van aanvallen door terroristen. Daarnaast is het voorstelbaar dat een terrorist het internet zou willen gebruiken (als wapen) om grootschalige verstoring of ontwrichting te veroorzaken. Vooralsnog zijn er geen aanwijzingen dat deze dreiging momenteel heel groot is .[3]

> 2.8 Eigenschappen van actoren

De hierbovengenoemde actoren hebben wij primair onderscheiden op basis van intentie. Er zijn echter ook andere eigenschappen op basis waarvan de actoren met elkaar te vergelijken zijn. Hiervan geven wij in tabel 2 een indicatief overzicht, inclusief de intentie, het primaire doelwit, de middelen, het volume en de gewenste zichtbaarheid van de diverse actoren.

	Intentie (doel)	Primair doelwit	Middelen	Volume	Zichtbaarheid
Staten	Geopolitieke positie verbeteren (interne machtspositie vergroten)	Overheden, multinationals, vitale infrastructuur, burgers (in het geval van bepaalde regimes)	Hoog	Midden	Laag
Private organisaties	Informatiepositie verbeteren	Eigen concurrenten	Hoog	Klein	Laag
Beroepscriminelen	Geld verdienen	Diensten met een financiële component Burgers	Midden tot hoog	Groot	Laag tot midden
Terroristen	Angst zaaien Politieke doelen	Doelwitten met een hoge impact Ideologisch gemotiveerde doelwitten	Laag tot midden	Klein	Hoog
Hacktivisten	Een gedachtegoed uitdragen	Ideologisch gemotiveerde doelwitten (zeer divers)	Laag tot midden en groeiend	Midden	Hoog
Scriptkiddies	Kijken of iets kan, lol trappen	Alle doelwitten	Laag	Groot	Midden

Tabel 2. Eigenschappen van actoren (indicatief)

De beschreven actoren zijn geen homogene groepen. Als gevolg daarvan is het lastig om een algemene inschaling te geven van de actoren als geheel. Voor de inschaling is daarom uitgegaan van de meest 'geavanceerde' subgroep binnen de betreffende actor. In het geval van beroepscriminelen zijn er bijvoorbeeld voldoende criminelen die zelf weinig middelen ter beschikking hebben. Daar staat tegenover dat er ook los georganiseerde verbanden bestaan, die als geheel meer middelen ter beschikking hebben.

Onder middelen vallen de beschikbare capaciteiten en instrumenten waarover een actor beschikt of kan beschikken om een aanval uit te voeren. Dit kan indirect ook een indicator zijn voor de mogelijke impact van een groep. Als het gaat om middelen is het denkbaar dat er interactie tussen actoren plaatsvindt, waarbij de ene groep kennis of kunde inkoopt bij een andere groep.

Het volume is een indicator voor de hoeveelheid van dergelijke aanvallen, waarbij moet worden opgemerkt dat dit een zeer grove indicatie is. Met name de actoren die baat hebben bij een lage zichtbaarheid, opereren grotendeels onder de radar. Inzicht verkrijgen in aantallen aanvallen, is daarom dan ook zeer lastig.

[3] NCTb (2010) en Beidel (2011).

Als laatste is de gewenste zichtbaarheid een factor die deels gekoppeld is aan de intentie van de dreigersgroep. Voor een beperkt aantal actoren is de zichtbaarheid van de aanval een belangrijk aspect voor het plegen van de aanval, terwijl anderen juist buiten de schijnwerpers willen blijven.

Bovenstaande daderprofielen kunnen worden getoetst aan incidenten die de laatste tijd hebben plaatsgevonden. De dDos-aanvallen in reactie op de Wikileaks-affaire passen bij het daderprofiel van de hacktivisten. Uit idealistische overwegingen werd daarbij de publiciteit gezocht. Andere incidenten zijn moeilijker te duiden, zoals het Diginotarincident, dat nog in onderzoek is. Op basis van gegevens uit openbare bronnen lijkt de aanval enerzijds te passen in het profiel van de statelijke actor, bijvoorbeeld gezien het feit dat de aanval in eerste instantie voor een deel ongedetecteerd is gebleven. Anderzijds past de publiciteit die door de vermeende dader is gegeven aan de aanval weer niet bij een statelijke actor. Het Diginotarincident bevestigt dat attributie van digitale aanvallen complex en lang niet eenduidig is.

3

> Dreigingen

Dreigersgroepen hebben, zoals in hoofdstuk 2 beschreven, bepaalde intenties. Er ontstaat een concrete dreiging als een dreigersgroep niet alleen de intentie heeft om bepaalde kwaadaardige activiteiten uit te voeren, maar ook de capaciteit heeft om dit te doen. Dit kan eventueel door met een hulpmiddel een kwetsbaarheid te misbruiken.

> 3.1 Soorten dreigingen

We onderscheiden drie soorten dreigingen: informatiegerelateerde dreigingen, systeemgerelateerde dreigingen en indirecte dreigingen. De onderverdeling informatiegerelateerd / systeemgerelateerd is gebaseerd op de typologie *Computer Network Exploitation (CNE) en Computer Network Attack (CNA)*.[4] Het derde type dreiging, de indirecte dreigingen, bestaat uit neveneffecten, waarbij het slachtoffer niet het directe doelwit van de dreigersgroep is.

In tabel 3 wordt de relatie weergegeven tussen de drie soorten dreigingen en de kwaliteitsaspecten van informatie die relevant zijn in het vakgebied informatiebeveiliging.

Directe dreigingen	Systeemgerelateerd		Informatiegerelateerd
Indirecte dreigingen	Neveneffecten		
Kwaliteitsaspect	Beschikbaarheid	Integriteit	Vertrouwelijkheid

Tabel 3. Relatie tussen soorten dreigingen en kwaliteitsaspecten van informatie

Informatiegerelateerde dreigingen ontstaan als dreigersgroepen de intentie hebben om informatie te verzamelen, te manipuleren, te publiceren of te misbruiken. Voorbeelden hiervan zijn identiteitsfraude en digitale spionage. Systeemgerelateerde dreigingen ontstaan als dreigersgroepen de intentie hebben om de dienstverlening of de bedrijfsvoering van een organisatie te verstoren of te onderbreken. Een voorbeeld hiervan is een DoS-aanval op de onlinedienstverlening van een organisatie. Indirecte dreigingen als gevolg van neveneffecten zijn een aparte categorie, die bestaat uit effecten die een bedreiging kunnen vormen voor cybersecurity, maar die een gevolg zijn van de hierboven beschreven directe dreigingen. DigiNotar is hiervan het beste voorbeeld. De inbreuk op de systemen van DigiNotar heeft zeer ingrijpende gevolgen gehad voor de continuïteit van gegevensverwerking en -uitwisseling binnen de Nederlandse overheid, maar het is vrijwel uitgesloten dat dit het directe doel van de aanvaller is geweest. De effecten van de DigiNotar-hack voor Nederland en de Nederlandse overheid zijn daarmee, hoe ingrijpend ook, slechts neveneffecten geweest van de oorspronkelijke aanval.

In het resterende gedeelte van dit hoofdstuk worden de dreigingen uitgewerkt die gedurende de rapportageperiode het meest in het oog springen.

> 3.2 Informatiegerelateerde dreigingen

Informatie, in het bijzonder vertrouwelijke en gevoelige informatie, is waardevol voor verschillende dreigersgroepen voor financieel gewin, voor het verbeteren van de eigen positie of om schade aan te brengen aan anderen.

> 3.2.1 Digitale spionage

> 3.2.1.1 *Gericht op overheden*

Er is grote interesse in vertrouwelijke overheidsinformatie en aanvallers zijn bereid grote inspanningen te verrichten om een aanval op te zetten en verborgen te houden. Staten zijn hierin voor de hand liggende actoren. De dreiging van digitale spionage is voor overheden een constante dreiging waarmee rekening moet worden gehouden.

[4] Deze typologie is geïntroduceerd in Joint Chiefs of Staff (2006).

Kwaadwillenden, waaronder andere staten en criminelen, maken veelvuldig gebruik van gerichte aanvallen om systemen binnen overheden te besmetten en op die manier gevoelige informatie te onderscheppen.[5] GOVCERT.NL krijgt regelmatig meldingen dat functionarissen binnen de Europese en Nederlandse overheden doelwit zijn van gerichte aanvallen. Om een computer te besmetten worden e-mailberichten met een bijlage gestuurd, vaak pdf-bestanden, die gericht zijn aan een specifieke functionaris. Een besmette computer is voor aanvallers een belangrijk kanaal voor het verkrijgen van vertrouwelijke informatie.

De afgelopen maanden was een aantal gerichte aanvallen ook in het nieuws, waaronder:

- In december 2010 infecteerden kwaadwillenden via malafide pdf-bestanden systemen van het Franse Ministerie van Financiën.
- In januari 2011 werd ontdekt dat 150 van de 170.000 systemen binnen het Franse ministerie besmet waren. Hieruit blijkt hoe gericht de aanvallers te werk zijn gegaan. Frankrijk is in 2011 voorzitter van de 'Group of Twenty' (G20). Kwaadwillenden bleken op zoek naar documenten over de aankomende G20-top. Volgens de Franse minister van Financiën zijn zij daarin geslaagd, maar waren de onderschepte documenten 'relatively unimportant'.
- Een tweede aanval richtte zich op de Europese Commissie (EC). Over deze aanval zijn minder details bekend. Kwaadwillenden hebben zich bij deze aanval toegang verschaft tot de e-mailaccounts van medewerkers van de EC. Naar verluidt was de gebruikte malware professioneel en verwijderde het zich soms 'ineens' van een systeem.
- Ook de infrastructuur van de Australische overheid kwam onder vuur te liggen.[6] Diverse computers, waaronder die van minister-president Julia Gillard en verschillende ministers, raakten besmet. Details over hoe deze besmetting heeft kunnen ontstaan, ontbreken. Wel is bevestigd dat de e-mailcorrespondentie gedurende meer dan een maand, is onderschept.

> 3.2.1.2 *Gericht op private organisaties*

Ook voor private organisaties is digitale spionage een serieuze dreiging. Zicht op daadwerkelijke incidenten is beperkt, omdat getroffen bedrijven begrijpelijkerwijs zeer terughoudend zijn met het delen van informatie over dergelijke incidenten. De aard van deze dreiging komt, afgezien van het specifieke doelwit, globaal overeen met digitale spionage gericht op overheden.

Een specifieke vorm van digitale spionage, gericht op beveiligingsbedrijven, heeft tijdens de rapportage-periode meerdere malen plaatsgevonden, waarbij de DigiNotar-hack voor Nederland het meest prominent was. Deze bedrijven waren echter niet het uiteindelijke doel van de aanval, maar eerder een *stepping stone* om andere vormen van misbruik te faciliteren. Er is namelijk informatie buit gemaakt die heel praktisch kan worden ingezet bij latere (gerichte) aanvallen op derde partijen. Omdat dergelijke derde partijen zich ook in Nederland kunnen bevinden, is daarmee de dreiging van digitale spionage enigszins vergroot. Momenteel zijn nog geen aanvallen in Nederland bekend op partijen waarbij gebruikgemaakt is van informatie uit eerdere aanvallen bij beveiligingsbedrijven.

Deze vorm van spionage, waarvan we drie concrete gevallen in de navolgende tekst toelichten, is een directe dreiging voor beveiligingsbedrijven, maar door de aard van de informatie ook in tweede instantie een dreiging voor anderen. Daarnaast heeft deze vorm van spionage tevens een indirecte dreiging tot gevolg die verder wordt uitgewerkt in paragraaf 3.4.2.

Vertrouwelijke informatie over two factor *authenticatiemiddel van RSA buit gemaakt*

RSA, een beveiligingsbedrijf dat onder andere authenticatiemiddelen levert, maakte 17 maart 2011 bekend dat onbekenden zich toegang hadden verschaft tot hun netwerk.[7] De aanvallers hebben, volgens RSA, informatie weten te bemachtigen, maar RSA heeft niet meer details bekend gemaakt. Wel heeft RSA de Amerikaanse beursautoriteit SEC formeel op de hoogte gebracht. Dit is een indicator voor de ernst van de inbraak.[8] Op basis van de beperkte informatie die RSA heeft vrijgegeven,concludeert Steve Gibson dat het voor de hand ligt dat in ieder geval een deel van het product SecurID (een *two factor* authenticatiemiddel) gecompromitteerd is.[9]

---

5 Uitgebreide achtergrondinformatie is na te lezen in AIVD (2010).
6 Benson (2011).
7 Coviello (2011).
8 United States Securities & Exchange Commission (2011).
9 Gibson (2011).

Dit product wordt ook in Nederland op grote schaal gebruikt, zowel binnen de overheid als bij private partijen. Uiteindelijk heeft RSA aangeboden de SecurID-tokens van een aantal van haar klanten te vervangen.[10]

Eind mei 2011 zijn drie mogelijk gerelateerde incidenten bekend geworden: bij Lockheed Martin, L2 en Northrup Grumman, bedrijven die opdrachten voor het Amerikaanse Ministerie van Defensie uitvoeren. Bij deze incidenten is vermoedelijk informatie over de SecurID-tokens ingezet. Hoewel de betrouwbaarheid van de informatie die nu in de media beschikbaar is, moeilijk is in te schatten, is de relatie tussen deze drie incidenten en de eerste aanval op RSA zeer voorstelbaar.

Een mogelijkheid is dat een staat bij Lockheed Martin en Northrup Grumman wilde inbreken om militaire geheimen te bemachtigen, maar dat dit bemoeilijkt werd door het gebruik van RSA SecurID-tokens door deze bedrijven voor toegang tot het netwerk. Door een gerichte aanval met e-mailberichten konden de aanvallers toegang krijgen tot SecurID-informatie bij RSA, waardoor zij alsnog succesvol bij Lockheed Martin en Northrup Grumman konden inbreken.[11]

Frauduleuze certificaten aangemaakt na inbraak bij certificaatleverancier Comodo

Het tweede incident waarbij de aanval zelf heel duidelijk een voorbereiding was voor verdere aanvallen op derden, is een aanval op een belangrijke businesspartner van Comodo. Comodo is een leverancier van beveiligingscertificaten, die onder andere gebruikt worden voor beveiligde webcommunicatie. Bij een partner heeft een aanvaller enkele certificaten en de bijbehorende geheime sleutels weten te bemachtigen.[12] Het ging om certificaten voor webdiensten met heel veel gebruikers, zoals Skype, Live.com, Yahoo.com en GMail.

Na enige tijd werd de aanval opgeëist door een anonieme persoon, die claimde op individuele basis gehandeld te hebben.[13] Hierbij werd voldoende bewijs geleverd om vast te stellen dat deze bron inderdaad bij de aanval betrokken is.[14] Het is echter niet uitgesloten dat meer personen bij de aanval betrokken zijn en dat er mogelijk voor een staat gehandeld is.

Omdat met deze certificaten het beveiligde internetverkeer voor deze websites kon worden onderschept, liepen de toegangsgegevens van miljoenen gebruikers van deze diensten risico. Deze aanval is ontdekt, de certificaten zijn teruggetrokken en niet meer bruikbaar.[15]

Frauduleuze certificaten aangemaakt en ingezet na inbraak bij DigiNotar

Een soortgelijk incident vond enkele maanden later plaats bij beveiligingscertificatenleverancier DigiNotar. Zij detecteerde in juli 2011 dat er binnengedrongen was op haar *Certificate Authority (CA)* infrastructuur. Met CA-infrastructuur worden beveiligingscertificaten gegenereerd. Deze certificaten worden gebruikt voor het beveiligen van websites, het elektronisch ondertekenen van documenten en het versleutelen van communicatie. Op alle CA-servers van DigiNotar zijn sporen van de hacker aangetroffen en uiteindelijk heeft de hacker honderden frauduleuze certificaten gegenereerd.[16] Een gebruiker in Iran gaf op een Google-forum aan hoe hij probeerde in te loggen op zijn gmail-account en van zijn browser een waarschuwing kreeg over de betrouwbaarheid van het certificaat.[17] Het bleek na inspectie van de gebruiker inderdaad te gaan om een frauduleus Google-certificaat. Omdat het serienummer van dit certificaat niet kon worden teruggevonden in de registraties van het CA-systeem, moet geconcludeerd worden dat het totaal aantal gegenereerde frauduleuze certificaten onbekend is.[18]

---

10 Coviello (2011).

11 Hypponen (2011).

12 Comodo (2011) & Kehayias (2011).

13 Een eerste onderzoek naar de inbraak leverde op dat het IP-adres van de aanvaller behoorde tot de adressenreeks van een Iraanse internetprovider.

14 Bright (2011b) & Fisher (2011).

15 Hoewel de aanval volgens Comodo snel is opgemerkt en bekendgemaakt, was hiermee de dreiging niet weggenomen. Alle software die de frauduleuze certificaten herkende als bonafide, moest worden geüpdatet. Veel softwareleveranciers kwamen na verloop van tijd dan ook met updates, waarmee software de certificaten als malafide kon herkennen

16 Fox-IT (2011).

17 De forumposter (Borhani 2011) maakte gebruik van Google Chrome als browser. Chrome maakt gebruik van een speciale techniek (certificate pinning) om in bepaalde gevallen sneller te kunnen detecteren dat een frauduleus certificaat wordt gebruikt. Zie ook Langley (2011).

18 Vasco (2011).

Omdat DigiNotar leverancier is van beveiligingscertificaten voor onderdelen van de Nederlandse overheid, had het incident specifiek voor Nederland grote gevolgen. De afhankelijkheid van de Nederlandse overheid van DigiNotar als leverancier van beveiligingscertificaten had als gevolg dat de dienstverlening van meerdere overheidsinstanties verstoord werd. De Nederlandse overheid greep in en overheidsinstanties moesten overstappen op een andere leverancier.

Daarnaast geeft het incident bij DigiNotar eveneens het belang aan van het direct melden van incidenten. Ondanks de uitvoering van een beveiligingsaudit bleken frauduleuze certificaten nog steeds in omloop te zijn. Hierdoor liepen meerdere partijen gevaar zonder daar bewust van te zijn.

Onderzoek naar de inbraak bij DigiNotar gaf tevens aan dat de ter plekke getroffen beveiligingsmaatregelen onvoldoende waren om deze inbraak te voorkomen. Op de meest kritieke servers is malware gevonden die met antivirussoftware gedetecteerd had kunnen worden. Dergelijke software was op de computersystemen echter niet aanwezig, zoals bleek uit bevindingen van het Fox-IT-onderzoek. Daarnaast was op de publieke webserver verouderde en ongepatchte software geïnstalleerd. Alle CA-servers waren lid van hetzelfde Windows-domein en toegang tot deze servers werd via dezelfde gebruikersnaam en hetzelfde wachtwoord verkregen. Het administrator wachtwoord van de CA-servers was niet erg sterk en kon makkelijk worden gekraakt. Verder was er geen scheiding tussen kritische componenten of deze scheiding werkte niet goed. [19]

> 3.2.2 Publicatie van persoonsgegevens of vertrouwelijke informatie

Publicatie van vertrouwelijke informatie of persoonsgegevens is een dreiging voor overheden, bedrijven en personen. Terwijl actoren die zich bezighouden met het verzamelen van gegevens bij digitale spionage veelal buiten de schijnwerpers willen blijven, gebruiken andere actoren, voornamelijk hacktivisten, publicatie van gegevens als middel ter ondersteuning van hun doelstellingen.

De afgelopen periode zijn opvallend veel datalekken bekend geworden. Dergelijke datalekken treffen alle neutrale actoren. Zowel overheden als private organisaties zijn slachtoffer van datalekken, aangezien hun databestanden gecompromitteerd worden en vervolgens online gepubliceerd. Als hierbij ook persoonsgegevens van klanten betrokken zijn, worden burgers ook geraakt door de lekken. Voorbeelden hiervan uit de afgelopen periode zijn het lekken van alle e-mailadressen en wachtwoorden van leden van datingsite Pepper.nl, klanten van de website cheaptickets.nl, het Sony Playstation Network en meerdere lekken bij SonyBMG. Het gaat in sommige wereldwijde gevallen ook om enorme hoeveelheden persoonsgegevens: er zijn bijvoorbeeld van zo'n 100 miljoen gebruikers van Sony's Playstation Network persoonsgegevens buit gemaakt.

Opvallend is dat er relatief veel mensen zakelijke e-mailadressen gebruiken voor internetdiensten die zij persoonlijk gebruiken. Dit was bijvoorbeeld het geval bij pepper.nl. Het risico van vermenging van privé- en zakelijk internetgebruik komt prominent naar voren bij deze datalekken. De informatie die gelekt wordt, is zeer bruikbaar voor gerichte aanvallen, als men bijvoorbeeld privé hetzelfde wachtwoord gebruikt als op het werk.

GOVCERT.NL monitort publieke uitingen van diverse groeperingen en nieuwsbronnen die over sites met datalekken publiceren. Er hebben zich al meerdere incidenten voorgedaan waarbij gevoelige informatie over medewerkers van de Rijksoverheid en uit de vitale sectoren is gelekt. Ook hierbij was sprake van het gebruik van zakelijke e-mail voor privézaken.

Kwaadwillenden gaan ook gerichter te werk. Aaron Barr, de CEO van HBGary Federal, leverancier van beveiligingssoftware en -diensten[20], sprak enige tijd geleden het vermoeden uit dat hij de leider van Anonymous op het spoor was. Hierop besloot Anonymous de aanval te openen op Barr en zijn bedrijf, en is veel vertrouwelijke bedrijfsinformatie buit gemaakt en geopenbaard. Anonymous wist snel volledig toegang te krijgen tot de kennelijk slecht beveiligde systemen van HBGary. Deze toegang werd gebruikt om 40.000 e-mailberichten te stelen, salarisinformatie te bemachtigen, data te vernietigen en de website aan te passen.[21] Ook werd het systeem van beveiligingsonderzoeker en eigenaar van HBGary zélf, Greg Hoglund, overgenomen met vergelijkbare gevolgen. Een groot gedeelte van de gegevens is online geplaatst. Uit deze gegevens zijn]onder andere klantgegevens af te leiden van de NSA, Interpol en enkele Nederlandse overheidsinstellingen. GOVCERT.NL heeft de betrokken Nederlandse partijen op de hoogte gebracht.

[19] Fox-IT (2011).

[20] HBGary is een bedrijf dat software en diensten levert voor met name forensische opsporings- en inlichtingendiensten. HBGary ontwikkelt bijvoorbeeld specialistische malware voor opsporingsdiensten.

[21] Bright (2011).

> 3.2.3 Digitale identiteitsfraude

Voor criminelen zijn persoonsgegevens een belangrijke voorwaarde om misbruik te kunnen maken van de identiteit van een ander met financieel gewin als uiteindelijk doel. Zij hanteren verschillende methoden om persoonsgegevens te bemachtigen. Een bekende methode is het onttrekken van gegevens aan met malware besmette computers. Het achterhalen van gegevens door middel van phishing is een andere manier, maar hergebruik uit datalekken is ook een mogelijkheid.

Jaar	Schade	Klachten
2009	€ 1.900.000	onbekend
2010	€ 9.800.000	1383
2011 (eerste helft)	€ 11.200.000	2418

Tabel 4. Overzicht schade internetbankieren

Phishing is al jaren een succesvol aanvalsinstrument, waarmee inloggegevens of andere persoonsgegevens worden verkregen. Phishingmails werden oorspronkelijk voornamelijk verstuurd uit naam van private instellingen. Banken in het bijzonder hebben veel last van phishing en ondervinden daarvan ook schade. Zowel de financiële schade evenals de klachten vertonen een stijging. Uit de toelichting van de Nederlandse Vereniging van Banken (NVB) wordt duidelijk dat phishing de meest voorkomende manier is waarop fraude met internetbankieren plaatsvindt. In tabel 4 staat een overzicht van de schade en het aantal klachten van de afgelopen jaren.[22]

Tegenwoordig wordt ook de overheid misbruikt als afzender van phishingmails. In het begin van 2011 hebben een paar incidenten plaatsgevonden waarbij uit naam van de overheid phishingmails verstuurd zijn. Dit is voor de overheid, maar zeker ook voor de burger een zorgelijke ontwikkeling. De kans op dit soort phishingaanvallen en de belangstelling voor DigiD, neemt toe naarmate steeds meer diensten digitaal door de overheid verleend worden. In dit licht zijn ook kwetsbaarheden in websites van overheden zeer relevant, daar deze ook een ingang kunnen bieden aan kwaadwillenden om aan persoonsgegevens te komen.[23]

Naast het verleiden van burgers om hun gegevens te verstrekken, blijven kwaadwillenden bedrijven aanvallen om op grootschalige wijze persoonsgegevens te vergaren. Meerdere incidenten illustreren deze constatering. In het eerste kwartaal van dit jaar hebben twee datalekken een prominente rol gekregen in de media. Dit zijn een datalek bij de marketingfirma Epsilon en bij het PlayStation Network (PSN) van Sony.

Bij het Epsilon-datalek zijn namen en e-mailadressen van individuele cliënten bemachtigd die onder andere door banken en hotels bij Epsilon waren ondergebracht. Met deze informatie kunnen aanvallers hun phishing-aanvallen veel specifieker en doelgerichter maken. Ook kunnen aanvallers een bericht sturen uit naam van een organisatie, waarmee het potentiële slachtoffer al een relatie heeft. Namen en e-mailadressen samen met informatie over relaties tussen bedrijven en klanten kunnen als basis dienen voor een nieuwe aanval.

In het geval van het PSN-datalek hebben aanvallers persoonsgegevens van 77 miljoen klanten van Sony bemachtigd. Sony heeft gemeld dat het ook een oude database met creditcardgegevens en rekeningnummers betrof waarin ook klanten uit Nederland stonden. Het gaat in totaal om 23,4 miljoen records.[24] De creditcard-gegevens van het PSN-lek kunnen bijvoorbeeld misbruikt worden op webwinkels, waardoor de rekeningen van de aankopen bij het slachtoffer terechtkomen. Of dit daadwerkelijk gebeurd is, is onbekend.

Identiteitsfraude wordt soms ook mogelijk gemaakt door kwetsbaarheden die ontstaan door de wijze waarop instellingen hun gebruikers authenticeren. Zo was de Nederlandse Emissieautoriteit (NEa), verantwoordelijk voor de handel in CO_2-emissierechten in Nederland, eind 2010 doelwit van een aanval. Met malware trachtten aanvallers de inloggegevens van gebruikers van het handelssysteem van emissiecertificaten te onderscheppen.

[22] Nederlandse Vereniging van Banken (NVB) (2010) en (2011).

[23] Op 3 oktober hebben onafhankelijke onderzoekers aangetoond dat dergelijke kwetsbaarheden op meerdere plekken aanwezig zijn, zie hiervoor de Winter (2011).

[24] Sony (2011).

Een ander gepubliceerd voorbeeld is de fraude die is gepleegd met DigiD, bij de Belastingdienst. Deze fraude was mogelijk omdat het burgerservicenummer voor een toeslagaanvraag niet overeen hoefde te komen met het burgerservicenummer van de DigiD-gebruiker (de aanvrager).[25]

Inmiddels zijn echter ook andere authenticatiemethoden, zoals het versturen van sms-berichten, kwetsbaar voor misbruik. Dit draagt ook bij aan een toename in de dreiging van identiteitsfraude, aangezien bepaalde publieke en private instellingen deze methode hanteren voor het authenticeren van gebruikers en/of transacties. Dit wordt verder uitgewerkt in paragraaf 5.1.2.1.

Verder houden andere beroepscriminelen zich bezig met andere vormen van internetfraude. Een prominent voorbeeld is internetgerelateerde fraude via handelssites zoals Marktplaats, Speurders etc.. Op 8 oktober 2010 is, in het kader van de proeftuin Internetgerelateerde Fraude, een digitaal meldpunt gelanceerd voor internetgerelateerde fraude gepleegd via handelsplaatsen. Over een periode van 10 maanden zijn meer dan 25.000 meldingen binnengekomen (ruim 30.000 op jaarbasis) waarbij ook beter zicht is verkregen op veelplegers. Terwijl het aantal meldingen procentueel gezien maar een fractie is van alle advertenties op de handelssites treft dit veel burgers die erbij betrokken zijn geraakt. In vergelijking met voorgaande jaren is een toename geconstateerd in het gemiddeld aantal meldingen per dag. Terwijl het in 2009 ging om een gemiddelde van 15 meldingen per dag en in 2010 om 25 meldingen per dag, is dit totaal gegroeid tot 77 meldingen per dag over de gemeten periode. Zoals beschreven in het evaluatierapport: "[v]oor de lancering bedroeg het aandeel meldingen 0,015% van het totaal aantal advertenties. Na de lancering is dit bijna verdubbeld, naar 0,026%".[26]

> 3.3 Systeemgerelateerde dreigingen

Onder systeemgerelateerde dreigingen worden dreigingen verstaan die gericht zijn op verstoring van de beschikbaarheid of uitvoering van een dienst of organisatie. Dit kan betekenen dat de dienst onbereikbaar gemaakt wordt of gesaboteerd wordt en andere acties gaat uitvoeren.

> 3.3.1 Gerichte verstoring van vitale infrastructuur

Hoewel Stuxnet heeft aangetoond dat gerichte verstoring van ICS een concrete dreiging is, is deze dreiging voor Nederland momenteel niet waarschijnlijk.[27] Stuxnet bleek een succesvolle en zeer gerichte cyberaanval op Iraanse uraniumverrijkingsinstallaties. Stuxnet maakte misbruik van verschillende kwetsbaarheden in de Siemens-software van de ICS en in Microsoft Windows. Iran heeft toegegeven dat door deze sabotage hun atoomprogramma meer vertraging heeft opgelopen.[28] Israël, en mogelijk ook de Verenigde Staten, worden gezien als meest waarschijnlijke daders.

Stuxnet is behoorlijk complex en het volledig doorgronden van de werking en het doelwit heeft wel een jaar geduurd. Pas sinds het voorjaar van 2011 lijkt de werking en het doelwit van Stuxnet echt ontrafeld.[29] Gezien het zeer specifieke doelwit is de bestaande Stuxnet-malware geen directe bedreiging voor Nederlandse overheden of bedrijven, maar wel een belangrijke waarschuwing. Omdat Stuxnet beschikbaar is op het internet en wordt nagebouwd, is toegang tot informatie over Stuxnet en het ontwikkelen van varianten laagdrempeliger geworden.[30] Uiteindelijk kunnen kwaadwillenden op Stuxnet gebaseerde varianten ontwikkelen om ook ICS van andere (vitale) processen te manipuleren.[31] Om een effectieve variant van Stuxnet te ontwikkelen is overigens wel diepgaande kennis nodig van het proces dat men wil beïnvloeden, voor simpel digitaal vandalisme is copycatgedrag daarentegen voldoende. De toenemende bekendheid van kwetsbaarheden in ICS-software biedt echter meerdere mogelijk-heden voor dreigersgroepen om aanvallen te plegen op ICS. In paragraaf 5.2.1.2 gaan we verder in op deze kwetsbaarheden.

[25] Belastingdienst (2011) & Verkade (2011).
[26] Programma Aanpak Cybercrime (PAC) (2011).
[27] In GOVCERT.NL (2010a) worden de algemene cyberrisico's binnen procesbesturingssystemen (of Industrial Control Systems), vaak ook SCADA genoemd, nader toegelicht.
[28] Clayton (2010).
[29] In GOVCERT.NL (2010b) staan meer details. GOVCERT.NL (2010a: 18,19) beschrijft Stuxnet in het bijzonder en de beveiliging van procesbesturingen in het algemeen.
[30] Thabet (2011).
[31] Meerdere ICS-securityexperts zien dit ook als een reële dreiging. Zie bijvoorbeeld Langer (2011) & Peterson (2011).

> 3.3.2 Verstoring van (online)dienstverlening

Verstoring van (online)dienstverlening is een concrete dreiging van de Nederlandse overheid en private organisaties in Nederland. Verstoringen worden voornamelijk uitgevoerd uit ideologische overwegingen, waarbij een aanval vrij 'onverwacht' kan plaatsvinden en specifieke doelwitten niet gemakkelijk te voorspellen zijn.
Uiteenlopende instanties en bedrijven zijn de afgelopen periode het slachtoffer geworden van digitale aanvallen, waarbij de aanvallers handelden uit ideologische overwegingen. Dit was het geval tijdens de WikiLeaks-affaire. Anonymous, sympathisanten van WikiLeaks, verstoorden met een DoS-aanval onder andere de websites van bedrijven die stopten met betalingstransacties van WikiLeaks te verwerken: Paypal en Mastercard. Tijdens de WikiLeaks-affaire zijn DoS-tools gepubliceerd waardoor een breed publiek er gemakkelijk toegang toe had. Iedereen met een snelle internetverbinding kon meedoen met een aanval waartoe via sociale media werd opgeroepen.[32] Op deze manier kunnen hacktivisten toenadering zoeken met scriptkiddies om de schaal van de aanval te vergroten.

De website rijksoverheid.nl was in februari 2011 zwaar overbelast en gedurende enkele uren niet of slecht bereikbaar. De oorzaak bleek een DoS-aanval waarbij de aanvallers de website bestookten met grote hoeveelheden verzoeken om op die manier legitieme verzoeken te blokkeren of ernstig te vertragen. Het doel van de aanval is niet bekend.

Niet alleen rijksoverheid.nl heeft last gehad van deze aanval. Ook een grote Nederlandse bank kreeg op ongeveer hetzelfde moment aanvallen te verwerken. De bank kampte enkele dagen met storingen en uitval van diensten als iDeal.[33] Zowel de Rijksoverheid als de bank hebben aangifte gedaan bij de politie.

Uit onderzoek is gebleken dat de aanvallen afkomstig waren van een beperkt aantal geïnfecteerde websites. Dit wijkt af van het traditionele patroon bij DoS-aanvallen, waarbij een aanval veelal afkomstig is van pc's van thuisgebruikers. De aanvaller maakt in een dergelijk scenario misbruik van een geïnfecteerde pc of de eigenaar installeert zelf een DoS-programma op zijn systeem, zoals is gebeurd bij de aanvallen op politie.nl en om.nl, eind 2010.

Met de nieuwe methode kan een krachtiger aanval worden uitgevoerd die niet afhankelijk is van een eindgebruiker en die daardoor langer actief kan blijven. Daarnaast heeft de aanvaller de mogelijkheid de DoS-aanval overal vanaf internet aan te sturen.

De (imago)schade en overlast van een DoS-aanval kunnen aanzienlijk zijn. De meeste aanvallen richten zich op websites. Andere doelwitten zijn ook mogelijk: mailservers, authenticatie-servers (bijvoorbeeld DigiD) of servers voor het uitvoeren van betalingen (bijvoorbeeld iDeal). De effecten van DoS-aanvallen zijn divers: inkomstenderving (webwinkels), onmogelijkheid om online aangifte te doen (politie), slechte bereikbaarheid van bedrijven voor leveranciers of personeel dat wil telewerken, verstoorde overheidscommunicatie et cetera. Ook vitale sectoren kunnen hinder ondervinden, omdat bijvoorbeeld beheervoorzieningen op afstand voor service en onderhoud niet bereikbaar zijn. Ten slotte bestaat de kans dat een aanval ook andere diensten beïnvloedt die zijn ondergebracht bij dezelfde provider. Zo had de DoS-aanval op om.nl gevolgen voor politie.nl. Dit is een punt van aandacht voor de ministeries die nu allemaal via rijksoverheid.nl bereikbaar zijn en een van de indirecte dreigingen waarop we in paragraaf 3.4 ingaan.

Door de toegenomen toegankelijkheid van DoS-aanvallen, neemt de dreiging van verstoring van onlinedienstverlening toe. Zoals hierboven beschreven kan een dergelijke aanval onder andere ingezet worden door hacktivisten om de dienstverlening van een doelwit, hetzij de overheid of het bedrijfsleven, te verstoren.

[32] De strafbaarheid van DoS-aanvallen schrikt daarbij mogelijk af.
[33] 'Betalingsverkeer iDeal ondervindt hinder' (2011).

> 3.4 Indirecte dreigingen

Iedereen die gebruikmaakt van ICT, is daarmee voor een groot deel afhankelijk van de producten van derden. Aanvallen op die derden kunnen daarmee grote impact hebben op de continuiteit, exclusiviteit of integriteit van de eigen dienstverlening en informatie. In de volgende paragrafen worden de meest relevante neveneffecten van dit moment genoemd.

> 3.4.1 Verstoring van bedrijfsvoering door malwarebesmetting

Verstoring van de bedrijfsvoering als gevolg van een malwarebesmetting is een belangrijke dreiging voor zowel de overheid, het bedrijfsleven als de academische wereld op dit moment. Het gaat in dit geval specifiek om besmettingen door 'ongerichte' malware, dat wil zeggen malware die zichzelf ongeremd verspreid met als doel zoveel mogelijk systemen te besmetten om deze daarna in een botnet in te zetten en af te scannen op waardevolle informatie. Deze ongeremde verspreiding kan (delen van) een bedrijfsnetwerk onderuithalen, maar ook als dat niet gebeurt kan het weer schoonmaken van het netwerk erg kostbaar zijn voor een organisatie, zowel in directe kosten voor het schoonmaken als in indirecte kosten als gevolg van verloren productiviteit. GOVCERT.NL wordt geregeld ingeschakeld voor assistentie bij malwareuitbraken bij haar deelnemers.

> 3.4.2 Verstoring van bedrijfsvoering door aanval bij een derde partij

Een geslaagde aanval bij een derde partij kan ingrijpende gevolgen hebben voor de kwetsbaarheid van de eigen organisatie, sector of – in het geval van DigiNotar – het eigen land. Deze dreiging is met name in het afgelopen jaar sterk gegroeid.

De aanvallen op DigiNotar en RSA, zoals beschreven in paragraaf 3.2.1.2, hebben laten zien wat de effecten in de praktijk kunnen zijn. De geslaagde aanval op RSA heeft ook voor andere bedrijven grote impact gehad. Naast de eerder beschreven aanvallen op de defensiebedrijven Lockheed Martin en Northrup Grumman, gaat het om al die andere organisaties die gebruikmaakten van RSA-tokens en die uit beveiligingsoverwegingen hebben moeten besluiten hun toegangsmiddel te vervangen of bepaalde diensten – die hiermee werden beveiligd – tijdelijk stop te zetten.

Ditzelfde geldt in het geval van DigiNotar. De inbreuk op de systemen van DigiNotar heeft zeer ingrijpende gevolgen gehad voor de continuïteit van gegevensverwerking en -uitwisseling binnen de Nederlandse overheid, waarbij ook het gebrek aan inzicht in de daadwerkelijke afhankelijkheid een belangrijke factor is geweest. Toch is het vrijwel uitgesloten dat dit het directe doel van de aanvaller is geweest. De effecten van de DigiNotar-hack voor Nederland en de Nederlandse overheid zijn daarmee, hoe ingrijpend ook, slechts neveneffecten geweest van de aanval.

Een specifieke situatie, waarbij de afhankelijkheid van een derde partij erg groot is, is de situatie waarbij gebruik wordt gemaakt van clouddiensten. Dit aspect wordt verder uitgewerkt in paragraaf 5.3.1.

> 3.4.3 Verstoring van dienstverlening door aanval bij een derde partij

DDoS-aanvallen zijn vrij grove aanvallen. Als gevolg daarvan wordt bij een dergelijke aanval vaak niet alleen de dienst van het doelwit getroffen, maar ook andere diensten die 'in de buurt staan'. Deze dreiging is beperkt.

Een voorbeeld hiervan is de website politie.nl, die onbereikbaar werd toen de website om.nl onder vuur lag. Dit was het gevolg van het feit dat ze bij dezelfde provider waren ondergebracht.

> 3.5 Dreigingsoverzicht

Op basis van de inzichten in actoren (wie zijn ze, wat willen ze en wat kunnen ze) en de daadwerkelijke dreigingen zoals beschreven in dit hoofdstuk, kan een overzicht worden gemaakt van de ernst van diverse dreigingen. In tabel 5 staat dit overzicht.
Horizontaal kan worden afgelezen welke dreigingen uitgaan van een dreigersgroep. Verticaal kan worden afgelezen met welke dreigingen en dreigersgroepen verschillende doelwitten in Nederland rekening moeten houden. Deze tabel is nadrukkelijk niet bedoeld om voor individuele gevallen te bepalen welke dreigersgroep verantwoordelijk is voor een incident. Daarvoor is uiteraard gericht onderzoek nodig.

Tabel 5. Dreigingsoverzicht naar dreigersgroep en doelwit

Dreigersgroepen	Doelwitten: Overheid	Doelwitten: Private organisaties	Doelwitten: Burgers
Staten	Digitale Spionage en sabotage	Digitale spionage en sabotage	
Private organisaties		Digitale spionage	
Hacktivisten	Publicatie van vertrouwelijke gegevens en digitale verstoring	Publicatie van vertrouwelijke gegevens en digitale verstoring	Publicatie van vertrouwelijke gegevens
Terroristen	Sabotage	Sabotage	
Beroepscriminelen	Cybercrime (waaronder digitale (identiteits-)fraude)Neveneffect: verstoring door malwarebesmetting	Cybercrime (waaronder digitale (identiteits-)fraude)Neveneffect: verstoring door malwarebesmetting	Cybercrime (waaronder digitale (identiteits-)fraude)
Scriptkiddies	Digitale verstoring	Digitale verstoring	

(legenda bij tabel)

Kleur	Betekenis
	Hoog
	Middel
	Laag
	N.v.t of onbekend

De dreiging van vreemde mogendheden gaat voornamelijk uit naar de Nederlandse overheid en multinationals en momenteel in mindere mate naar organisaties in de vitale infrastructuur. Relevant, maar qua omvang zeer klein is de dreiging die van vreemde mogendheden uitgaat naar onderdanen die zich in Nederland bevinden. Over de dreiging die direct uitgaat van private organisaties is weinig bekend. Overlap met de dreiging vanuit staten is hier mogelijk, omdat moeilijk is vast te stellen wie achter een aanval zit.

Beroepscriminelen richtten zich traditioneel voornamelijk op het bedrijfsleven, en dan veelal op de financiële sector. Daarbij wordt veelal diefstal gepleegd door middel van identiteitsfraude, waarbij bestaande identiteiten van burgers in het spel zijn. Er zijn daarnaast aanwijzingen dat nu, met de groei van e-overheidsdiensten, ook de overheid een interessanter doelwit vormt voor beroepscriminelen. De hulpmiddelen die beroepscriminelen gebruiken, met name malware, zijn gemaakt om zichzelf op grote schaal te verspreiden en besmetting te veroorzaken, wat zowel voor overheid als bedrijfsleven een belangrijke indirecte dreiging is. Tenslotte is de dreiging die vanuit beroepscriminelen uitgaat naar burgers aanzienlijk. Het gaat om onder andere identiteitsfraude en om andere typen van fraude, die weliswaar in individuele gevallen vaak relatief beperkt zijn van omvang, maar waar het wel om een aanzienlijk aantal gevallen gaat.

De dreiging die uitgaat van de groep hacktivisten is klein, maar groeiend. Hacktivisten kiezen hun doelwitten vrij onvoorspelbaar en ongeacht of het doelwit publiek of privaat is, zijn daarbij vrijwel altijd persoonsgegevens in het spel.

Terroristen hebben weliswaar de intentie om grootschalige verstoring of ontwrichting te veroorzaken, maar vooralsnog zijn er geen aanwijzingen dat zij de capaciteiten hebben, en dat deze dreiging heel groot is. Scriptkiddies, ten slotte, vormen nauwelijks een serieuze bedreiging voor de drie genoemde doelwitten, maar richten zich, met hun beperkte middelen, voornamelijk op overheid en private organisaties.

4

> Hulpmiddelen

Voor het uitvoeren van aanvallen maken de dreigersgroepen gebruik van een aantal middelen die voor diverse doeleinden misbruikt kunnen worden. De belangrijkste hulpmiddelen op technisch vlak zijn exploits, malware en botnets. Er zijn andere middelen, zoals spam en social engineering, maar op basis van de rapportageperiode is er geen aanleiding om deze middelen uitgebreid toe te lichten.

> 4.1 Exploits

Wanneer in software een kwetsbaarheid bestaat, betekent dit niet gelijk dat deze kwetsbaarheid ook misbruikt wordt. Een exploit is een manier om misbruik te maken van een kwetsbaarheid. Een exploit is een stuk programmacode, een verzameling gegevens of een opeenvolging van commando's die specifiek is gemaakt om een bepaalde kwetsbaarheid in software te misbruiken om daarmee effecten te veroorzaken die niet bedoeld of verwacht waren. Vrijwel elke exploit is dan ook gemaakt voor een specifieke kwetsbaarheid.

Exploits kunnen op verschillende manieren worden ingezet. Een exploit voor een kwetsbaarheid in Adobe Reader wordt verstopt in een pdf-bestand, zodat bij het openen van het bestand de kwetsbaarheid wordt misbruikt. Het effect kan zijn dat de aanvaller de controle over de computer kan overnemen. Een exploit voor een kwetsbaarheid in een webbrowser kan worden verstopt in een webpagina en exploits voor kwetsbaarheden in besturingssystemen worden vaak ingebouwd in malware.

Door technologische vooruitgang in de kwaliteit van standaardsoftware (zoals het inbouwen van beschermingsmaatregelen) is het de afgelopen jaren moeilijker geworden om succesvolle exploits voor kwetsbaarheden te maken. De waarde van werkende exploits is daarmee omhooggegaan. Je zou zelfs kunnen zeggen dat het een vak is geworden om exploits te maken.

Een bepaald soort exploits (genaamd *zero day exploits*) is speciaal gemaakt om misbruik te maken van kwetsbaarheden die nog niet algemeen bekend zijn. De kans dat met een dergelijke exploit een succesvolle aanval kan worden uitgevoerd, is groter dan met een gewone exploit, omdat verdediging tegen misbruik van onbekende kwetsbaarheden erg lastig is. Dergelijke *zero day exploits* hebben dan ook een nog grotere waarde dan gewone exploits. Deze exploits zien we dan ook vaker terug bij gerichte aanvallen, zoals Stuxnet, dan bij grootschalige aanvallen. Een van de gevolgen hiervan is dat er nu organisaties zijn die kwetsbaarheden en exploits niet meer openbaar maken maar verkopen. Sommige softwareleveranciers, zoals bijvoorbeeld Google, proberen het onderhands verkopen van exploits tegen te gaan door zelf geld te bieden aan onderzoekers voor de kwetsbaarheden die zij vinden. De bedragen die geboden worden, zijn echter laag.

> 4.2 Malware

Malware is een samentrekking van de woorden *malicious* en *software*: het is kwaadaardige software, die ten grondslag ligt aan veel aanvallen en die een belangrijke rol speelt in de ontwikkeling van botnets. Innovators blijven doorgaan in hun malware-ontwikkeling en richten zich in deze tevens op andere platformen. Een actueel voorbeeld hiervan zijn mobiele platformen, waar nieuwe aanvallen gesignaleerd zijn.

Zo is er een mobiele versie opgedoken van malware die specifiek gemaakt is om bankgegevens te onderscheppen: de Zeus-malware. De kracht van deze variant is dat het ook de sms-berichten kan onderscheppen die voor authenticatie van de transactie worden gebruikt, aangezien die ook op de mobiele telefoon binnenkomen. Het percentage nieuwe malware voor mobiele apparaten is volgens een leverancier in 2010 met 46% gestegen in vergelijking met 2009.[34] Het is voor de hand liggend dat dit mede gerelateerd is aan de groei van mobiele apparatuur, zoals beschreven in paragraaf 5.3.2.

[34] McAfee (2010).

Toch zijn er momenteel slechts enkele honderden stuks malware voor mobiele platformen ten opzichte van honderdduizenden voor desktopplatformen. De verwachting blijft dat serieuze aanvallen gericht op mobiele apparatuur de komende jaren zullen toenemen. Mobiele malware kan in ieder geval ingezet worden door criminelen voor het aanvallen van bankrekeningen. Daarnaast kan afhankelijk van het gebruik van de mobiele apparatuur het tevens een doelwit zijn voor het vergaren van vertrouwelijke informatie van overheden en bedrijfsleven.

> 4.3 Botnets

Botnets zijn netwerken van computers die door middel van een malwarebesmetting gekaapt zijn. Ze worden vanwege hun flexibiliteit en veelzijdigheid gezien als het Zwitsers zakmes van cybercriminelen en andere actoren. Ze nemen al enkele jaren een centrale plaats in als hulpmiddel bij veel financieel gemotiveerde aanvallen en bij verstoringen (de zogenoemde DoS-aanvallen). Hierdoor zijn botnets in ieder geval een bruikbaar aanvalsmiddel voor criminelen en hacktivisten. Botnets kunnen ontstaan omdat grote aantallen computers op internet kwetsbare software bevatten en die als gevolg daarvan op afstand over te nemen zijn.

Botnets gebruiken voor communicatie steeds vaker versleuteling en een groeiend aantal botnets wordt niet centraal maar decentraal aangestuurd. Deze veranderingen dienen om opsporing en interventie te bemoeilijken.

In opdracht van het Ministerie van Economische Zaken, Landbouw en Innovatie is onderzoek gedaan naar de hoeveelheid besmette computers per provider in Nederland.[35] Uit de resultaten komt naar voren dat meer dan de helft (60%) van de geïnfecteerde systemen via drie van de grootste Nederlandse providers internettoegang ontvangen.[36] Een klein aantal ISP's veroorzaakt dus ongewild relatief veel overlast. De verschillen tussen providers in Nederland zijn volgens de onderzoekers opmerkelijk, maar kleiner dan in het buitenland. Om deze cijfers in breder perspectief te trekken kan een vergelijking getrokken worden met internationaal onderzoek. Wereldwijd zijn de netwerken van vijftig ISP's samen goed voor ongeveer de helft van alle besmette systemen die deel uitmaken van een botnet.[37]

In de afgelopen periode zijn enkele grote botnets uit de lucht gehaald. Hierbij was sprake van een internationale publiekprivate samenwerking. Opsporingsdiensten, veiligheidsdiensten, CERTs, softwareleveranciers, onderzoekers en antivirusleveranciers werkten op projectbasis samen om een of meer botnets aan te pakken. Nederland heeft hierin wereldwijd een voortrekkersrol vervuld, mede door acties van het KLPD (i.c. het Team High Tech Crime), GOVCERT.NL en LeaseWeb. Gelet op het grote aantal actieve botnets zijn dit helaas nog bescheiden successen.

35 Van Eeten et al. (2011).
36 In totaal deden veertien providers mee aan het onderzoek.
37 Van Eeten et al. (2010).

5

> Kwetsbaarheden

Dit hoofdstuk beschrijft op hoofdlijnen enkele belangrijke factoren die bijdragen aan kwetsbaarheid voor dreigingen in het cyberdomein. Deze lijst met factoren is niet uitputtend, maar samengesteld op basis van relevante incidenten of ontwikkelingen uit de rapportageperiode. Er is onderscheid tussen enerzijds menselijke en organisatorische factoren en anderzijds technische factoren, aangevuld met nieuwe technologieën.

In het algemeen kan worden gezegd dat elke dreigersgroep misbruik zou kunnen maken van de in dit hoofdstuk benoemde factoren. De beschreven factoren zijn generiek en betreffen zowel overheid, bedrijfsleven als burgers. De mate waarin zij kwetsbaar zijn, wisselt sterk en zal daarom niet aan de orde komen in dit hoofdstuk.

> 5.1 Menselijke en organisatorische factoren

De beveiliging van informatie is een complex vakgebied dat binnen vrijwel elke organisatie van direct belang is voor de bedrijfsvoering. Deze paragraaf beschrijft enkele factoren op menselijk en organisatorisch vlak die bijdragen aan kwetsbaarheid voor dreigingen.

Onvoldoende managementaandacht voor informatiebeveiliging leidt vrijwel zeker tot een gebrek aan een samenhangend informatiebeveiligingsbeleid, wat gebrekkige beveiliging en daaruit voortvloeiende kwetsbaarheid voor (moedwillige) verstoring tot gevolg kan hebben. Een opvallend onderwerp op dit vlak uit de afgelopen periode is de beveiliging van voicemaildiensten en de manier waarop de overheid daarmee is omgegaan. Dit heeft de overheid kwetsbaar gemaakt voor spionage en misbruik.

Een organisatorisch probleem is de manier waarop organisaties omgaan met versleutelingstechnieken. De aard van deze technieken vereist periodieke evaluatie en herijking, iets dat binnen veel organisaties niet gebeurt. Gsm is daar een specifiek en actueel voorbeeld van.

Ten slotte benoemen we in deze paragraaf de gedetailleerde vastlegging en verwerking van privacygevoelige informatie. Deze vastlegging kan op zichzelf een inbreuk betekenen op de privacy, maar heeft tot gevolg dat er grote verzamelingen ontstaan van zeer waardevolle informatie. Het ongewild uitlekken daarvan maakt de eigenaren van de informatie kwetsbaar voor dreigingen als identiteitsfraude.

> 5.1.1 Onvoldoende aandacht voor beveiliging

Goede beveiliging van informatie is voor vrijwel elke organisatie van direct belang voor de bedrijfsvoering. Om organisatiebreed informatie op een adequate wijze te beschermen is een gecoördineerde aanpak van security-activiteiten (security management) van essentieel belang. Hieronder vallen bijvoorbeeld risicomanagement, informatieclassificatie en een samenhangend informatiebeveiligingsbeleid. Uit de praktijk blijkt vaak dat security management pas echt effectief is, als de top van een organisatie het belang ervan onderschrijft.

Daarnaast moet er actief voor gezorgd worden dat het beleid niet slechts op papier bestaat, maar ook in praktijk gebracht wordt. Idealiter leidt dit tot een situatie waarin een organisatie bewust risico's afweegt en deze ofwel accepteert, afwendt of zo nodig maatregelen neemt om ze te verkleinen.

Het beeld dat nu vooral ontstaat, is dat sommige organisaties, zowel dienstaanbieders als afnemers, pas actie ondernemen als gesignaleerde kwetsbaarheden media-aandacht ontvangen. Voorbeelden hiervan zijn de beveiliging van voicemailboxen tegen caller-ID spoofing [38] en lekke websites waarover geschreven werd in het kader van Lektober. Deze incidenten hebben uiteindelijk (mede) gefungeerd als motivatie om stappen te nemen om beveiligingsproblemen op te lossen. Hierdoor lijkt het alsof er vooraf geen bewuste afweging is gemaakt van de potentiële risico's die gepaard gaan met het negeren van kwetsbaarheden. Kwetsbaarheden waarover partijen geïnformeerd zijn of waarvoor oplossingen beschikbaar en bekend zijn. Dit geeft over het geheel een beeld weer van onvoldoende aandacht voor informatiebeveiliging. Dit beeld is in sommige gevallen herkenbaar, maar zeker niet algemeen van toepassing – organisaties die het wel goed doen, en incidenten die niet gebeuren, halen nooit het nieuws.

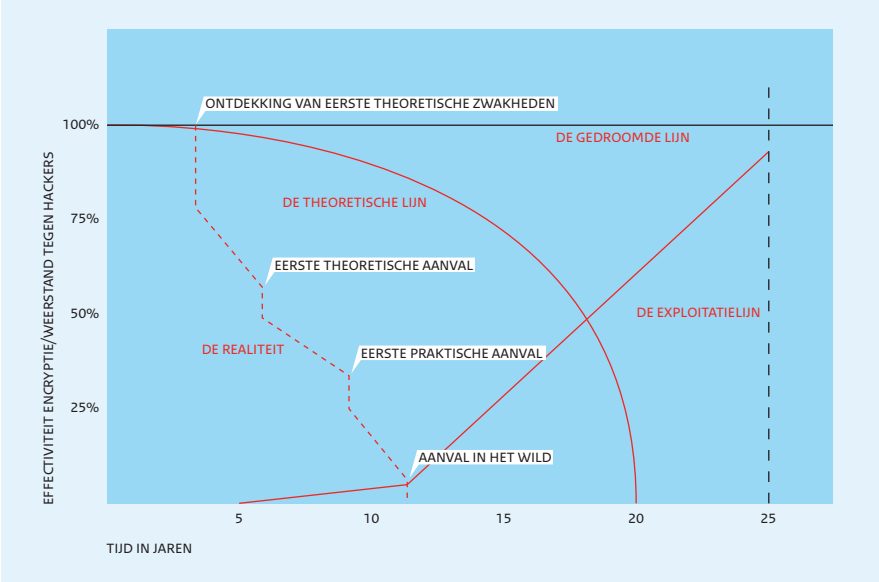
[38] Voor achtergrondinformatie zie GOVCERT.NL (2011).

> 5.1.2 Onvoldoende herijking van verouderde versleutelingstechnieken

Versleutelingstechnieken spelen een belangrijke rol bij het garanderen van integriteit en vertrouwelijkheid van waardevolle informatie. Deze technieken verouderen echter onder invloed van twee factoren. Ten eerste zorgt toenemende rekenkracht van computers ervoor dat elke versleutelingstechniek op termijn uiteindelijk simpelweg 'door te rekenen' zal zijn. Ten tweede bevatten de technieken altijd onvolkomenheden, die door aanvallers misbruikt kunnen worden. Elke versleutelingstechniek zal dus op termijn vervangen moeten worden voordat deze te zeer verouderd is en onvoldoende bescherming biedt. Dit gebeurt in de praktijk niet altijd voldoende. In de Verenigde Staten is hieruit lering getrokken. Al vele jaren bestaan daar richtlijnen voor het gebruik van versleuteling: welke technieken gebruik je voor welke informatie en op welke termijn moet de techniek worden vervangen door een modernere variant.

In figuur 4 is schematisch de veroudering van versleutelingstechnieken weergegeven. Versleutelingstechniek wordt vaak ingezet als oplossing die je implementeert en daarna vergeet. Dit is in de figuur de gedroomde lijn. Elke techniek veroudert echter onder invloed van toenemende rekenkracht. De theoretische lijn in de figuur geeft deze afnemende effectiviteit van versleuteling door de tijd heen weer.

De realiteit is echter nog complexer. Onderzoekers en aanvallers zoeken onvolkomenheden in een techniek en proberen te achterhalen hoe de techniek daarmee doorbroken kan worden. Uiteindelijk resulteert dat in echte aanvallen in gecontroleerde omstandigheden, gevolgd door daadwerkelijke aanvallen in de praktijk. Vanaf het moment dat aanvalsmethoden publiek bekend zijn, is te verwachten dat misbruik sterk groeit (de exploitatielijn).



Figuur 4. Levensduur van encryptie-algoritmen

In tabel 6 is globaal aangegeven waar bepaalde technieken zich momenteel bevinden. Dit betekent dus dat technieken die zich in de onderste groep bevinden, voor veel doeleinden onvoldoende beveiliging bieden.

Staat techniek	Techniek (toepassing)
Eerste theoretische zwakheden	- KASUMI (3G, UMTS Telefonie) - WPA2 - AES 128 (Wifi)
Eerste theoretische aanval	- SHA-2 (o.a. SSL-certificaten)
Eerste praktische aanval	- WPA2 - TKIP (Wifi) - SHA-1 (o.a. SSL-certificaten) - SSL3.0 / TLS 1.0 (beveiligde verbindingen)
Aanval in het wild	- A5/1 (gsm telefonie) - DECT (telefonie)
Cryptografiekerkhof	- MD5 (SSL-certificaten) - Mifare classic (ov-chipkaart, toegangspassen) - Content Scrambling System (dvd) - WEP (Wifi) - DES

Tabel 6. Huidige staat van versleutelingstechnieken (bij benadering)

5.1.2.1 *Een voorbeeld: verouderd gsm-protocol kwetsbaar voor afluisteren*

De versleuteling in het huidige gsm-protocol is een voorbeeld van de hierboven beschreven veroudering van versleutelingstechnieken. Dit voorbeeld geeft ook aan hoe complex het kan zijn om protocollen te vervangen. De laatste jaren zijn er meerdere kwetsbaarheden bekend geworden in het nog steeds meest gebruikte gsm-protocol (2G) dat gebruikt wordt door mobiele telefoons. De tot nu toe bekendste kwetsbaarheid werd aangetoond door Karsten Nohl. Hij heeft eind december 2010 live laten zien dat hij in staat is om met afluisterapparatuur van enkele tientjes een versleuteld gesprek op te vangen, te ontsleutelen en af te spelen.[39]
De software die hiervoor ontwikkeld is, is grotendeels publiekelijk beschikbaar op internet. Op dit moment biedt de versleuteling in het 2G gsm-protocol feitelijk geen bescherming meer tegen het afluisteren van gesprekken door een aanvaller met enige kennis van zaken.

Een aantal telecomoperators is begonnen met het nemen van maatregelen. Het gaat echter om verouderde technologie en de kosten van aanpassingen zijn hoog, waardoor er weinig animo is om maatregelen voor gsm te nemen. De kosten komen terug in vervanging of aanpassing van de infrastructuur van de operators zelf, maar ook in mogelijke vervanging van telefoons en sim-kaarten.
Inmiddels komen ook de eerste kwetsbaarheden in het mobiel internetprotocol GPRS aan het licht.[40]
Net als bij gsm vormen ook hierbij verouderde versleutelingsprotocollen en configuratiefouten een zwakke schakel. Een praktische aanval zoals bij gsm is nog niet getoond, maar is binnenkort wel te verwachten.

Een nieuw risico is het gebruik van zogenaamde femtocellen door mobiele providers. Dit zijn kleine UMTS-zenders die bij klanten thuis of in kantoren worden geplaatst om de mobiele dekking te verbeteren. In Groot-Brittannië wisten hackers via een lek in een specifiek type femtocell onder meer het sleutelmateriaal van de klanten van de telecomprovider te achterhalen.[41] Door kwetsbaarheden in dergelijke apparatuur kunnen aanvallen op de mobiele netwerkprovider worden uitgevoerd.

> 5.1.3 Gedetailleerde vastlegging en verwerking van privacygevoelige informatie

Het op grote schaal verzamelen en gedetailleerd opslaan van privacygevoelige informatie, in het bijzonder persoonsgegevens, is een kwetsbaarheid die misbruikt wordt voor in ieder geval een tweetal dreigingen: *digitale identiteitsfraude* en *publicatie van persoonsgegevens of gevoelige informatie*. Het palet aan privacygevoelige informatie dat verzameld en opgeslagen wordt, is uiteenlopend. Voorbeelden zijn: surfgedrag dat wordt opgeslagen om profielen te vormen die gebruikt kunnen worden voor gerichte reclame, en locatiegegevens van smartphones die worden verzameld en verstuurd naar de fabrikant. Maar ook persoonsgegevens die voor de interne bedrijfsvoering worden gebruikt, kunnen hieronder vallen. Zo vindt in de Verenigde Staten al meerdere jaren een

39 GOVCERT.NL heeft in december 2009 al gewaarschuwd voor deze aanval, zie GOVCERT.NL (2009).
40 Nohl & Melette (2011).
41 The Hacker's Choice (THC) (2011).

beweging plaats om het gebruik van *social security numbers* voor interne bedrijfsvoering zoveel mogelijk te beperken, in zowel de publieke als de private sector.

In de eerste maanden van 2011 was er veel aandacht voor de privacyaspecten rondom het volgen van het surfgedrag van gebruikers. Ongeacht het doel van het volgen van het surfgedrag (analyse of advertenties), is het resultaat hetzelfde: de organisatie die het gedrag volgt (we noemen deze organisaties voor het gemak 'profielbeheerders'), krijgt een duidelijk en gedetailleerd beeld van gebruikers. Wanneer meerdere websites gebruikmaken van dezelfde profielbeheerder, is deze zelfs in staat om het gedrag van één gebruiker over meerdere (vaak duizenden) websites te volgen. Een veel gebruikt mechanisme voor het ondersteunen van profielen zijn cookies.

Analysemechanisme	Aantal websites
Google Analytics	77
SiteStat	46
Omniture / 2o7	12
IlseMedia	8
NedStat	7
Yahoo! Web Analytics	4
Xiti	4
AddThis	3
Overigen (23 mechanismen)	30

Tabel 7. Meest gebruikte analysemechanismen in de top 100 van Nederlandse websites

Uit onderzoek van de homepages van de Nederlandse top 100 websites blijkt dat op 59% van de websites advertenties staan en op 92% van de websites het gebruikersgedrag geanalyseerd wordt via een externe website. Sommige websites maken zelfs gebruik van meerdere advertentie- of analysewebsites. De tabellen 7 en 8 geven de meest voorkomende analysemechanismen en advertentieaanbieders in de top 100 van Nederlandse websites weer.

Advertentieaanbieder	Aantal websites
Google Ad Services	16
Google Syndication	10
CDN WebAds	10
MediaPlex	6
RevSci	5
AdMeta	4
TradeDoubler	3
Ligatus	3
Overigen (24 aanbieders)	32

Tabel 8. Meest gebruikte advertentieaanbieders in de top 100 van Nederlandse websites

De keerzijde is dat deze informatie een belangrijke en soms de enige inkomstenbron vormt voor dienstverleners en dat sommige gebruikers het daaruit resulterende gerichte adverteren op prijs stellen.

Do-not-track functionaliteit in browsers
Nieuwe versies van browsers ondersteunen de zogenoemde 'do-not-track'-functionaliteit (DNT). Do-not-track betekent dat de gebruiker kan aangeven dat hij niet wil dat de website die hij bezoekt zijn surfgedrag volgt. In de browser kan de gebruiker een lijst met websites opgeven waarvan hij niet wil dat deze het surfgedrag in kaart brengen. Elke keer als de browser een dergelijke website opent, voegt de browser automatisch een kenmerk in ('DNT: 1') waardoor deze website weet dat de gebruiker niet gediend is van 'tracking'.

Er zijn voor eindgebruikers verschillende mogelijkheden om het volgen van surfgedrag tegen te gaan. Een voorbeeld van een maatregel is de do-not-track-functionaliteit in browsers (zie kader). De Europese Unie heeft in november 2009 de 'e-privacy richtlijn' (2009/136/EG) verder aangescherpt, waardoor de privacy van gebruikers juridisch gezien beter is beschermd.[42] Het is voor websites niet verplicht om de do-not-track-optie te volgen. Daarnaast zijn er andere mechanismen in browsers, waarmee gebruikers gevolgd kunnen worden die moeilijk te detecteren en te verwijderen zijn.

> 5.2 Technische factoren

> 5.2.1 Kwetsbaarheden van soft- en hardware

Nog steeds is de gebrekkige kwaliteit van software een belangrijke kwetsbaarheid. Zowel bij het ontwerp, de implementatie en configuratie worden fouten gemaakt waardoor aanvallers de mogelijkheid krijgen binnen te dringen in systemen. Belangrijke oorzaken van fouten zijn het niet duidelijk specificeren van beveiligingseisen, het ontbreken van beveiligingsexpertise, zowel aan de kant van de uitvoerder als bij de opdrachtgever, en het niet goed toezien op de invulling en testen van de beveiligingseisen. Dit zijn feitelijke organisatorische oorzaken, die gevolgen hebben voor de techniek. Hoewel kwetsbaarheden in soft- en hardware altijd zullen blijven bestaan, en streven naar perfectie een onrealistisch gegeven is, verdient veiligheid van software desondanks aandacht.

> 5.2.1.1 *Kwetsbaarheden in websites en standaardsoftware*

Bij websites wordt vaak op basis van standaardsoftware een specifieke webapplicatie gebouwd. Nog steeds worden onveilige websites opgeleverd en dit leidt geregeld tot datalekken of erger, zowel in het bedrijfsleven als bij de overheid. Dit wordt uitgebreid beschreven in 3.2.2 en 3.2.3. Begin juni werd bekend dat de website van de Dienst Uitvoering Onderwijs (DUO, voorheen de IB-groep) onvoldoende beveiligd was, waardoor derden uit naam van DUO gegevens van bezoekers hadden kunnen vragen en verzamelen.[43] Dit laatste is zeer relevant omdat er een reële dreiging is van phishen uit naam van de overheid, bijvoorbeeld om achter DigiD-gegevens te komen. Sindsdien zijn er nog enkele opvallende lekken geopenbaard.

Webwereld heeft de maand oktober 2011 uitgeroepen tot 'lektober' en daarbij aangegeven elke dag van deze maand een ICT-privacylek te onthullen in een dienst of website.[44] Webwereld heeft daarbij aangegeven verantwoordelijk om te gaan met de onthullingen en de getroffen organisaties vooraf in te lichten.

Recent Amerikaans onderzoek heeft enig inzicht gegeven in de staat van beveiliging van websites.[45] Het is gebleken dat 80% van de onderzochte websites kwetsbaar waren voor de tien belangrijkste beveiligingsrisico's voor websites.[46] Uit de resultaten kan worden geconcludeerd dat deze websites daarmee ook niet voldoen aan de normen die gelden voor de betalingsindustrie.[47] Opvallend hierbij was dat ontwikkelaars van beveiligingsproducten en -diensten het veel slechter deden dan gemiddeld.

---

42 'De lidstaten dragen zorg voor dat de opslag van informatie of het verkrijgen van toegang tot informatie die reeds is opgeslagen in de eindapparatuur van een abonnee of gebruiker, alleen is toegestaan op voorwaarde dat de betrokken abonnee of gebruiker toestemming heeft verleend, na te zijn voorzien van duidelijke en volledige informatie overeenkomstig Richtlijn 95/46/EG, onder meer over de doeleinden van de verwerking.'

43 'Hacker ontdekt gat in website DUO' (2011).

44 Van der Meijs (2011).

45 Veracode (2011).

46 De OWASP top 10 (zie OWASP 2010) is de de facto standaard binnen de softwarewereld waarin de belangrijkste risico's voor websites worden beschreven.

47 De OWASP top 10, die door de onderzoekers is gebruikt, wordt ook toegepast door de PCI-council in de beveiligingsstandaard voor de betalingsindustrie.

Voor een aantal van de datalekken die de afgelopen periode hebben plaatsgevonden, hebben aanvallers gebruikgemaakt van SQL-injection. Terwijl de kwetsbaarheid voor SQL-injection al enige tijd bekend is en de middelen bestaan om deze kwetsbaarheid te verhelpen, wordt duidelijk uit de incidenten dat dit bij meerdere websites nog niet heeft plaatsgevonden. Deze kwetsbaarheid in het bijzonder wordt misbruikt door hacktivisten voor het bemachtigen en vervolgens lekken van data.

Bij standaardsoftware is de situatie iets anders. De laatste jaren was al een trend zichtbaar van stabilisatie van het aantal nieuwe kwetsbaarheden dat in software werd gevonden. In 2010 is voor het eerst sinds lange tijd het aantal nieuw gemelde kwetsbaarheden significant gedaald naar 4365 (van 5535 kwetsbaarheden in software in 2009). Dit is mogelijk een gevolg van toegenomen aandacht voor beveiliging tijdens het ontwikkelen van software, maar kan ook een gevolg zijn van een bepaald aantal kwetsbaarheden dat wel bekend is in kleine kring, maar niet publiek wordt gemaakt. Toch worden er nog elke dag 12 nieuwe kwetsbaarheden bekendgemaakt. Ondanks een daling van het aantal nieuwe kwetsbaarheden zijn en blijven computers en netwerken dus nog steeds kwetsbaar.

Leveranciers brengen verbeteringen (patches) uit voor de software die specifieke kwetsbaarheden kunnen oplossen. Gebruikers van de software moeten patches daarna installeren om de kwetsbaarheid in hun eigen installatie te verhelpen. Patchen is een van de belangrijkste maatregelen die individuele organisaties kunnen nemen om de eigen weerbaarheid te verhogen. Dit patchen is vaak nog geen geautomatiseerd proces, waardoor het gevoelig is voor verstoring of simpelweg niet gebeurt. Als gevolg daarvan blijft een deel van de computers kwetsbaar.

> 5.2.1.2 *Kwetsbaarheden in industriële systemen*

Stuxnet heeft aangetoond dat een complexe aanval op procesbesturing realiteit is geworden. De aanwezigheid en de toename van ICS-kwetsbaarheden is een significante bouwsteen waar kwaadwillenden misbruik van kunnen maken. In de eerste helft van 2011 is een aanzienlijk aantal kwetsbaarheden bekendgemaakt in software voor ICS, veelal in gebruik in vitale sectoren, zoals de energie- en watersector.

Kwetsbaarheden in ICS-software bieden extra mogelijkheden voor aanvallen op de vitale sector, naast kwetsbaarheden in standaardsoftware. Procesbesturing in de vitale sectoren kan worden overgenomen of informatie kan worden gemanipuleerd. De bekende Stuxnet-worm had dit tot doel.

In een aantal gevallen werd niet alleen de kwetsbaarheid bekendgemaakt, maar ook de exploitcode, de manier waarop de kwetsbaarheid misbruikt kan worden. In meerdere gevallen gebeurde de onthulling zonder afstemming met de leverancier van het betreffende product. Uit ervaringen met standaardsoftware is bekend dat een dergelijke manier van onthullen de kans op misbruik aanzienlijk vergroot. Zolang er geen oplossing voor de kwetsbaarheden is, is de betreffende software die in gebruik is, ook daadwerkelijk kwetsbaar. Dit kan lang duren: er bestaan aanzienlijke verschillen in de snelheid waarmee softwareleveranciers oplossingen voor kwetsbaarheden uitbrengen. Van een aantal is bekend dat zij de gepubliceerde kwetsbaarheden soms al binnen een maand hebben opgelost, maar voor een gedeelte van de betreffende producten is nog steeds geen oplossing. Deze producten zijn dan ook nog steeds kwetsbaar.

Kwetsbaarheden kunnen daardoor blijven bestaan, terwijl een oplossing al voorhanden is. Voor de aanpak en coördinatie van enkele van deze problemen is in de Verenigde Staten in 2010 een specifieke organisatie opgericht: ICS-CERT.[48]

In vergelijking met 2010 is het aantal ontdekte en gepubliceerde kwetsbaarheden in 2011 tot nu toe (tot augustus 2011) spectaculair gestegen. ICS-CERT meldde in heel 2010 20 kwetsbaarheden in ICS-software. Tot augustus 2011 waren dit er al circa 60. Verder zijn in de CVE-database over 2010 circa 12 ICS-gerelateerde kwetsbaarheden opgenomen.[49] Tot aan augustus 2011 zijn al 33 nieuwe kwetsbaarheden toegevoegd. Beide bronnen laten dus een sterke groei zien in het aantal ontdekte kwetsbaarheden. Een ontwikkeling die in het trendrapport voorzien werd. Maar niet alleen het publiceren van kwetsbaarheden neemt toe, ook verschijnen er tools die het gebruik van de kwetsbaarheden eenvoudiger maken.[50]

---

[48] ICS-CERT staat voor Industrial Control Systems Computer Emergency Response Team, een door de Amerikaanse overheid in 2010 opgerichte organisatie die zich specifiek richt op (preventie van) incidenten in de industrie en de daarin gebruikte specialistische systemen.

[49] De CVE-database is een genummerde lijst van alle gemelde ICT-kwetsbaarheden wereldwijd.

[50] Recent verscheen er een update van het 'scada exploit tool ' agora pack. Zie voor meer info ICS-CERT (2011).

> 5.2.2 Zwakheden in infrastructurele protocollen van internet

> 5.2.2.1 *Kwetsbaarheden in het PKI-stelsel*

De effecten die het DigiNotar-incident in Nederland en in de rest van de wereld teweeg heeft gebracht, zijn symptomen van de wijze waarop het wereldwijde certificatensysteem werkt. Het certificatensysteem is bedoeld om (onder andere) de identiteit van websites te kunnen vaststellen en elektronische handtekeningen te kunnen zetten. Wereldwijd zijn er zo'n 600 vertrouwde partijen aangewezen die de bevoegdheid hebben om de identiteit van een website vast te stellen en deze te koppelen aan een certificaat. Als een van deze partijen zegt dat een bepaald certificaat klopt, dan nemen alle internetgebruikers ter wereld aan dat dit klopt. Nu is de afgelopen tijd gebleken dat er bij een van die 600 partijen wel eens iets fout kan gaan en daarmee wankelt feitelijk het gehele systeem. Het gehele systeem is namelijk gebaseerd op vertrouwen, in dezelfde mate, in alle vertrouwde partijen wereldwijd.

In het geval van DigiNotar is gebleken dat bij een Nederlandse partij frauduleus certificaten zijn gemaakt voor websites in het buitenland. Maar evenzogoed kunnen bij alle andere certificaatuitgevers, elders ter wereld, certificaten worden uitgegeven voor Nederlandse websites, waaronder websites van banken, van andere bedrijven, van overheden, enz. Dit kan ook als de betreffende website zelf al een certificaat heeft. Of een dergelijk frauduleus verkregen certificaat ergens voor kwaadaardige doeleinden wordt ingezet, is bijna niet te achterhalen. Soms merkt iemand het op, zoals in het geval van het Google-certificaat in Iran. De overgrote meerderheid van gebruikers is niet eenvoudig in staat om de juistheid en daarmee de betrouwbaarheid van een certificaat te controleren.

Betere controle bij Nederlandse certificaatuitgevers in Nederland kan op korte termijn meer zekerheid geven over de betrouwbaarheid van Nederlandse partijen. Dit heeft echter geen invloed op de mogelijkheid dat buitenlandse certificaatuitgevers ook (frauduleuze) certificaten kunnen uitgeven voor Nederlandse domeinen. Overigens heeft een aanvaller naast een certificaat ook toegang nodig tot het verkeer tussen bezoeker en de betreffende website om een aanval te doen slagen. Dit is op verschillende manieren te bereiken: door verkeer om te leiden, bijvoorbeeld door manipulatie van *Domain Name Servers (DNS)* of *Border Gateway Protocol-berichten (BGP)*, of door de communicatie op andere wijze te onderscheppen. Momenteel zijn er geen aanwijzingen dat er in Nederland actief misbruik wordt gemaakt van frauduleuze certificaten.

Het structureel verhelpen van deze kwetsbaarheid is complex en vereist internationaal een wijziging van het certificatensysteem. Echte oplossingen of vervangende systemen zijn er momenteel niet, enkele mogelijke oplossingsrichtingen bevinden zich momenteel in de ideeënfase. Een alternatief is om tekortkomingen van het systeem te accepteren en op andere wijze de impact van incidenten te verkleinen.

> 5.2.2.2 *Kwetsbaarheden in routeringprotocollen*

In het Trendrapport van GOVCERT.NL van 2009 is er al uitgebreid aandacht geweest voor de kwetsbaarheden in routeringprotocollen. De kwetsbaarheden die toen zijn belicht, bestaan nog steeds en er worden maar mondjesmaat verbeteringen doorgevoerd.

Het internet is ooit ontworpen als militair netwerk, bedoeld om robuust en veerkrachtig te zijn, zodat het ook blijft werken als delen van het netwerk uitvallen. Bij het ontwerp is te weinig aandacht geschonken aan de integriteit van de informatie die nodig is om het netwerk goed te beheren, waardoor de fundamenten beperkingen op deze gebieden hebben. Doordat het gebruik van internet elk jaar intensiveert en onze afhankelijkheid ervan steeds verder toeneemt, worden deze beperkingen in de fundamenten steeds nijpender. Zo werden in enkele communicatieprotocollen zwakheden ontdekt die grote impact kunnen hebben op de betrouwbaarheid van het internet. In de media is destijds uitgebreid aandacht besteed aan deze ontdekkingen en sommige gingen zelfs zo ver om te stellen dat het internet 'stuk' was. Hoewel dit laatste zeker niet het geval is, leiden deze incidenten wel tot een belangrijke constatering: de fundamenten van het internet sluiten niet aan bij de eisen die het moderne gebruik ervan stelt.

Er is met name aandacht geweest voor kwetsbaarheden in twee protocollen (de talen die computers met elkaar spreken), die van fundamenteel belang zijn voor een goede werking van het internet: DNS en BGP. Deze protocollen zorgen ervoor dat computers elkaar op internet op een zo efficiënt mogelijke manier weten te vinden. De kwetsbaarheden in DNS en BGP vertonen overeenkomsten. Succesvolle uitbuiting van de daarin ontdekte kwetsbaarheden zou ertoe kunnen leiden dat het netwerkverkeer tussen computers wordt omgeleid, afgeluisterd of gemanipuleerd. Iemand die een verbinding probeert te maken met de website van zijn bank of van de overheid kan in zo'n geval bijvoorbeeld ongemerkt doorgestuurd worden naar een nep-website, waarna zijn inloggegevens afgegeven worden aan de internetcrimineel. De kwetsbaarheden zijn ernstig, vooral omdat ze door het fundamentele karakter van de protocollen raken aan de basis van het internet. De gevolgen ervan kunnen dan ook groot zijn. Maar toch komen deze kwetsbaarheden niet helemaal als een verrassing. Dat de genoemde protocollen kwetsbaarheden bevatten – die in de praktijk ook worden uitgebuit – is al langer bekend. In het geval van DNS is er zelfs al ruim tien jaar een veiliger alternatief (DNSSEC), maar dat wordt nog maar zelden gebruikt. Ook voor BGP zijn er alternatieven, maar die worden slechts langzaam of helemaal niet in gebruik genomen. Het probleem is dat de eigenaren van netwerken wel de kosten van deze aanpassingen dragen, maar ze hebben er zelf op de korte termijn weinig voordeel bij.

Hoewel kwetsbaarheden in DNS en BGP niet nieuw zijn, is het gemak waarmee de aanvallen kunnen worden ingezet veel groter geworden. Al vele jaren wordt ervoor gewaarschuwd dat de basisprotocollen waarop internet draait, niet veilig zijn.[51] De toegenomen afhankelijkheid van het internet, voor zowel het bedrijfsleven als de overheid, als voor de samenleving als geheel, maakt dat we deze kwetsbaarheden met grote urgentie moeten verhelpen. Gezien de omvang van het internet en de versnipperde verantwoordelijkheden is dit een moeilijke opgave.

> 5.2.2.3 *Kwetsbaarheden gerelateerd aan het nieuwe internetprotocol IPv6*

Internetadressen, noodzakelijk voor het communiceren tussen computers, zijn op dit moment praktisch op. De laatste groepen werden op 1 februari 2011 aan de vijf regionale beheerders van adressen uitgedeeld.[52] Dit vergroot de noodzaak tot het migreren naar internetadressen in een nieuw formaat en met een nieuw protocol: IPv6, de opvolger van het huidige IPv4. IPv6 lost een aantal problemen op, maar brengt ook nieuwe beveiligingsrisico's met zich mee.

[51] Bellovin (2004) & Schneider (1999).

[52] RIPE (2011).

Wat zijn IP, IPv4 en IPv6?
IP staat voor Internet Protocol. Dit is het protocol dat het mogelijk maakt dat computers op internet bereikbaar zijn en met elkaar kunnen communiceren. IPv4 is de versie van het protocol dat op dit moment in gebruik is. Het biedt ruimte aan zo'n 4,3 miljard IP-adressen. IPv6 is de opvolger die naast een aantal andere verbeteringen ruimte biedt aan een praktisch oneindig aantal IP-adressen.

De staat van IPv6 in Nederland

- Van alle netwerken in Nederland ondersteunt ongeveer 38% naast IPv4 ook IPv6. Dit is vrij hoog in vergelijking met de andere landen in Europa (gemiddeld 18%)[1].
- Internetprovider XS4All biedt IPv6 standaard aan haar klanten. In de eerste helft van dit jaar hadden 7.000 klanten dit geactiveerd en maakten ruim 4.000 klanten hier ook daadwerkelijk gebruik van[2].

[1] *http://v6asns.ripe.net/v/6?s=NL;s=_EU*
[2] *https://blog.xs4all.nl/2011/04/18/ipv6-nietsdoen-is-geen-optie/*

Ten eerste komen meer tekortkomingen in het IPv6-protocol en in IPv6-implementaties naar boven nu organisaties IPv6 vaker implementeren. IPv6-implementaties bevatten, net als andere software, fouten. Daar komt bij dat beveiligingsonderzoekers steeds meer interesse krijgen in kwetsbaarheden in IPv6, waardoor ook op dit gebied nieuwe aanvalsmethoden en tekortkomingen naar voren komen.[53]

Ten tweede is ondersteuning voor IPv6 vaak wel ingebouwd in besturingssystemen, maar nog niet in alle bovenliggende applicaties, waaronder beveiligingsprogramma's. Dit kan ertoe leiden dat een computer automatisch en ongewenst bereikbaar is via IPv6, terwijl beveiligingsprogramma's het IPv6-verkeer niet inspecteren.

Ten derde wordt na migratie naar IPv6 veel apparatuur direct vanaf internet bereikbaar die nu in de praktijk wordt afgeschermd door *Network Address Translation (NAT)*.[54] Directe toegankelijkheid geeft kwaadwillenden, meer nog dan nu, de mogelijkheid om de apparatuur op afstand over te nemen en in te zetten voor illegale doeleinden. NAT wordt breed gebruikt, zowel binnen de overheid als binnen het bedrijfsleven en de thuisgebruikers. Bij deze laatste groep gaat het daarbij om zeer diverse apparatuur. Naast gewone computers gaat het bijvoorbeeld ook om mediacenters, spelcomputers en allerlei andere consumentenapparatuur met netwerkfunctionaliteit, waarvan te verwachten valt dat het met de beveiliging ervan niet goed gesteld is.

> 5.3 Nieuwe ontwikkelingen

Nieuwe technologieën brengen nieuwe kwetsbaarheden met zich mee. Factoren die hieraan bijdragen (en die ook mede bepalen of een ontwikkeling het predicaat 'nieuw' nog steeds verdient), zijn het feit dat software – die deel uitmaakt van deze technologie – aan vrijwel geen enkele standaard of richtlijn hoeft te voldoen, de druk van de *time-to-market* waaronder leveranciers opereren, onvolwassenheid van technologieën, maar ook onbekendheid met technologieën, waardoor deze onjuist of niet optimaal worden ingezet of onverwachte bijeffecten hebben. Twee belangrijke technologieën die momenteel nog steeds in relevantie toenemen, zijn clouddiensten en mobiele platformen.

> 5.3.1 Vermindering van beheersbaarheid bij uitbesteding en cloud

Het uitbesteden of 'naar de cloud brengen' van bedrijfsprocessen of -informatie kan bepaalde risico's verminderen, maar introduceert ook nieuwe risico's bij een organisatie. Bij uitbesteding van diensten of taken kan de eindverantwoordelijkheid voor informatiebeveiliging niet uitbesteed worden. Toch heeft de klant bij cloudcomputing vrijwel geen controle over of kennis van de exacte locatie van de ICT, die zich soms in het buitenland bevindt of met anderen wordt gedeeld. Het is daardoor moeilijk te overzien of voor de bedrijfsinformatie wordt voldaan aan de privacy- en vertrouwelijkheidseisen en welk juridisch regime geldt voor incidenten of voor terbeschikkingstelling van data aan overheidsdiensten ter plaatse. Specifieke eisen aan beveiliging en beheer van standaard clouddiensten zijn nauwelijks te stellen. De mate van besturing is dan voor de individuele opdrachtgever minder groot.

Leveranciers van clouddiensten – zeker die met interessante klanten – zijn een aantrekkelijk doelwit voor diverse typen aanvallers, zoals voor cybercriminelen en statelijke actoren. Hoe meer data in huis, des te aantrekkelijker.

[53] Heuse (2011).
[54] Carter (2011).

De klant krijgt dan onbedoeld een hoger risicoprofiel door aansluiting bij een gewilde leverancier. Een treffend voorbeeld hiervan is dat NASDAQ eerder dit jaar in februari verdachte bestanden heeft aangetroffen op eigen servers.[55] NASDAQ gaf aan dat hun dienst 'Director's Desk' mogelijk getroffen was.[56] Director's Desk is een dienst gericht op bestuursleden van beursgenoteerde bedrijven. De dienst bevat bedrijfskritische, financiële gegevens en contactgegevens ten behoeve van onder andere elektronische bestuursvergaderingen.

Het uitbesteden aan de cloud kan gegevens potentieel kwetsbaar maken voor onder andere digitale spionage en publicatie van persoonsgegevens of gevoelige informatie.

> 5.3.2 De groei van mobiliteit maakt misbruik aantrekkelijker

De penetratiegraad van mobiele apparatuur is hoog en blijft toenemen. Mobiele apparatuur is een aantrekkelijk doelwit voor aanvallers: ze zijn vrijwel altijd online, bieden toegang tot een schat aan persoonlijke informatie, bieden mogelijkheden tot het afnemen van diensten en uitvoeren van financiële transacties en zijn vaak slechts in beperkte mate beveiligd. Vooral de 'app cultuur' draagt bij aan deze kwetsbaarheid en aantrekkingskracht, aangezien bepaalde apps overal bij kunnen en daardoor deuren openen voor potentieel misbruik. Hoewel het aantal bekende malwarevarianten toeneemt, zijn er momenteel slechts enkele honderden stuks malware voor mobiele platformen ten opzichte van honderdduizenden voor desktop-platformen. De verwachting is dat serieuze aanvallen gericht op mobiele apparatuur de komende jaren sterk zullen toenemen, zeker als financiële instellingen met nieuwe diensten hiervoor komen.

Verdere groei van mobiel gebruik kan mobiele platformen aantrekkelijker maken. Mobiel bankieren en betalen, bijvoorbeeld, staan in Nederland nog in de kinderschoenen. Een tweede factor die in de toekomst wellicht van invloed kan zijn, is de aankomende *end of life* van Windows XP voor de desktop. In april 2014 zal Microsoft stoppen met het verhelpen van beveiligingsproblemen op dit platform. Welk effect dit zal hebben, is moeilijk in te schatten. Enerzijds kan het aandeel van nieuwere versies van Windows, vooral Windows 7, vanaf dat moment groeien ten opzichte van XP. Qua beveiliging staat Windows 7 op een hoger niveau dan XP, waardoor thuiscomputers veiliger en de mobiele markt interessanter zou kunnen worden. Anderzijds kunnen mensen die juist niet overstappen, achterblijven met een onveiliger en dus aantrekkelijker systeem voor potentieel misbruik.

[55] Barrett (2011).
[56] Nasdaq (2011).

6

Referenties

Algemene Inlichtingen- en Veiligheidsdienst (AIVD) (2010). *Kwetsbaarheidsanalyse Spionage: Spionagerisico's en de nationale veiligheid.*

Barrett, D. (2011). 'Hackers Penetrate Nasdaq Computers.'
http://online.wsj.com/article/SB10001424052748704709304576124502351634690.html

Beidel, E. (2011). 'State Dept. Official: Terrorists Lack Cyber Skills'. *National Defense Magazine*.
www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=444

Belastingdienst (2011). 'Meldpunt Toeslagfraude.'
http://www.toeslagen.nl/particulier/actueel/2011091901_meldpunt_toeslagfraude.html

Bellivon, S. (2004). 'A Look Back at "Security Problems in the TCP/IP Protocol Suite".' *Proceeding ACSAC '04 Proceedings of the 20th Annual Computer Security Applications Conference*.
www.cs.columbia.edu/%7Esmb/papers/acsac-ipext.pdf

Benson, S. (2011). 'ASIO plugs security gap.' *The Daily Telegraph*.
http://www.dailytelegraph.com.au/asio-plugs-major-national-security-gap/story-fn6b3v4f-1226030258902

'Betalingsverkeer iDeal ondervindt hinder' (2011).
http://www.nu.nl/internet/2451236/betalingsverkeer-ideal-ondervindt-hinder.html

Borhani, A. (2011). 'Is This MITM Attack to Gmail's SSL?' Forum post.
http://www.google.co.uk/support/forum/p/gmail/thread?tid=2da6158b094b225a&hl=en

Bright, P. (2011a). 'Anonymous speaks: the inside story of the HBGary hack.'
http://arstechnica.com/tech-policy/news/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack.ars/

Bright, P. (2011b). 'Independent Iranian Hacker Claims Responsibility for Comodo Hack.' WIRED.
http://www.wired.com/threatlevel/2011/03/comodo_hack/

Carter, E. (2011). 'Securing IPv6.' http://blogs.cisco.com/security/securing-ipv6/

Clayton, M. (2010). 'Stuxnet: Ahmadinejad admits cyberweapon hit Iran nuclear program.' *Christian Science Monitor.*
http://www.csmonitor.com/USA/2010/1130/Stuxnet-Ahmadinejad-admits-cyberweapon-hit-Iran-nuclear-program

Comodo (2011). 'Comodo report of incident.'
http://www.comodo.com/Comodo-Fraud-Incident-2011-03-23.html

Coviello, A. (2011). Open letter to RSA customers. http://www.rsa.com/node.aspx?id=3872

Eeten, M.J.G. van, H. Asghari, J.M. Bauer & S. Tabatabaie (2011). *Internet Service Providers and Botnet Mitigation; A Fact-Finding Study on the Dutch Market*. Report prepared for the Netherlands Ministry of Economic Affairs, Agriculture and Innovation.

Eeten, M. van, J. Bauer, H. Asghari & S. Tabatabaie (2010). *The Role of Internet Service Providers in Botnet Mitigation: An Empirical Analysis Based on Spam Data*. STI Working Paper 2010/5. Paris: OECD.
http://www.oecd.org/officialdocuments/displaydocument/?doclanguage=en&cote=dsti/doc(2010)5.

Fisher, D. (2011). 'Alleged Comodo Hacker Posts Forged Mozilla Cert, Private Key.'
http://threatpost.com/en_us/blogs/alleged-comodo-hacker-posts-forged-mozilla-cert-private-key-032911

Fox-IT (2011). *DigiNotar Certificate Authority breach 'Operation Black Tulip.'* Interim report.

Gibson, S. (2011). 'Reverse Engineering RSA's 'Statement''.
http://steve.grc.com/2011/03/19/reverse-engineering-rsas-statement/

GOVCERT.NL (2009). *Afluisteren GSM dichterbij.* Factsheet 2009-04.

GOVCERT.NL (2010a). *Nationaal Trendrapport Cybercrime en Digitale Veiligheid 2010.*

GOVCERT.NL (2010b). *Stuxnet – een geavanceerde en gerichte aanval.* Factsheet 2010-02.

GOVCERT.NL (2011). *Kwetsbaarheden in voicemaildiensten.* Factsheet 2011-02.

'Hacker ontdekt gat in website DUO' (2011). *RTL Nieuws.*
http://www.rtl.nl/components/actueel/rtlnieuws/2011/06_juni/07/binnenland/website_duo_lek.xml

Heuse, M. (2011). Personal website. http://ip6hacking.com/

Hypponen, M. (2011). 'How We Found the File That Was Used to Hack RSA.'
http://www.f-secure.com/weblog/archives/00002226.html

ICS-CERT (2011). GLEG AGORA SCADA+ EXPLOIT PACK UPDATE 1.4. ICS-CERT Alert.
http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-11-230-01.pdf

Joint Chiefs of Staff (2006). *Information Operations.* http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf

Kehayias, A. (2011). 'Enhancements Made to Comodo's eMerchant Site Security Scanning Tool.'
http://blogs.comodo.com/it-security/data-security/the-recent-ra-compromise/en

Langley, A. (2011). Public Key Pinning.
http://www.imperialviolet.org/2011/05/04/pinning.html

Langner (2011). Company website. www.langner.com

McAfee (2010). *McAfee Threats Report: Fourth Quarter.*
http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2010.pdf

Meijs, S. van der, (2011). 'Lektober: iedere dag een privacylek op Webwereld.' *Webwereld.*
http://webwereld.nl/nieuws/108052/lektober--iedere-dag-een-privacylek-op-webwereld.html

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2011). *Brief aan Tweede Kamer over Cloud Computing.*
http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/kamerstukken/2011/04/20/kamerbrief-over-cloud-computing/kamerbrief-over-cloud-computing.pdf

Nasdaq (2011). 'Important announcement.'
http://www.nasdaq.com/includes/announcement-2-5-11.aspx

Nationaal Coördinator Terrorismebestrijding (NCTb) (2010). Jihadisten en het Internet - Update 2009
http://www.nctb.nl/Images/JihadismeUpdate2009-NL%20def_tcm91-279290.pdf

Nationale Cyber Security Strategie: Slagkracht door samenwerking (2011).

Nederlandse Vereniging van Banken (NVB) (2010). *'57 miljoen euro schade voor banken door fraude in 2010.'*
www.nvb.nl/home-nederlands/nieuws/nieuwsberichten/57-miljoen-euro-schade-voor-banken-door-fraude-in-2010.html

Nederlandse Vereniging van Banken (NVB) (2011). 'Nieuwe campagne in strijd tegen toenemende fraude.' http://www.nvb.nl/home-nederlands/dossiers/visies-en-standpunten/phishing_laat-u-niet-vangen_.html

Nohl, K. & L. Melette (2011). GPRS Intercept: *Wardriving your country.* Presentation given at Chaos Communication Camp (CCC) 2011. http://events.ccc.de/camp/2011/Fahrplan/events/4504.en.html
OWASP (2010). 'OWASP Top 10 for 2010.' http://www.owasp.org/index.php/Top_10

Peterson, D. G. (2011). *Personal website.* http://www.digitalbond.com

Programma Aanpak Cybercrime (PAC) (2011). *Evaluatie Proeftuin Internet gerelateerde Fraude.*

Pluijm, U. van der, (2011). 'Duinrell-hacker jat 80 duizend mailadressen.' *Webwereld.* http://webwereld.nl/nieuws/106823/duinrell-hacker-jat-80-duizend-mailadressen---update3.html

RIPE Network Coordination Centre (n.d.) 'FAQ: IPv4 Exhaustion.' http://www.ripe.net/internet-coordination/ipv4-exhaustion/faq

Schneider, F. B. (1999). *Trust in Cyberspace.* The National Academies Press. http://www.nap.edu/openbook.php?record_id=6161

Sony (2011). Customer Service Notification. http://www.soe.com/securityupdate

Thabet, A. (2011). 'Reversing Stuxnet's Rootkit (MRxNet) Into C++'. http://blog.amrthabet.co.cc/2011/01/reversing-stuxnets-rootkit-mrxnet-into.html

The Hacker's Choice (THC) (2011). 'The Vodafone Access Gateway / UMTS Femto cell / Vodafone Sure Signal.' http://wiki.thc.org/vodafone

United States Securities & Exchange Commission (SEC) (2011). Filing detail. http://www.sec.gov/Archives/edgar/data/790070/000119312511070159/0001193125-11-070159-index.htm

Vasco (2011). 'DigiNotar reports security incident.' *Persbericht.* http://www.vasco.com/company/press_room/news_archive/2011/news_diginotar_reports_security_incident.aspx

Veracode (2011). *State of Software Security Report: The Intractable Problem of Insecure Software.* Vol. 3.

Verkade, T. (2011). 'Massafraude met belastingtoeslagen via DigiD.' *NRC Handelsblad.* http://www.nrc.nl/nieuws/2011/09/19/massafraude-met-belastingtoeslagen-via-digid/

Winter, B. de, (2011). Lek2: 7 gemeenten kwetsbaar voor DigiD-lek. *Webwereld.* http://webwereld.nl/nieuws/108111/lek2--7-gemeenten-kwetsbaar-voor-digid-lek.html

7

Begrippenlijst

2G/3G
2G is een afkorting voor tweede generatie draadloze telefoontechnologie. Het voordeel van 2G was dat de verbindingen digitaal versleuteld werden. 3G is de opvolger van 2G, ook wel UMTS of CDMA genoemd. 3G heeft voordelen voor beveiliging en communicatiesnelheid ten opzichte van 2G.

Authenticatie
Authenticatie is het nagaan of een bewijs van identiteit van een gebruiker, computer of applicatie overeenkomt met vooraf vastgelegde echtheidskenmerken.

Bluetooth
Bluetooth is een standaard voor draadloze communicatie voor het uitwisselen van gegevens over korte afstanden, gespecificeerd door Ericsson in 1994.

Border Gateway Protocol (BGP)
Border Gateway Protocol is het belangrijkste routeringsprotocol van het internet: het definieert de manier waarop informatie over netwerkroutes tussen netwerken wordt uitgewisseld.

Bot/Botnet
Een bot is een geïnfecteerde computer die op afstand, met kwade bedoelingen, bestuurd kan worden. Een botnet is een verzameling van dergelijke geïnfecteerde computers die centraal bestuurd kunnen worden. Botnets vormen de infrastructuur voor veel vormen van internetcriminaliteit.

Card Verification Value (CVV)/ Card Verification Code (CVC)
De CVV of CVC is een beveiligingsmaatregel die fraude met credit- of debetkaarten moet tegengaan.

Cloud/Clouddiensten
Een op internet (de 'wolk') gebaseerd model voor systeemarchitectuur, waarbij vooral gebruikgemaakt wordt van *Software as a Service (SaaS)*. Afnemers en gebruikers van cloudcomputingdiensten hebben niet noodzakelijkerwijs expertise in of controle over de technologische infrastructuur in de 'cloud'.

Certificaat
(zie Secure Sockets Layer certificaat)

Certificate Authority (CA)
Een certificate authority is, in een PKI-stelsel, een organisatorisch verband dat wordt vertrouwd om certificaten te maken (genereren), toe te wijzen en in te trekken.

Common Vulnerabilities and Exposures (CVE)
CVE is een unieke gemeenschappelijke identificatie van publiekbekende informatiebeveiligingskwetsbaarheden.

Computer Emergency Response Team (CERT)
Een team dat primair tot doel heeft om incidenten te voorkomen en, wanneer deze toch optreden, adequaat op te treden om de impact ervan te beperken.

Computer Network Attack (CNA)
Het vernielen van systemen om zo het systeem zelf, de data die zich erin bevindt of de processen die ermee aangestuurd worden, te verstoren of te vernielen.

Computer Network Exploitation (CNE)
Het binnendringen van digitale systemen om zo de informatie die daarin zit of meeverstuurd wordt, te verkrijgen.

Cookie
Een cookie is informatie die door een webserver op de computer van een eindgebruiker wordt opgeslagen. Deze informatie kan bij een volgend bezoek van de eindgebruiker aan de webserver weer opgevraagd worden. Cookies kunnen worden gebruikt om gebruikersinstellingen te bewaren en ook om de gebruiker te volgen.

Data breach/datalek
Het onopzettelijk naar buiten komen van vertrouwelijke gegevens.

Denial of Service (DoS), Distributed Denial of Service (DDoS)
Denial of Service is de benaming voor een type aanval waarbij een bepaalde dienst (bijvoorbeeld een website) onbereikbaar wordt voor de gebruikelijke afnemers van de dienst. Een DoS op een website wordt vaak uitgevoerd door de website te bestoken met veel netwerkverkeer, waardoor deze onbereikbaar wordt.

DigiD
De digitale identiteit van burgers, waarmee ze zich identificeren en authenticeren op websites van de overheid. Zo weten overheidsinstellingen dat ze echt met een bepaalde burger te maken hebben.

Domain Name System (DNS)
DNS is het systeem dat internetdomeinnamen koppelt aan IP-adressen en omgekeerd. Zo staat het adres 'www.govcert.nl' bijvoorbeeld voor IP-adres '62.100.52.109'.

Do-not-track (DNT)
Een mogelijkheid die geboden wordt door moderne browsers om te voorkomen dat iemands surfgedrag via cookies door derden wordt gevolgd.

End of Life
In de softwarewereld betekent de *end of life* van een product de datum waarop een product niet langer door de leverancier als gangbare software wordt beschouwd. Als software *end of life* is, maakt de leverancier over het algemeen geen updates meer en wordt ook geen ondersteuning meer geleverd.

Europay Mastercard Visa (EMV)
Een standaard voor betaalkaartsystemen op basis van chipkaarten en chipkaartbetaal-terminals. De chipkaart vervangt kaarten met een magneetstrip die makkelijk te kopiëren zijn.

Exploit/exploitcode
Software, gegevens of opeenvolging van commando's die gebruikmaken van een kwetsbaarheid in software of hardware om onbedoeld of onverwacht gedrag daarvan te veroorzaken.

General Packet Radio Service (GPRS)
GPRS is een techniek waarmee over een bestaand gsm-netwerk mobiele data verstuurd kan worden.

Global Positioning System (GPS)
Een plaatsbepalingssysteem op basis van satellieten tot op enkele meters nauwkeurig. Gps wordt onder andere gebruikt voor navigatie.

Global System for Mobile Communications (GSM)
Gsm is een standaard voor digitale mobiele telefonie. Gsm wordt beschouwd als de tweede generatie mobiele telefoontechnologie (2G).

Hacker
De meest gangbare en de in dit document gehanteerde betekenis van hacker is iemand die met kwaadaardige bedoelingen probeert in te breken in computersystemen. Oorspronkelijk werd de term hacker gebruikt voor iemand die op onconventionele wijze gebruikmaakt van techniek (waaronder software), veelal met als doel beperkingen te omzeilen of onverwachte effecten te bereiken.

HyperText Markup Language (HTML/HTML5)
HTML is een opmaaktaal voor de specificatie van documenten, voornamelijk bedoeld voor webpagina's.

Industrial Control Systems (ICS) / Supervisory Control And Data Acqusition (SCADA)
Supervisory Control And Data Acquisition, het verzamelen, doorsturen, verwerken en visualiseren van meet- en regelsignalen van verschillende machines in grote industriële procescontrolesystemen.

Identiteitsfraude
Het bewust de schijn oproepen dat een kwaadwillende de identiteit van een ander heeft die niet bij hem hoort.

Internet Protocol (IP)
Protocol dat zorgt voor adressering van datapakketten, zodat ze bij het beoogde doel aankomen.

Internet Service Provider (ISP)
Leverancier van internetdiensten, vaak simpelweg aangeduid als 'provider'. De geleverde diensten kunnen zowel betrekking hebben op de internetverbinding zelf als op de diensten die men op het internet kan gebruiken.

Kwetsbaarheid
Een zwakke plek in hardware of software, die kan worden misbruikt voor ongewenste activiteiten.

Malware
Samentrekking van 'malicious' en 'software', kortom: kwaadaardige software. Malware is de term die tegenwoordig als generieke aanduiding wordt gebruikt voor onder andere virussen, wormen en Trojaanse paarden.

Man-in-the-middle-aanval
Aanval waarbij de aanvaller zich tussen twee partijen bevindt, bijvoorbeeld een internetwinkel en een klant. Hierbij doet de aanvaller zich richting de klant voor als de winkel en andersom. Als tussenpersoon kan de aanvaller uitgewisselde gegevens afluisteren en/of manipuleren.

Meldplicht
In geval van gegevensverlies en integriteitschending van informatiesystemen moet de eigenaar van dit systeem dit melden bij de nationale toezichthouder.

Network Address Translation (NAT)
Een manier om IP-adressen te herbruiken. Een tijdelijk antwoord op het opraken van IP-adressen.
Zorgt er mede voor dat systemen buiten een organisatie niet direct bereikbaar zijn.

Open Web Application Security Project (OWASP)
OWASP is een not-for-profit wereldwijde organisatie, gericht op het verbeteren van de beveiliging van applicatiesoftware.

Patch
Een patch (letterlijk: 'pleister') kan bestaan uit reparatiesoftware of kan wijzigingen bevatten, die direct in een programma worden doorgevoerd om het desbetreffende programma te repareren of te verbeteren.

Payment Card Industry (PCI) compliance
De Payment Card Industry Data Security Standard (PCI DSS) is een informatiebeveiligingsstandaard voor organisaties die kaarthouderinformatie verwerken voor debit, credit, e-purse, GEA- en BEA-kaarten.

Personal Digital Assistant (PDA)
Een PDA is een mobiel apparaat dat functioneert als een persoonlijke informatiemanager.

Phishing
Verzamelnaam voor digitale activiteiten die tot doel hebben persoonlijke informatie aan mensen te ontfutselen. Deze persoonlijke informatie kan worden misbruikt voor bijvoorbeeld creditcardfraude, maar ook voor wat in het Engels identity theft wordt genoemd; het stelen van iemands identiteit.

Public Key Infrastructure (PKI)
Een Public Key Infrastructure is een verzameling organisatorische en technische middelen waarmee je op een betrouwbare manier een aantal zaken kunt regelen, zoals het versleutelen en ondertekenen van informatie en het vaststellen van de identiteit van een andere partij.

Remote Access
Op afstand kunnen verwerken van gegevens met een communicatieverbinding.

Rootkit
Een stuk software dat een aanvaller meer rechten op een computersysteem geeft, terwijl de aanwezigheid van deze software wordt verborgen voor het besturingssysteem.

Secure Sockets Layer (SSL)/SSL-certificaat
Een SSL-certificaat is een bestand dat fungeert als digitale identificatie van een persoon of systeem. Het bevat tevens PKI-sleutels om gegevens tijdens transport te versleutelen. Een bekende toepassing van SSL-certificaten zijn de met HTTPS beveiligde websites.

Shimmen
Een aanvalsmethode op chipkaarten, waarbij de communicatie tussen terminal en chipkaart wordt afgeluisterd en eventueel gemanipuleerd.

Skimmen
Het onrechtmatig kopiëren van de gegevens van een elektronische betaalkaart, bijvoorbeeld een pinpas of creditcard. Skimmen gaat vaak gepaard met het bemachtigen van pincodes, met als uiteindelijk doel betalingen te verrichten of geld op te nemen van de rekening van het slachtoffer.

Social engineering
Een aanvalstechniek waarbij misbruik wordt gemaakt van menselijke eigenschappen als nieuwsgierigheid, vertrouwen en hebzucht met als doel vertrouwelijke informatie te verkrijgen of het slachtoffer een bepaalde handeling te laten verrichten.

Spoofen/ IP-Spoofing
Spoofen betekent 'je voordoen als een ander', meestal in kwaadaardige zin. Bij IP-Spoofing wordt het IP-adres van een andere computer gebruikt, hetzij om de herkomst van netwerkverkeer te maskeren, hetzij om de computer daadwerkelijk als een andere computer voor te laten doen.

Tablet
Een draagbare computer waarbij het beeldscherm tevens de belangrijkste invoermogelijkheid is.

Token
Een fysiek apparaat dat een geautoriseerde gebruiker van computerdiensten helpt bij het vaststellen van de identiteit van die gebruiker.

Tweefactorauthenticatie
Een manier van authenticeren waarbij twee onafhankelijke bewijzen voor een identiteit zijn vereist. Dit bewijs kan zijn: kennis over, bezit van of biometrische eigenschappen die de identiteit van de aanvrager bewijst.

Universal Mobile Telecommunications System (UMTS)
Zie 2G/3G.

Universal Serial Bus (USB)
Specificatie van een standaard van de communicatie tussen een apparaat, in veel gevallen een computer, en randapparatuur.

Webapplicatie
De term waarmee het geheel wordt aangeduid van software, databases en systemen die betrokken zijn bij het correct functioneren van een website, waarbij de website het zichtbare gedeelte is.

Wi-Fi
Een handelsmerk van de Wi-Fi Alliance. Een apparaat met Wi-Fi kan draadloos communiceren met andere apparatuur tot op enkele honderden meters.

Zero day exploit
Een zero day exploit is een exploit die misbruik maakt van een kwetsbaarheid waarvoor nog geen patch beschikbaar is.

Colofon

Bij de totstandkoming van dit Cybersecuritybeeld Nederland is door GOVCERT.NL nauw samengewerkt met:
Algemene Inlichtingen- en Veiligheidsdienst (AIVD)
Korps Landelijke Politiediensten (KLPD)
KPN
Militaire Inlichtingen- en Veiligheidsdienst (MIVD)
Nationaal Coördinator Terrorismebestrijding (NCTb)

Vragen over de inhoud van dit Cybersecuritybeeld Nederland kunt u richten aan info@govcert.nl
of telefonisch via 070 8887555.

Dit document is gepubliceerd onder de voorwaarden beschreven in de Creative Commons Naamsvermelding-NietCommercieel-GelijkDelen 3.0 Nederland licentie:
http://www.creativecommons.org/licenses/by-nc-sa/3.0/nl/

J-10912
Uitgave december 2011

< GOVCERT.NL >
Wilhelmina van Pruisenweg 104
2595 AN Den Haag

Postbus 117
2501 CC Den Haag

Telefoon: 070 888 75 55
Fax: 070 888 75 50
E-mail: info@govcert.nl