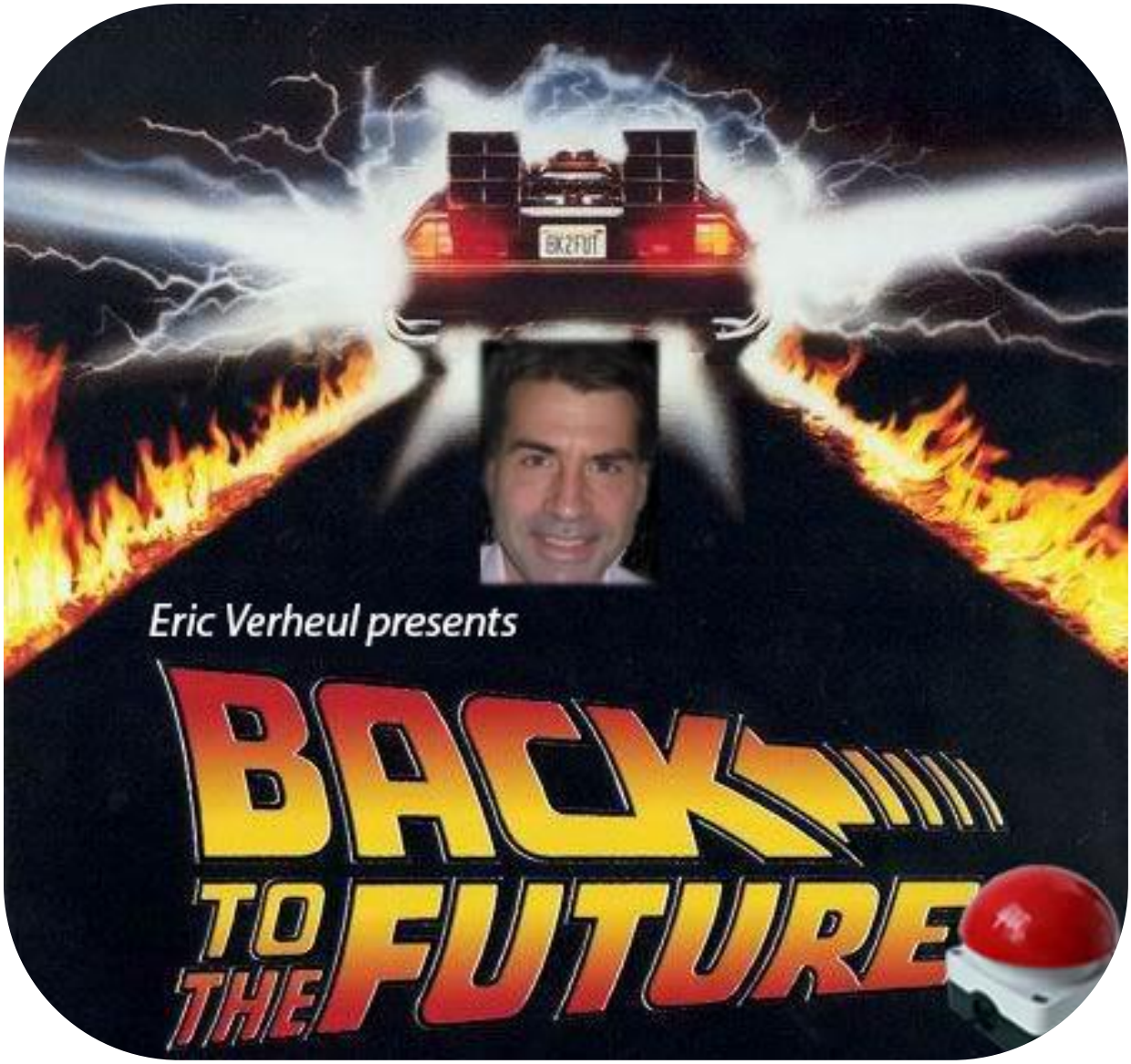
Cybersecurity: back to the future

Rede in verkorte vorm uitgesproken bij de aanvaarding van het ambt van hoogleraar aan de Faculteit der Natuurwetenschappen, Wiskunde en Informatica met als leeropdracht Financial Information Security op donderdag 30 januari 2014



Mijnheer de Rector Magnificus,

Zeer gewaardeerde toehoorders,

In deze lezing wil ik eerst in algemene zin ingaan op wat cybersecurity is. In het tweede gedeelte wil ik ingaan op wat ik beschouw als een van de zwakke plekken van cybersecurity en waar ik mij zorgen over maak. En dat is de cybersecurity van u als burger. Op dit aspect van cybersecurity wil ik mij ook richten vanuit mijn leeropdracht financial information security. Over dit onderwerp zal ik direct ook een proefballonnetje op laten gaan.

Wat is Cybersecurity en wat is het niet?

Laat ik beginnen met het definiëren van cybersecurity vanuit onze Nationale Cyber Security Strategie (cf. [1.]). Hierin wordt gesteld:

"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."

Vanuit deze definitie ontstaat het beeld dat cybersecurity toch vooral je uiterste best doen is om *alle* gevaren uit te sluiten en er zelfs vrij van te zijn. Het PDF document [1.] van de overheid waaruit ik deze definitie heb gehaald, bevestigt dit beeld.

Hierin zijn namelijk alle mogelijke PDF beveiligingsopties aangezet. Behalve een digitale handtekening dan; die zou nog enigszins op zijn plaats zijn geweest. Dit betekende dat ik deze definitie niet eens kon selecteren vanuit het document maar had moeten overtypen. Het is een mooie illustratie van zinloze, eenvoudig te verwijderen beveiliging die alleen maar ergernis geeft bij gebruikers.

Wat mist in bovenstaande definitie is de notie 'risico'. Cybersecurity is namelijk niet het vrij zijn van risico's maar het zo goed mogelijk kennen van deze risico's en deze onder controle hebben.

Acceptatie van risico's kan ook juist van voordeel zijn. Bijvoorbeeld om kosten te sparen of om gebruikersvriendelijkheid te verhogen.

Ik ken bedrijven die zo risico avers zijn dat hun medewerkers zelfs niet handsfree in de auto mogen bellen. Die bedrijven houd ik altijd gekscherend voor wat er gebeurt als er een calamiteit optreedt waarbij de medewerkers wel moeten bellen vanuit de auto. Ik stel mij zo voor dat ze allemaal in botsingen terecht komen omdat ze niet gewend zijn met het risicio om te gaan.

Ook ons eigen lichaam heeft niet als strategie gekozen om de manifestatie van risico's volledig te voorkomen (cf. [2.]). De essentie van het defensie systeem van ons lichaam is het snel kunnen signaleren en reageren op risico manifestatie en niet zo zeer op het uitsluiten daarvan. Of om met Nietzsche te spreken "Was mich nicht umbringt, macht mich stärker".

De cybersecurity uitdaging van een organisatie is dus niet het volledig uitsluiten van risico's. Het lastige van beveiligingsrisico's is de veel koppigheid van hun verschijningsvorm. Veel van mijn technische studenten hebben de gedachte dat een organisatie veilig is als er geen systemen zijn die te hacken zijn. Maar technische computerbeveiliging is maar één verschijningsvorm. Dit wordt ook geïllustreerd door de brede stroom van beveiligingsincidenten.

Om er maar eens wat te noemen. Een kwetsbaarheid kan zijn dat het management van de organisatie weinig aandacht en budget geeft aan cybersecurity of niet het goede voorbeeld geeft. Zoals bij de Britse politiechef [3.] die in 2009 met geheime plannen werd gefotografeerd op weg naar de premier. Het kan ook zijn dat een organisatie zijn fysieke beveiliging onvoldoende op orde heeft zoals bij de Rotterdamse Kunsthal in 2012 ([4.]). Of dat de organisatie zijn medewerkers onvoldoende voorziet van cybersecurity trainingen zodat ze zonder nadenken allerlei email bijlagen openen. Daarover later meer. Of dat de organisatie medewerkers toegang blijft geven tot computersystemen terwijl ze van functie zijn veranderd. Dit kostte de Franse bank Society General maar liefst 4 miljard Euro in 2012. Zie [5.], [6.].

Een organisatie kan een externe medewerker ook onbeperkt toegang geven tot zeer geheime informatie die hij in grote hoeveelheden en ongeregistreerd mee naar buiten kan nemen zoals bij het NSA in 2013 is gebleken. Wat mij overigens het meest verbaast aan de Edward Snowden affaire is de kennelijk slechte staat van cybersecurity bij het NSA. Ik denk dat hackers, ook niet mijn technische studenten, een schijn van kans maken om bij het NSA binnen te komen. Maar kennelijk heeft NSA – zoals veel andere organisaties – onvoldoende aandacht aan andere kwetsbaarheden gegeven. Zie [7.], [8.].

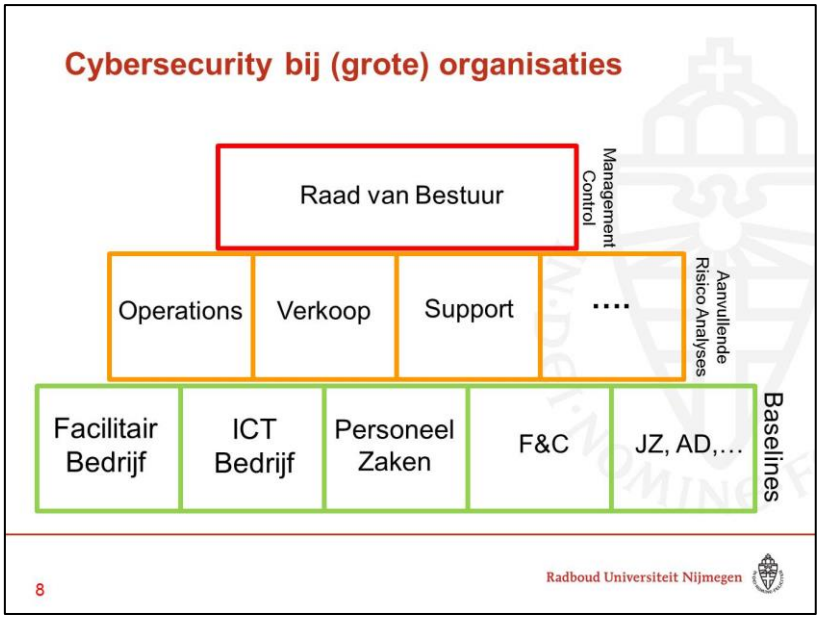
Cybersecurity bij (grote) organisaties

Met deze selectie heb ik u de veel koppigheid geïllustreerd van cybersecurity.

Zoals ik al eerder aangaf, de cybersecurity uitdaging van een organisatie is het kennen en voldoende controleren van zijn beveiligingsrisico's. Op andere terreinen zoals financiën is dit een bekend verschijnsel en maakt onderdeel uit van wat ook wel *corporate governance* wordt genoemd.

De leidende norm rond cybersecurity is ISO 27001 ([9.]). Deze norm is ook door de rijksoverheid en het College Bescherming Persoonsgegevens geadopteerd. Zie [10.] en [11.]. Binnen deze norm wordt het risico analyse proces gezien als de drijvende kracht. In andere normen worden meer richtlijnen gegeven voor het uitvoeren van dit proces. Mijn beeld is dat er soms heel gewichtig wordt gedaan over risico analyses maar dat de resultaten generiek van aard en teleurstellend zijn.

Ruwweg stel ik mij twee soorten risico analyses voor die een organisatie zou moeten voor de adressering van hun cybersecurity risico's.



Eerst een 'gezond verstand' risico analyse vanuit de ondersteunde diensten van de organisatie. Dit leidt tot een beveiligingsbaseline. Het facilitair bedrijf doet dat voor de fysieke beveiliging dus 'sloten op de deur'. ICT doet dat voor rudimentaire computerbeveiliging zoals 'wachtwoorden' en security patching. Personeel Zaken doet dat voor personele beveiliging zoals geheimhouding verklaringen en achtergrond controles. Houd het simpel en doe vooral wat je buurman ook doet. Een voorbeeld van zo'n baseline document is de Basisrichtlijn Informatiebeveiliging Rijksdienst van eind 2012 oftewel het BIR. Zie [12.].

Daar bovenop moet het lijnmanagement samen met ICT aanvullende risico analyses uitvoeren rond de bedrijfsprocessen waar zij verantwoordelijk voor zijn, inclusief de daarbij gebruikte systemen. Als de verantwoordelijkheden voor bedrijfsprocessen niet duidelijk zijn dan heeft de organisatie een heel ander probleem denk ik.

De input en de output van de risico analyses moeten daarbij aansluiten op de belevingswereld van de medewerkers in de bedrijfsprocessen. Neem daarom als input gewoon de beveiligingsincidenten die eerder of elders zijn gebeurd en als output de 'lessons learned' voor de eigen organisatie. Wat dat betreft zou ik ook iedereen aanraden het tweede rapport van Fox-IT [13.] – en niet het eerste – over het DigiNotar incident eens goed door te nemen.

Mijn overtuiging is dat een organisatie die consequent lering trekt uit beveiligingsincidenten al tot de top van de beveiligde organisaties zou behoren. In dat kader zou ik dan ook als werkdefinitie voor cybersecurity willen meegeven: "Cybersecurity is zorgen dat ernstige beveiligingsincidenten die in het verleden zijn gebeurd bij de organisatie of andere organisaties niet weer kunnen gebeuren."

Vanuit die gedachte zou het erg prettig zijn als bijvoorbeeld het Nationale Cybersecurity Centrum een inventarisatie zou bijhouden en beschikbaar stellen van beveiligingsincidenten uit de media en geanonimiseerd uit andere bronnen. Voor technische kwetsbaarheden zijn dergelijke inventarisaties

er wel maar daar die zijn niet bijzonder interessant voor het management en medewerkers in de bedrijfsprocessen.

Het is de rol van het management van de organisatie om te zorgen dat bovenstaand geschetste proces vorm wordt gegeven. Dat wil zeggen, dat de onderkende maatregelen worden geïmplementeerd, gecontroleerd en dat het management zorgt dat ze hier de greep op houdt door de juiste rapportage lijnen. Hoe dit moet, staat beschreven in de ISO 27001 norm aan de hand van een management cyclus.

Omdat het management van een organisatie meer verantwoordelijkheden heeft dan cybersecurity kan men niet verwachten dat zij zich hiermee in detailniveau bezig kunnen houden. Een security officer houdt daarom de management cyclus draaiende en deze escaleert naar het management als partijen hun verantwoordelijkheden niet nemen. En in die escalatie zit de echte management verantwoordelijkheid.

Het management moet zich in mijn visie wel met die beveiligingsdetails bezighouden die direct van levensbelang zijn voor de organisatie. En dat cybersecurity van levensbelang kan zijn voor een organisatie heeft het DigiNotar incident laten zien. DigiNotar was twee maanden na optreden van het incident failliet. Zie [14.].

Cybersecurity zaken die van direct levensbelang zijn voor de organisatie, zijn de zaken die te maken hebben met wat Advanced Persistent Threat of APT aanvallen genoemd wordt. Zie [15.]. Bij dit type aanval bezit een organisatie iets, laten we het 'kroonjuwelen' noemen, die een persistente tegenstander, heel graag wil hebben. De tegenstander is daarbij bereid veel inspanning te plegen en kosten te maken.

Een van de eerst gedocumenteerde APT aanvallen was in 2002, GhostNet, waarin – naar verluidt – de Chinese overheid informatie wilde hebben over wat de Dalai Lama in zijn schild voerde. Zie [16.]. In 2012 is een APT aanval op een financiële topman van Coca Cola bekend geworden waarbij acquisitie plannen van Coca Cola in China werden gestolen ter waarde van 2,4 miljard dollar. Zie [17.]. In beide gevallen waren de aanvallen zelf tamelijk eenvoudig. Bij Coca Cola kreeg de topman een nep email

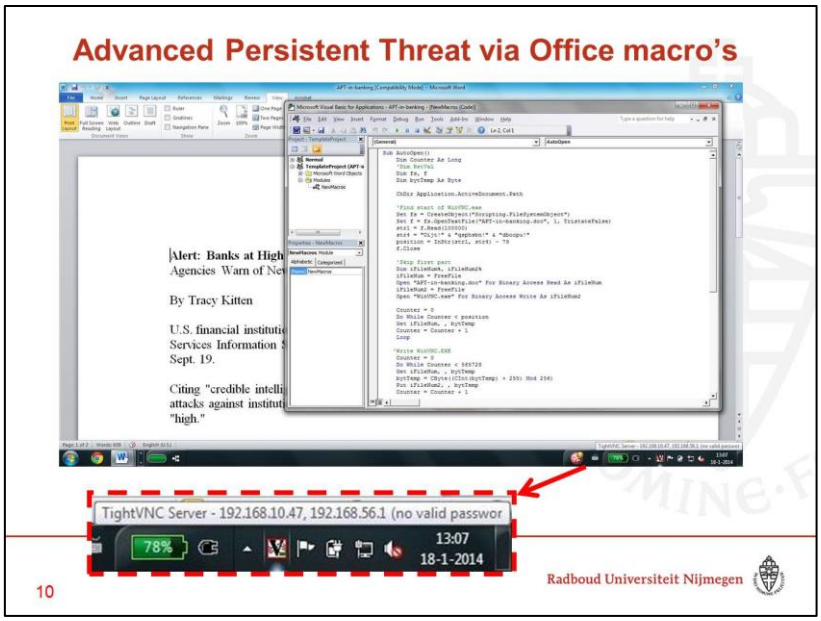
van zijn directeur en toen hij de bijlagen opende werd zijn computer overgenomen. Juist omdat de aanvallen helemaal niet zo 'advanced' zijn of hoeven te zijn is de term *Advanced* in APT eigenlijk misleidend. Waar het om gaat is de persistentie van de tegenstander. In dit verband noem ik ook het Verizon '2013 Data Breach Investigation Report' [18.]. Bij maar liefst 68% van de onderzochte computerinbraken is de initiële 'voet tussen de deur' niet technisch geavanceerd.

Op eigen bodem is het DigiNotar incident uit 2011 ook een APT voorbeeld. Een vergelijkbaar incident deed zich ook in 2011 voor bij het bedrijf RSA waar cryptografische sleutels van hun *one-time-password* tokens werden gestolen. Zie [19.], [20.], [21.]. In beide gevallen is een eerste ingang gecreëerd waarna de aanvaller zich door de netwerklagen heen heeft weten te breken tot de kroonjuwelen. Bij RSA was de eerste ingang overigens ook het openen van een email bijlage. Opmerkelijk bij beide APT aanvallen is dat de betrokken kroonjuwelen eigenlijk de kroonjuwelen van anderen waren en dat de aangevallen organisatie slechts als springplank werd gebruikt. Bij RSA waren de aanvallers uit op toegang tot Lockheed Martin die ondermeer de JSF maakt. En bij DigiNotar waren de aanvallers uit op de emails van Iraanse dissidenten. Zie [22.].

Het lijkt daarbij alsof de meeste APT aanvallen uit China komen, maar ik denk dat de aanvallers uit andere landen er gewoon wat bedrevener in zijn. Zo is in 2013 naar voren gekomen dat GCHQ (de Britse evenknie van NSA) ook een APT aanval heeft uitgevoerd op Belgacom maar dat Belgacom dit zelf niet heeft opgemerkt tot Edward Snowden dit onthulde. Zie [23.]. Het eerder genoemde Verizon rapport [18.] geeft overigens aan dat bij een ruime meerderheid van de door hen onderzochte computerinbraken de betrokken partijen daar pas na enkele maanden achter kwamen omdat een externe partij ze op de hoogte bracht.

Het is mijn overtuiging dat het management van een organisatie zich in detail blijvend zou moeten bemoeien met APT aanvallen. De vragen zijn simpel: hebben wij kroonjuwelen of die van anderen en hebben wij persistente tegenstanders die daar op uit zijn. In feite is dat gewoon een aanvulling op de aandacht die het management van organisaties nu al geeft aan mogelijke vijandige overnames van het bedrijf, de markt of het werkterrein.

Mijn beeld daarbij is dat organisaties niet optimaal hebben geleerd van de genoemde APT incidenten. Ter illustratie, sommige organisaties, en niet de minste, hebben de beveiliging van hun Microsoft Office macro's bewust verlaagd. Zie [24.].



Een macro is een geautomatiseerde opdracht in een Office document (bijvoorbeeld Excel of Word) die bij onveilige configuratie automatisch kunnen worden uitgevoerd bij opening van het document. Met onveilige macro instellingen is iedere opening van een Office document vanuit de email of internet in feite een soort Russisch roulette waardoor de eerdere incidenten bij RSA, Coca Cola en de Dalai Lama zich kunnen herhalen. Ik gaf al aan dat Verizon in zijn onderzoek constateerde dat 68% van de inbraken eenvoudig is begonnen!

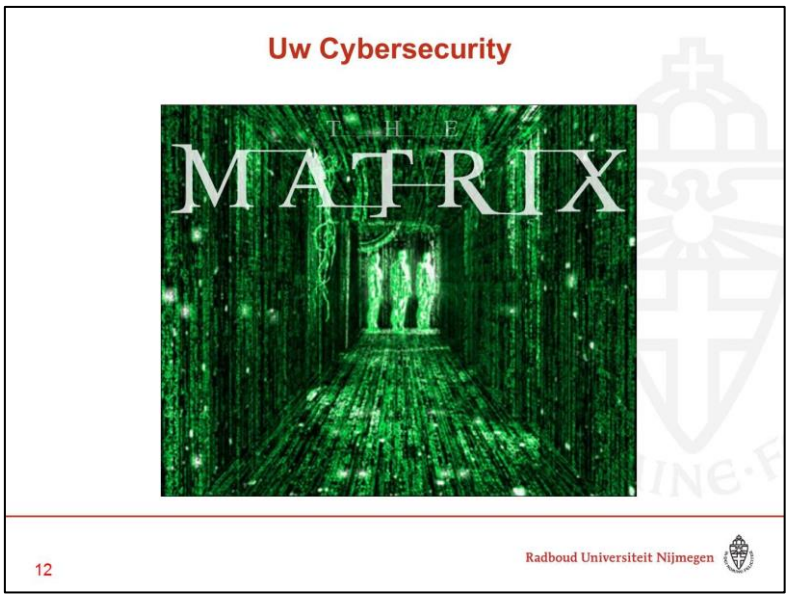
De reden voor de verlaagde Office beveiliging is dat vooral grote organisaties legacy applicaties hebben die op Office macro's zijn gebaseerd, zoals 'huisstijl' macro's. Opmerkelijk is de perceptie van dit risico. Organisaties schatten de verbonden risico's soms onterecht laag in met als argument dat er toch geen breed verspreide malware meer bestaat die hier misbruik van maakt, zoals in het verleden bijvoorbeeld het Melissa virus. De reden hiervoor is echter *juist* omdat thuisgebruikers niet aan de Office macro beveiligingsinstellingen komen zodat macro misbruik voor een *grootschalige* malware verspreider niet meer interessant is. Maar voor een persistente aanvaller die zich richt op een organisatie met onveilige Office instellingen is dit een buitenkans!

Samen met het Nationale Cyber Security Centrum heb ik hierover recent een *factsheet* ontwikkeld die vanaf vandaag van de NCSC website gedownload kan worden. Zie [24.].

En, als u toch bezig bent met Office beveiliging binnen uw organisatie dan zou ik ook gelijk navraag doen naar een ander leerpuntje uit bekende APT aanvallen: *email spoofing.* Zie [25.]. Ik kom regelmatig organisaties tegen, en niet de minste, waar het mogelijk is om vanaf het internet, interne emails te versturen. Dat wil zeggen dat het mogelijk is voor derden een email te sturen die afkomstig *lijkt* te zijn van bijvoorbeeld de directeur van de organisatie. Zoals bij Coca Cola is gebeurd en daar de start van een APT aanval vormde. U kunt het met weinig moeite gewoon zelf eens uitproberen vanuit uw thuis PC. Je kunt email spoofing overigens ook gebruiken om het probleem op te lossen. Wat ik weleens heb ik gedaan is een gespoofde email te sturen van de directeur van de organisatie naar het hoofd ICT met de vraag of die email spoofing nou eens eindelijk opgelost kon worden. Niet iedereen kon die grap waarderen, overigens.

De tijd laat niet toe om aan te geven wat een organisatie in mijn visie zou moeten doen als deze kroonjuwelen en persistente aanvallers heeft. Laat ik mij daarover beperken tot de suggestie dat de organisatie dergelijke kroonjuwelen zou moeten beschermen zoals de US Secret Service de Amerikaanse president. Daarbij worden alle mogelijke aanvalspaden constant geanalyseerd en zoveel mogelijk uitgesloten. Tijdens bezoeken van de Amerikaanse president aan Nederland werden daarom onder meer complete snelwegen afgesloten, brievenbussen verzegeld en putdeksels dichtgelast. Zie [26.], [27.]. Soms, dames en heren, is het gewoon noodzakelijk om paranoia te zijn.

Uw cybersecurity



In het tweede gedeelte van mijn lezing wil ik het over de cybersecurity hebben van u als burger.

Zonder dat we er veel erg in hebben, is de fysieke wereld aan het migreren naar de digitale wereld. Wie schrijft er nog brieven? Wie gebruikt er nog papieren overschrijvingsformulieren, papieren facturen, papieren fiscaal jaar overzichten en afgedrukte foto's? Dienstverleners denken door de inzet van het digitale kanaal te kunnen besparen op post, drukwerk en baliehandelingen. Banken zijn daarbij ook hun fysieke kantoorloketten aan het opheffen. In het regeerakkoord is de doelstelling opgenomen dat burgers in 2017 digitaal zaken met de overheid moeten kunnen doen. Zie [28.], [29.].

Veel van de zaken die vroeger fysiek in uw huis lagen, zijn nu in digitale vorm in uw computer opgeslagen. Uw computer verwordt daarmee steeds meer tot uw archiefkast en uw loket tot de wereld.

Door de afhankelijkheid van het digitale kanaal ontstaan nieuwe risico´s voor dienstverleners zoals DDOS aanvallen. De tijd laat niet toe om hier nu verder op in te gaan.

Maar door deze afhankelijkheid ontstaan ook nieuwe risico´s voor het individu. Wat opvalt, is dat we allerlei zaken in de digitale wereld doen die we nooit in de fysieke wereld zouden doen. Als we al een sleutel geven aan bijvoorbeeld een aannemer dan willen we die wel graag terug na oplevering. We zouden toch gek opkijken als de aannemer de sleutel houdt om onaangekondigd soms nog even te kijken of alles nog werkt. Toch doen we dat met onze computer wel. En vaak zijn er aannemers in onze computer aan het werk waar we helemaal niets van af weten. Ik heb weleens een weekend lang gekeken wat voor netwerk verkeer er allemaal werd opgestart vanaf mijn computer. En daaruit bleek dat er elke 30 minuten opgevraagd werd wat het weer in New York was, voor een applicatie waar ik het bestaan niet van wist.

Laten we de fysieke wereld eens in meer detail vergelijken met de digitale wereld aan de hand van beveiligingsincidenten. Als analogie van de woninginbraak neem ik besmetting van uw computer met malware. Malware is software die kwaadaardige bedoelingen heeft. Het is een wat breder begrip dan

computervirus. Anders dan een computervirus wil malware zich niet noodzakelijk verder verspreiden. Zie [30.].

Bij malware besmetting is een vreemde met kwaadwillende bedoelingen in ons *digitale* huis, in onze computer. Hierbij zal ik impliciet uitgaan van computers (laptop of desktop) gebaseerd op het Windows besturingssysteem. Beschouwt u dit alstublieft niet als kritiek op Windows beveiliging. Ik ga van Windows uit omdat dit verreweg het vaakst wordt gebruikt en mede daarom ook de meeste beveiligingsincidenten genereert.

Die vergelijking zal ik maken vanuit de volgende drie perspectieven:
1. Aantallen en schade
2. Detectie en duur van het incident, en
3. Herstel van de schade

Aantallen en schade door malware
Laat ik beginnen met aantallen en schade.

Het jaarlijkse aantal fysieke woninginbraken is volgens het CBS ongeveer 100.000 op een totaal van ongeveer 8 miljoen particuliere huishoudens. Zie [31.], [32.]. De gemiddelde directe financiële schade bij een woninginbraak wordt geschat op 1.800 Euro, dus 180 miljoen Euro op jaarbasis. Zie [33.].

Er zijn in Nederland volgens het CBS ongeveer 10 miljoen particuliere computers. Zie [34.]. Malware op onze computer biedt onbevoegden de mogelijkheid om *anderen* te schaden, bijvoorbeeld door het verder verspreiden van malware en spam. Malware biedt onbevoegden ook de mogelijkheid om de burger *zelf* te schaden, bijvoorbeeld door frauduleuze transacties te introduceren bij het internet bankieren. Malware geeft onbevoegden ook de mogelijkheid om onze persoonlijke informatie te bekijken en daar vervolgens misbruik van te maken bijvoorbeeld voor identiteitsdiefstal.

Dit werd december 2013 goed duidelijk met de aanhouding van een jongen uit Rotterdam. Zie [35.]

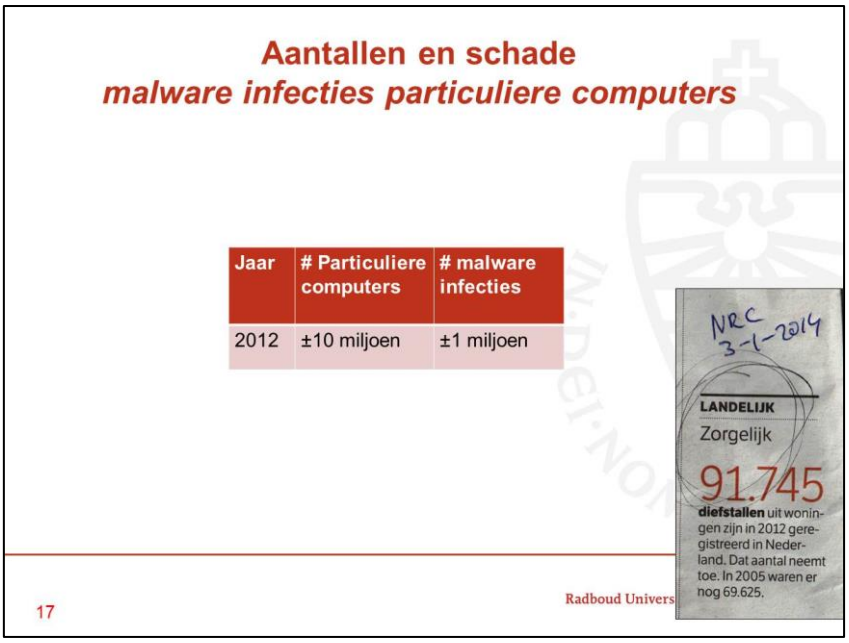
Deze jongen heeft naar verluidt twee duizend computers gehackt door de verspreiding van malware. Hij heeft niet alleen ruim 40 miljoen bestanden buitgemaakt maar hij heeft ook fotomateriaal op

websites geplaatst namens zijn slachtoffers. Ook heeft hij heimelijk filmpjes van individuen gemaakt met de ingebouwde camera's van deze computers. In 2007 is op kleinere schaal al iets dergelijks gebeurd bij de computer van RTL presentatrice Manon Thomas. Zie [36.]

Misschien is dit ook iets om aan te denken als u een nieuwe 'smartTV' gaat kopen. SmartTVs hebben tegenwoordig ook een ingebouwde camera en microfoon en internet connectiviteit. Ze hebben ook een internet browser die voor een malware besmetting kan zorgen. Malware op uw nieuwe smartTV kan dan betekenen dat derden rechtstreeks in uw huiskamer kunnen meekijken en meeluisteren. Dit wordt nog vergemakkelijkt doordat smartTVs vaak ook al over ingebouwde remote beheer mogelijkheden beschikken. Ik zou ook maar gelijk een pleister plakken over de camera van uw mooie, nieuwe smartTV.

Mijn verwachting is dat na de gerichte APT aanvallen op organisaties - waar ik eerder over vertelde - ook individuen hiervan steeds vaker het slachtoffer zullen gaan worden. Grooming, waarbij pedofielen contact leggen met kinderen via internet is ook een manifestatie van APT aanvallen op individuen. Zie [37.]. Een malware infectie op uw computer is niet onschuldig en kan grote consequenties hebben voor u en uw familie.

Schade die malware veroorzaakt is moeilijk te kwantificeren. Wat wel is te kwantificeren, is het jaarlijkse aantal malware infecties in Nederland.

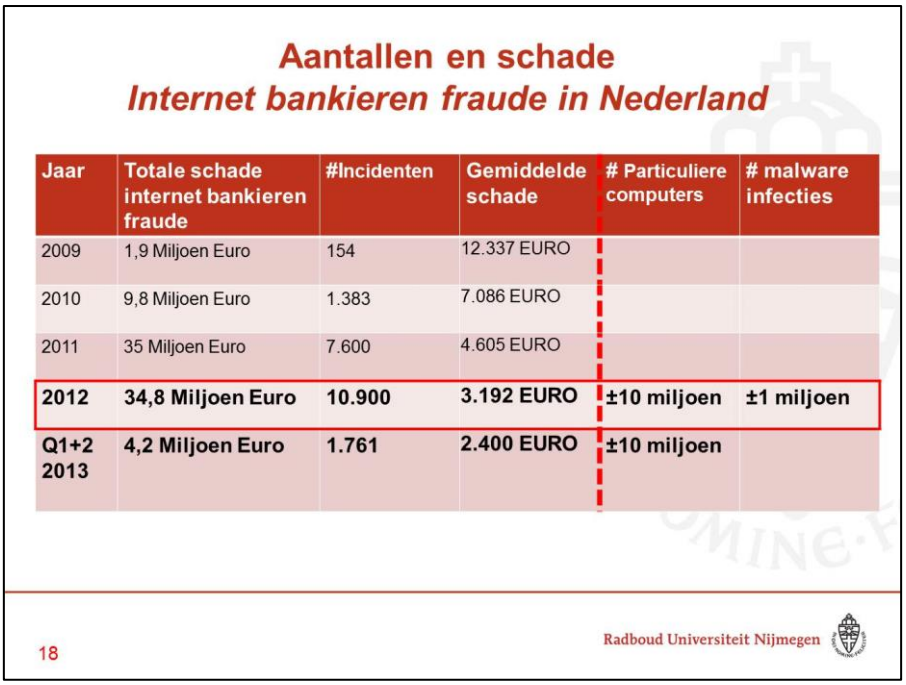


Op basis van het onderzoek van mijn Delftse collega Van Eeten schat ik het jaarlijkse malware infecties op ongeveer 1 miljoen, tien procent van het totaal aantal computers dus. Zie [38.].

Ook qua percentage zijn er dus veel meer digitale dan fysieke inbraken. In een NRC artikel van 3 januari 2014 werd het aantal fysieke inbraken al 'zorgelijk' genoemd. Zie [39]. Vanuit die gedachte is het aantal digitale inbraken dat dus al helemaal. Toch ben ik somber of we iets kunnen doen aan de aantallen malware infecties. Net zoals bij griepbesmetting, moeten we misschien gewoon leren leven met de gedachte dat onze computer soms besmet wordt. Opmerkelijk is dat het jaarlijkse griep infectie percentage ook rond de tien ligt, zie [40.].

Waar we wel iets aan kunnen doen is de signalering van en reactie op die infectie, daarover straks meer.

Laten we dan de directe financiële schade eens vergelijken tussen de fysieke en digitale inbraken. Zoals eerder gezegd, wordt de gemiddelde directe financiële schade bij een woninginbraak geschat op 1.800 Euro, dus 180 miljoen Euro op jaarbasis. Een vertaling van de directe financiële schade bij een digitale inbraak op een computer, is de schade die ontstaat middels internet bankieren fraude. Laten we daartoe de cijfers eens bekijken rond internet bankieren fraude zoals gepubliceerd door de Nederlandse Vereniging van Banken. Zie [41.].



Aantallen en schade
Internet bankieren fraude in Nederland

Jaar	Totale schade internet bankieren fraude	#Incidenten	Gemiddelde schade	# Particuliere computers	# malware infecties
2009	1,9 Miljoen Euro	154	12.337 EURO		
2010	9,8 Miljoen Euro	1.383	7.086 EURO		
2011	35 Miljoen Euro	7.600	4.605 EURO		
2012	**34,8 Miljoen Euro**	**10.900**	**3.192 EURO**	**±10 miljoen**	**±1 miljoen**
Q1+2 2013	**4,2 Miljoen Euro**	**1.761**	**2.400 EURO**	**±10 miljoen**	

18

Radboud Universiteit Nijmegen

Wat opvalt is dat de gemiddelde schade van een internet bankieren fraude incident vergelijkbaar lijkt te worden met die van woninginbraak, namelijk rond de 2.000 Euro. In absolute omvang is de schade van internet bankieren fraude minder dan 20% van die van woninginbraak. Wat ook opvalt dat het aantal incidenten, 11.000 in 2012, laag is in vergelijking met het aantal computers dat jaarlijks wordt geïnfecteerd met malware. Minder dan 1 procent van de malware infecties lijkt te leiden tot internet bankieren fraude. Deze conclusie wordt nog versterkt als men in overweging neemt dat bij een gedeelte van de internet bankieren fraude incidenten malware helemaal geen rond speelt. Waar ik op doel zijn de incidenten waarbij mensen bijvoorbeeld worden gebeld door een nep bankmedewerker en om codes worden gevraagd.

Dat het aantal frauduleuze internet bankieren transacties relatief laag is komt allereerst omdat het lastig is voor de crimineel om frauduleus overgeboekt geld in handen te krijgen. Hiervoor moeten zogenaamde geldezels worden ingezet, personen die bereid zijn om hun bankrekening te laten misbruiken. Dergelijke geldezels zijn lastig te vinden voor criminelen en dat werkt al als natuurlijke barrière bij internet bankieren fraude. Uiteindelijk is de geldezel trouwens het echte slachtoffer want daar gaat de bank naartoe om het geld terug te halen.

Dat het aantal frauduleuze transacties verder relatief laag is, komt ook omdat de Nederlandse banken de afgelopen jaren hebben geïnvesteerd in fraude detectie systemen. Zie [42.]. Een fraude detectiesysteem stelt een bank in staat om afwijkend transactie gedrag van zijn klanten te signaleren op basis van eerder transactiegedrag. Bij detectie van een dergelijke transactie kan de bank bij een hoge fraude indicatie de transactie gelijk weigeren of eerst contact zoeken met de klant over deze transactie. Het is met name die terugkoppeling met de klant die deze opzet zo effectief en gebruikersvriendelijk maakt. De Nederlandse banken publiceren helaas niet over de effectiviteit van hun fraude detectie mogelijkheden of over het percentage van frauduleuze internet bankieren transacties. In de Australische context zijn hier wel enige cijfers over bekend. Zie [43.]. Een eerste stap zou een eenduidige en vooral meetbare definitie zijn van een frauduleuze internet bankieren transactie.

Ik vat samen.

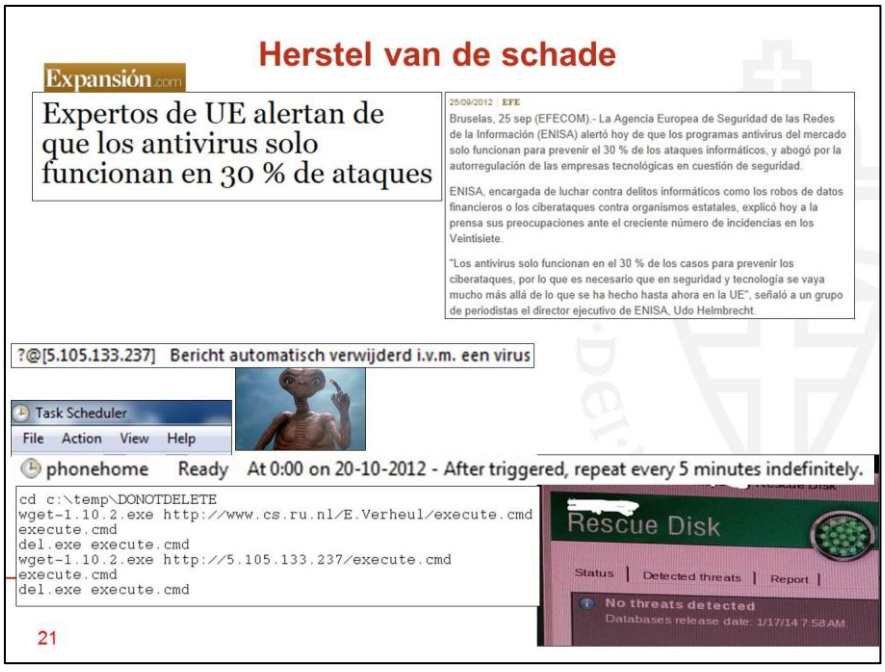
Het aantal fysieke inbraken bij de burger is 10 keer zo laag als de digitale computerinbraken. De directe financiële schade bij fysieke inbraken is echter 6 keer zo hoog als bij digitale inbraken en dus relatief veel hoger. Met de transitie van fysiek naar digitaal maak ik mij met name zorgen dat ook burgers steeds meer tegen gerichte aanvallen, APT aanvallen dus, zullen aanlopen waarbij met name hun persoonlijke levenssfeer in het geding is. Misbruik van persoonlijke informatie op computers, zoals kopieën van identiteitsdocumenten en wachtwoorden, kunnen ook leiden tot identiteitsdiefstal.

Ik wil mij nu richten op de detectie en duur van een incident en schadeherstel naar aanleiding daarvan. Ik zal beginnen met het laatste, schadeherstel.

Schadeherstel

Bij een fysieke inbraak is schadeherstel in beginsel overzichtelijk, de schade aan deuren en dergelijke moet worden hersteld. Daarbij zijn deze kosten, gemiddeld 1.200 Euro, veelal gedekt door de opstalverzekering. Schadeherstel voor de betrokkene is daarom simpel te realiseren. Zie [33.].

Laten we dit eens vergelijken met schadeherstel in de digitale situatie. Het lijkt eenvoudig om malware te verwijderen met behulp van anti-virus software. Er is echter consensus dat de prominente rol van anti-virus software voorbij is en dat we iets anders nodig hebben voor onze cybersecurity.



De directeur van het cybersecurity instituut van de Europese Unie, ENISA, heeft zich in 2012 publiekelijk laten ontvallen dat anti-virus software maar in 30 procent van de gevallen effectief is. Zie [44.]. Daar zal hij niet populair bij de anti-virus sofware industrie mee geworden zijn. Dit percentage is in lijn met andere onderzoeken die ik heb gezien en ook met het onderzoek dat studenten van mij

hebben uitgevoerd. Zie [45.], [46.]. De oorzaak daarvan is dat anti-virus software voornamelijk kijkt naar malware 'handtekeningen' en slechts beperkt naar heuristiek, naar gedrag op de computer dat wijst op malware. De malware ontwikkelaar kan daarbij zelf ook kijken of zijn malware wordt gedetecteerd. Anti-virus software kan daarbij wel worden verbeterd met heuristische mogelijkheden. Maar deze toevoeging betekent dat anti-virus software veel ingewikkelder voor gebruikers zal worden en waarbij deze ingewikkelde beslissingen zal moeten nemen. Beslissingen die ook kunnen betekenen dat diens computer niet meer werkt. En dat soort gebruikers wil je liever niet hebben bij je helpdesk.

Begrijpt u mijn alstublieft niet verkeerd. Ik roep niet op tot de afschaffing van anti-virus software, ik stel alleen dat de rol daarvan minder prominent zal zijn dan in het verleden. Wat dat betreft kunnen we een parallel trekken met de verminderde effectiviteit van penicilline bij bacteriële infecties.

Samenwerkende Duitse Internet Service Providers, ISPs, hebben het zogenaamde Botfrei intitatief opgericht dat burgers voorziet van software voor de schoning van besmette computers. Zie [47.]. Botfrei suggereert gebruikers ook om hun computer terug te zetten naar een eerdere toestand toen er nog geen malware actief was. Dat betekent dat de gebruiker regelmatig volledige backups moet maken van zijn computer. Botfrei geeft daarbij aan dat dit niet weggelegd is voor de meeste gebruikers.

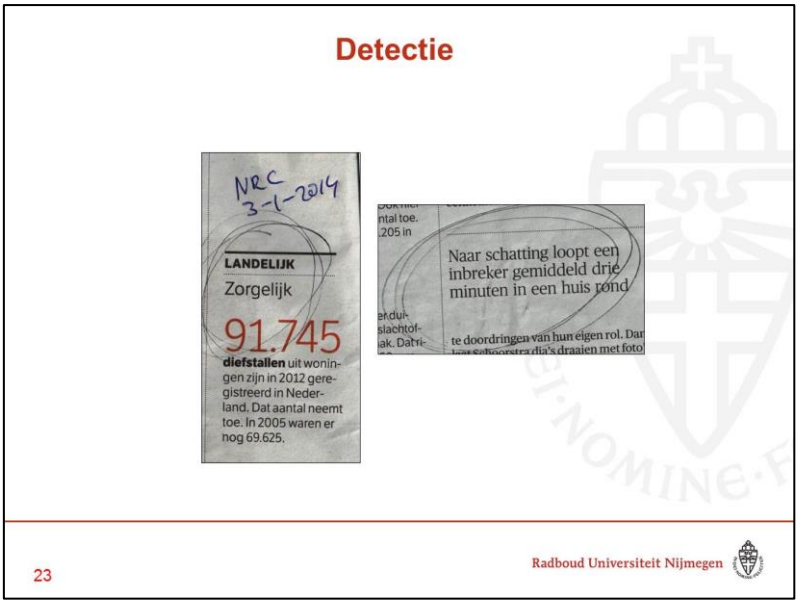
Extra complicerend van een volledige backup is dat je deze wel moet bewaren en terugzetten met behulp van een extern medium en niet met behulp van de besmette computer zelf. De malware kan zich immers nestelen in de backup data op de computer. Dat is geen denkbeeldig risico, het eerder genoemde ENISA, heeft al in 2008 malware gezien die iets dergelijks doet. Zie [48.].

Om de effectiviteit van anti-virus software zelf te testen, heb ik de volgende twee eenvoudige experimenten uitgevoerd. Ik heb een zogenaamde 'scheduled task' aangemaakt dat elke 5 minuten een scriptje van een website afhaalt en deze uitvoert. Het is de meest eenvoudige root-kit die er is. In het eerste experiment heb ik als website een persoonlijke website gebruikt. Bij het tweede experiment heb ik het adres van een kwaadaardige website gebruikt. Vanaf deze website was een paar dagen eerder getracht malware naar mij toe te sturen via email. Vervolgens heb ik de meest geavanceerde middelen toegepast van 5 vooraanstaande antivirus software leveranciers en van het Botfrei intiatief. U raadt het al, ze vonden allemaal niets. Daarmee wil ik niet zeggen dat deze middelen slecht zijn. Maar wat ik wil aangeven is dat ze gewoon voor een onmogelijke taak zijn gesteld. Misschien hadden ze wel wat gevonden als de kwaadaardige website die ik had gebruikt al op een zwarte lijst had gestaan. Maar die opzet is niet houdbaar met het voorziene gebruik van IPv6 waarbij er bij wijze spreken oneindig veel websites kunnen zijn. Zwarte lijsten zijn dan al helemaal niet meer effectief.

Ik concludeer dat als een gebruiker met zekerheid zijn besmette computer wil schonen hij deze terug zal moeten zetten naar een veilige toestand in het verleden vanaf een veilig middel. En dat is voor de meeste gebruikers op dit moment niet weggelegd.

Detectie/duur van de inbraken

Dat brengt ons op de detectie en duur van inbraken.



De gemiddelde fysieke inbraak duurt volgens een onderzoek uit 2009 niet langer dan 10 minuten. Zie [49.]. Volgens het eerdergenoemde NRC artikel [39.] is de duur zelfs maar 3 minuten. De betrokkene kan immers eenvoudig vaststellen dat er fysiek bij hem wordt of is ingebroken. Bijvoorbeeld omdat het slot is geforceerd of omdat de televisie weg is.

Hoe anders is dit bij digitale inbraken op de computer. Voor de gebruiker wordt alleen in bijzondere situaties duidelijk dat er malware actief is op zijn computer. Een bekende indicatie van malware besmetting is dat de computer steeds vreemde internet pagina's toont of dat vreemde programma's worden gestart. Een evidente indicatie is ook als de gebruiker slachtoffer is van randsomware. Daarbij is de computer geblokkeerd door malware en dit kan alleen worden opgeheven door betaling. Zie [50.].

Door combinatie van een aantal verschillende bronnen kunnen we de besmettingsduur ongeveer bepalen. Belangrijk daarbij zijn de metingen die Microsoft uitvoert met zijn anti-virus software, het Malicious Software Removal Tool oftewel MSRT. Dit is anti-virus software die onder meer elke tweede dinsdag van de maand wordt uitgevoerd door Microsoft in het kader van de Windows update service maar ook wanneer het nodig is om te reageren op acute beveiligingsproblemen. Op basis hiervan publiceert Microsoft de zogenaamde computers cleaned per mille (CCM) cijfers. Deze cijfers geven het promillage aan van de computers die zijn geschoond met MSRT. In het Microsoft Security Intelligence Report van juni 2013 [51.] wordt een CCM waarde van 3 aangegeven voor Nederland. Daaruit blijkt dus dat begin 2013 MSRT constateert dat drie op de duizend particuliere computers in Nederland besmet zijn met malware. In eerdere rapporten van Microsoft over andere tijdsperioden werd een vergelijkbaar of hoger CCM cijfer genoemd. Zie [52.].

Gecorrigeerd met de eerder genoemde effectiviteit van anti-virus software betekent dit dus dat 10 op de duizend particuliere computers in Nederland op dit moment geïnfecteerd is met malware. Of, anders gezegd, de kans dat er nu een inbreker in uw computer aanwezig is, is ongeveer één procent.

Dat getal van één procent is toch eigenlijk wel schokkend hoog te noemen. Ter vergelijking; de kans dat er nu een inbreker in een huis is, is ongeveer een honderdduizendste procent.

Het hoge getal van 1 procent is nauw verbonden met de duur van een malware infectie. Deze duur kunnen we ook inschatten met behulp van dit percentage en het totale aantal computers. Daarbij kom ik tot een besmettingsduur van 36,5 dagen, dus ruim een maand (vergelijk ook. [53.]).

En dat, dames en heren, is het grote probleem rond malware besmettingen. Niet dat we ze oplopen maar dat het zolang duurt voordat we het zien en er wat aan kunnen doen. Ik herinner u er nog aan dat de fysieke inbreker gemiddeld 3-10 minuten actief blijft.

Inschatting van de malware infectieduur
De kans van 1 procent laat zich uitdrukken als het product van de kans dat een computer in een jaar is geïnfecteerd en de kans dat dat bij een willekeurige inspectie wordt geconstateerd. Eerder is al aangegeven dat het aantal geïnfecteerde computers ongeveer 1 miljoen is op een totaal van 10 miljoen computers. Dus die eerste kans is 0.1. Die tweede kans laat zich uitdrukken als de gemiddelde infectieduur in dagen gedeeld door 365. Er volgt dat 0.1*T/365 gelijk is aan de eerder genoemde kans van 1 procent oftewel 0.01. Dan volgt dat de gemiddelde infectieduur T ingeschat kan worden met 36,5 dagen, dus ruim een maand. Merk op dat als we het jaarlijkse aantal besmette computers lager zouden inschatten dan 1 miljoen (cf. de toelichting bij [38.]) dat dan de schatting van de malware infectieduur nog groter zou zijn dan 36,5 dagen.

Inschatting kans dat in een huis wordt ingebroken
Met een vergelijkbare berekening kunnen we de kans inschatten dat er nu bij u wordt ingebroken. We gaan uit dat de gemiddelde inbraak 5 minuten duurt. Zie [39.] [49.]. Zoals eerder aangegeven, zijn er 8 miljoen particuliere huishoudens en jaarlijks 100.000 inbraken. Stel een grote matrix voor met 8 miljoen rijen die de huishoudens representeren. Verdeel elke rij in 525.600 vakjes corresponderend met het aantal minuten in een jaar. In totaal zijn er dus 8.000.000 x 525.600 vakjes. Kleur nu denkbeeldig in deze tabel die tijdvakjes rood waarin bij een bepaald huishouden (dus een bepaalde rij) wordt ingebroken. Dan zien we dus 100.000 x 5 = 500.000 rode vakjes verdeeld over de matrix. Immers, er zijn 100.000 inbraken die gemiddeld 5 minuten duren. De kans dat er nu een inbraak in een huis is, is dus de kans dat men bij willekeurig ´prikken´ in de matrix op een rood vakje stuit en die kans is:

$$\frac{500.000}{8.000.000 * 525.600} \approx 10^{-5}\%$$

Verdere analyse
Ik vat samen dat ik twee problemen heb gesignaleerd. Ten eerste hebben gebruikers onvoldoende detectie mogelijkheden; ze zien pas na ruim een maand dat hun computer is besmet. Ten tweede is het voor de gebruiker lastig om met zekerheid de computer te ontdoen van malware.

Binnen grotere organisaties worden deze problemen vaak gestructureerd opgepakt met een Security Operations Center of SOC. Zie [54.]. Een SOC monitort het netwerk verkeer op malware en biedt ondersteuning aan de gebruiker. De effectiviteit van een SOC blijkt bijvoorbeeld uit het

beveiligingsincident in juni 2013 waarbij malware via de website nu.nl werd verspreid. Dit werd als eerste door een SOC gesignaleerd. Zie [55.].

Waar ik heen wil, dames en heren, is dat er ook een burger-SOC zou moeten komen. In technische zin is zijn de middelen voor een SOC er al. De vraag is alleen *wie* de rol van de burger-SOC kan invullen. De meest voor de hand liggende partij lijkt mij de Internet Service Provider. De ISP zoals KPN, XS4ALL, UPC en Ziggo die de burger aan het internet verbindt. Zij zijn in staat, net zoals de banken dat ook al succesvol doen, om afwijkingen te zien in het surfgedrag van hun klanten die wijzen op malware besmetting.

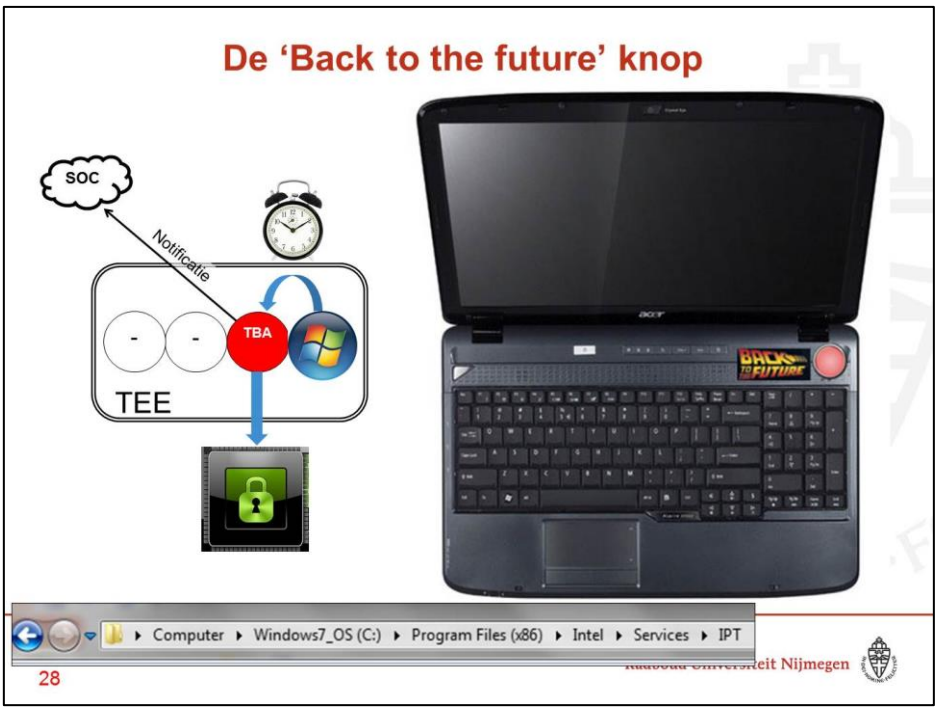
In beperkte zin vullen Nederlandse ISPs al een SOC rol in voor hun klanten. In november 2013 is daartoe in Nederland, in analogie met het Duitse Botfrei initiatief, ook de AbuseHUB opgericht door de grootste Nederlandse ISPs. AbuseHUB is een lofwaardig initiatief.

Maar uit het afgegeven AbuseHUB persbericht [56.] komt het beeld naar voren dat de ISPs zich toch vooral richten op de risico's die malware vormt voor hun *eigen* netwerken. Ik wil hiermee overigens niet suggereren dat ISPs nu hun klanten onvoldoende beschermen. Feitelijk is elke klant gewoon verantwoordelijk voor zijn eigen digitale veiligheid. Bovendien staat een dergelijke SOC functie door ISPs op gespannen voet met de Wet bescherming persoonsgegevens. Die bezwaren zijn overigens te overkomen door de gebruiker toestemming te laten geven. Mijn punt is dat de ISPs een prominente rol zouden *kunnen* hebben bij de bescherming van hun klanten.

Het belangrijkste struikelblok dat ik zie voor een ISP die de burger-SOC rol invult, is de opvolging van een detectie. De klant van de burger-SOC zal veelal advies willen hebben over wat nu te doen en dat kost veel tijd van de burger-SOC en daarmee geld. En omdat internet connectiviteit een commodity is geworden, waar prijs een belangrijke factor is, conflicteert dit met de ISP bedrijfsdoelstellingen. Het notificeren van de klanten over malware infecties zonder de juiste ondersteuning kan zelfs betekenen dat een ISP zich in zijn eigen voet schiet. Een klant kan immers zo geïrriteerd worden over het door hem gepercipieerde gebrek aan ondersteuning dat hij vertrekt naar een andere ISP die hem helemaal niet notificeert rond malware infectie.

Om uit deze impasse te komen, is het denk ik nodig dat we zorgen dat de burger-SOC de burger een eenvoudig, betrekkelijk risicoloos herstel voorstel kan doen. Niet door het uitvoeren van ingewikkelde en niet effectieve en niet toekomst vaste schoningen van computers met anti-virus software. Maar door te zorgen dat de computers van gebruikers eenvoudig kunnen terugkeren naar een veilige staat van *voor* de besmetting. Dat wil zeggen dat de programma's en processen op de computer als voorheen waren en waarbij – en dat is essentieel – de data van de gebruikers nog in de meest actuele vorm beschikbaar zijn. Door ze dus eigenlijk de mogelijkheid te bieden die een expert tot zijn beschikking heeft: het regelmatig maken van een betrouwbare *backup* en het eenvoudig kunnen terugzetten daarvan zowel van de programmatuur als van de documenten.

Ik merk op dat de meeste gebruikers zo ook aan digitale documenten werken; men maakt regelmatig een kopie van het document waar men naar terug kan keren als de laatste wijzigingen toch niet helemaal het gewenste effect hadden. Wat ik betoog is dat we iets dergelijks ook voor de computer zelf moeten hebben.



In een ideale opzet visualiseer ik dat als een 'back to the future' knop op computers. Daarmee wordt, net zoals in de gelijknamige film, een persoon in staat gesteld om terug te gaan naar het verleden om gemaakte fouten in de toekomst te kunnen herstellen. En zo'n knop zou niet alleen op onze Windows computer moeten komen, maar op alle toekomstige computers van gebruikers die met internet verbonden zijn. Dus ook op uw smart-TV met camera en ook op uw toekomstige auto. In de ideale situatie hebben partijen die de gebruiker kunnen waarschuwen over *malware* infecties dan geen conflicterende belangen meer. Ook kan de gebruiker zelf eenvoudig iets doen als zijn computer tekenen van infectie vertoont. Het devies is dan 'Bij geval van twijfel: druk op de back to the future knop'.

Een dergelijke 'back to the future' knop moet eenvoudig zijn voor gebruikers en uiteraard technisch betrouwbaar zijn. Feitelijk wordt deze opzet al toegepast in bepaalde omstandigheden. Bij desktop

virtualisatie software zoals Citrix, of op deze universiteit waar elke dag de student PCs opnieuw worden ‘ingespoeld’ via het netwerk. In zekere zin kunnen tablets op deze wijze al worden gebruikt door plaatsing van de gebruikersdata in de ‘cloud’. Zelf gebruik ik deze opzet al een jaar met behulp van een virtuele machine die ik elke maand terugzet.

Het gaat te ver om nu verdere schetsen te maken van hoe een dergelijke knop ontwikkeld zou moeten worden. Maar mijn verwachting is dat bijvoorbeeld de toepassing van de Cloud en Trusted Execution Technology een dergelijke knop technisch mogelijk maakt. Het idee is dat vanuit Windows periodiek een ‘Trusted Backup’ Applicatie wordt opgestart die niet ongemerkt gemanipuleerd kan worden vanuit malware. Dit is geen technologisch vergezicht. De technologie zit al in veel van de moderne computers maar wordt nog nauwelijks gebruikt. Zie [57.], [58.].

De knop zou kunnen worden ontwikkeld door een samenwerking van hardware en besturing softwareleveranciers, anti-virus software leveranciers, cloud service providers en ISPs. Alle digitale dienstverleners waaronder de overheid en banken zouden het initiatief financieel kunnen steunen.

Samenvatting

Dames en heren, ik vat mijn lezing samen:

- Cybersecurity is niet het vrij zijn van gevaar maar het in optimaal balans zijn met beveiligingsrisico’s. Nemen van risico’s kan ook voordelen geven. De Nederlandse overheid zou een andere definitie moeten hanteren voor cybersecurity.
- Management van organisaties zou zich inhoudelijk moeten bemoeien met APT aanvallen omdat die van direct levensbelang voor de organisatie zijn.
- Met de transitie van fysiek naar digitaal zullen ook burgers steeds meer tegen gerichte aanvallen aanlopen waarbij met name hun persoonlijke levenssfeer in het geding is. Misbruik van persoonlijke informatie op computers kan ook leiden tot identiteitsdiefstal.
- Computers van burgers zijn te lang (naar schatting minimaal een maand) geïnfecteerd met malware en lastig met zekerheid te schonen.
- Burgers zouden daarom – net zoals bedrijven – een Security Operations Center moeten hebben dat hun computers beschermt en monitort op malware. Een belangrijke rol daarvoor zie ik bij de ISPs die ze al gedeeltelijk invullen.
- Om het eenvoudig en betaalbaar te houden heb ik de ‘back-to-the-future’ knop voorgesteld. Hiermee kunnen burgers naar aanleiding van een waarschuwing hun computer eenvoudig en risicoloos terugbrengen naar een veilige toestand uit het verleden.

Dankwoord

Tot slot wil ik enkele woorden van dank uitspreken.

Allereerst wil ik de mensen danken die bijgedragen hebben aan mijn wetenschappelijke en praktische vorming op het terrein van de wiskunde, cryptografie en cybersecurity of die op andere manier hebben gezorgd dat ik hier nu sta. Om tijdsredenen kan ik helaas niet iedereen danken.

Ik wil de BVD (nu AIVD) danken dat zij mij alweer in 1993 de mogelijkheid hebben gegeven mij te bekwamen op het terrein van cybersecurity en mij ook de kans te geven daarin wetenschappelijk actief te zijn. Ik wil ze ook danken voor het mij bijbrengen van risicoanalyse en rapportage vaardigheden.

Mijn latere werkgever PwC wil ik om dezelfde redenen danken maar vooral om de mogelijkheden die zij mij hebben gegeven om interessante opdrachten te doen. Daarom gaat ook veel dank uit naar al mijn opdrachtgevers van de afgelopen jaren. Dank voor jullie vertrouwen en jullie praktijk inzichten!

Bart Jacobs en Erik Poll van de Radboud Universiteit wil ik danken voor hun steun voor het instellen van deze leerstoel evenals Gijs Boudewijn en Michael Samsom van de Nederlandse Vereniging van Banken.

Mijn ouders wil ik danken dat ze mij altijd gesteund hebben mijn eigen interesses te volgen.

De laatste dank gaat uit naar mijn lieve vrouw Jacqueline, zoon Stijn en dochter Olivia. Mijn kroonjuwelen. Ik ben dankbaar voor het harmonieuze gezin dat wij vormen en dat een solide basis vormt voor alles wat ik doe.

Ik heb gezegd.

Referenties/noten

Alle genoemde *Uniform Resource Locators* (URLs) zijn op 1 februari 2014 benaderd.

#	Referentie/noot
1.	'Cybersecurity Beeld Nederland 3', Nationaal Cyber Security Centrum, juni 2013. Zie https://www.ncsc.nl/binaries/nl/actueel/nieuwsberichten/cybersecuritybeeld-nederland-kwetsbaarheid-van-ict-onverminderd-hoog/1/NCSC%2BCSBN%2B3%2B3%2Bjuli%2B2013.pdf
2.	Vergelijk bijvoorbeeld Hoofdstuk 7 'The Battle Within: How the Human Body Defends Itself' uit het boek Searching for Safety, Aaron Wildavsky, Social Philosophy & Policy Center, Transaction Publishers, 2012.
3.	'Bob Quick resigns over terror blunder', The Telegraph, 9 april 2009. Zie http://www.telegraph.co.uk/news/uknews/5129561/Bob-Quick-resigns-over-terror-blunder.html
4.	'Dieven sloegen in Kunsthal hun slag door ontgrendelde museumdeuren', NRC.NL, 22 oktober 2012. Zie http://www.nrc.nl/nieuws/2012/10/22/dieven-sloegen-in-kunsthal-gemakkelijk-hun-slag-door-ontgrendelde-museumdeuren/
5.	'3 jaar cel voor Jérôme Kerviel', NRC NEXT, 6 oktober 2010, Zie http://www.nrc.nl/next/van/2010/oktober/06/3-jaar-cel-voor-jerome-kerviel-11951651
6.	'Kerviel, SocGen's rogue trader, is jailed - It was all his fault', The Economist Online, 5 oktober 2010. Zie http://www.economist.com/blogs/newsbook/2010/10/kerviel_socgens_rogue_trader_jailed.
7.	'Snowden heeft wellicht nog steeds toegang tot NSA-systeem', NRC, 16 december 2013.
8.	'Snowden sought Booz Allen job to gather evidence on NSA surveillance', South China Morning Post, 25 juni 2013. Zie http://www.scmp.com/news/hong-kong/article/1268209/snowden-sought-booz-allen-job-gather-evidence-nsa-surveillance
9.	ISO/IEC 27001 - "Information technology — Security techniques — Information security management systems — Requirements", Second edition, 2013-10-01, International Organization for Standardization. Zie www.iso.ch.
10.	'Besluit voorschrift informatiebeveiliging rijksdienst 2007', zie http://wetten.overheid.nl/BWBR0022141/
11.	'Richtsnoeren beveiliging van persoonsgegevens', College Bescherming Persoonsgegevens, 19 februari 2013. Zie http://www.cbpweb.nl/Pages/pb_20130219_richtsnoeren-beveiliging-persoonsgegevens.aspx.
12.	Zie http://www.wikixl.nl/wiki/ictu/index.php/Component_baseline_informatiebeveiliging_Rijksdienst.
13.	'Black Tulip Report of the investigation into the DigiNotar Certificate Authority breach', 13 augustus 2012, Fox-IT. Zie http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2012/08/13/black-tulip-update/black-tulip-update.pdf.
14.	'DigiNotar failliet verklaard', 20 september 2011, NRC.NL. Zie http://www.nrc.nl/nieuws/2011/09/20/diginotar-failliet-verklaard/.
15.	'De aanhouder wint (Advanced Persistent Threats)', Factsheet FS-2013-02c, 18 oktober 2013, Nationaal Cyber Security Centrum. Zie https://www.ncsc.nl/dienstverlening/expertise-advies/factsheets/factsheet-de-aanhouder-wint-advanced-persistent-threats.html.
16.	'Tracking GhostNet: Investigating a Cyber Espionage Network', 29 maart 2009, The SecDev Group. Zie http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network.
17.	'Coca-Cola 'targeted' by China in hack ahead of acquisition attempt', 5 november 2012, BBC NEWS. Zie http://www.bbc.co.uk/news/technology-20204671.

18.	'The 2013 Data Breach Investigations Report', Verizon, 2013. Zie http://www.verizonenterprise.com/DBIR/2013/.
19.	'EMC's RSA Security Breach May Cost Bank Customers $100 Million', Bloomberg, 8 juni 8, 2011. Zie http://www.bloomberg.com/news/2011-06-08/emc-s-rsa-security-breach-may-cost-bank-customers-100-million.html.
20.	'Lockheed Martin suspends remote access after network "intrusion"', 27 mei 2011, The Register. Zie http://www.theregister.co.uk/2011/05/27/lockheed_securid_hack_flap/.
21.	'Anatomy of an Attack', RSA FraudAction Research Labs. Zie https://blogs.rsa.com/anatomy-of-an-attack/.
22.	'Gehackt door Iraniërs', NRC.NL, 5 september 2011. Zie http://www.nrc.nl/next/van/2011/september/05/gehackt-door-iraniers-12033489.
23.	'Belgacom Attack: Britain's GCHQ Hacked Belgian Telecoms Firm', 20 september 2013, Spiegel Online. Zie http://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html.
24.	'Factsheet Office macro's', Nationaal Cyber Security Centrum, 30 januari 2014. Zie https://www.ncsc.nl/dienstverlening/expertise-advies/factsheets/factsheet-office-macros.html
25.	'Spoofed/Forged Email', CERT Carnegie Mellon University, 4 september 2002. http://www.cert.org/tech_tips/email_spoofing.html.
26.	'Rotterdam last putdeksels dicht voor bezoek Bill en Hillary', Den Haag houdt ze open, Trouw, 24 mei 1997. Zie http://www.trouw.nl/tr/nl/5009/Archief/archief/article/detail/2703625/1997/05/24/Rotterdam-last-putdeksels-dicht-voor-bezoek-Bill-en-Hillary-Den-Haag-houdt-ze-open.dhtml
27.	'Zelfs de brievenbussen worden verzegeld', Volkskrant, 6 mei 2005. Zie http://www.volkskrant.nl/vk/nl/2686/Binnenland/article/detail/689869/2005/05/06/Zelfs-de-brievenbussen-worden-verzegeld.dhtml.
28.	'Visiebrief digitale overheid 2017', 23 mei 2013. De minister van Binnenlandse Zaken en Koninkrijksrelaties, dr. R.H.A. Plasterk. Zie http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/kamerstukken/2013/05/23/visiebrief-digitale-overheid-2017/visiebrief-digitale-overheid-2017.pdf.
29.	'Bankkantoren op termijn dicht?' Zie http://www.marketingonline.nl/bericht/Bankkantoren-op-termijn-dicht.
30.	'Wat is malware?', Microsoft. Zie http://www.microsoft.com/nl-nl/security/resources/malware-whatis.aspx
31.	'Bevolking, huishoudens en bevolkingsontwikkeling; vanaf 1899', CBS, 15 januari 2013. Zie http://statline.cbs.nl/StatWeb/publication/?DM=SLNL&PA=37556&D1=45-52&D2=1,26,51,76,101,111-114&VW=T
32.	'Geregistreerde diefstallen; diefstallen en verdachten naar regio', CBS, 14 november 2013. Zie http://statline.cbs.nl/StatWeb/publication/?DM=SLNL&PA=80603ned&D1=0-14&D2=0-10,13-15,17-22,24&D3=0-2&D4=0&D5=l&VW=T
33.	'Woninginbraken en buurtkenmerken', Een onderzoek naar de samenhang tussen woninginbraken en buurtkenmerken in de gemeente Enschede, Elise Spanjer, 1 februari 2011. Zie http://essay.utwente.nl/63087/. In dit rapport wordt gesteld dat de totale Woningdiefstal gemiddeld 3.000 euro materiële schade met zich mee brengt. Daarbij verwijzend naar onderzoek van het Centrum criminaliteitspreventie veiligheid. Dit getal is voorgelegd aan een betrouwbare bron in de verzekeringswereld die anoniem wil blijven. Deze heeft aangeven dat dit getal klopt en dat het feitelijk is opgebouwd uit 1.800 Euro directe schade (veelal gedekt door de inboedelverzekering) en 1.200 Euro indirecte schade, schade veroorzaakt door de inbraak zelf (veelal gedekt door de opstalverzekering).

34.	'ICT, kennis en economie 2013', CBS, 1 juli 2013. http://www.cbs.nl/NR/rdonlyres/5A8B5B80-C917-4E1A-ADD6-138012961E89/0/2013i78pub.pdf. Sectie 4.1.1. van deze publicatie geeft aan dat in 2012 12,5 miljoen mensen een PC (laptop of desktop) bezat. Uit http://en.wikipedia.org/wiki/Usage_share_of_operating_systems blijkt dat minstens 80% van de besturingssystemen op Windows is gebaseerd is. Daaruit blijkt dat 10 miljoen particuliere PCs (laptop of desktop) in Nederland een redelijke schatting is.
35.	'18-jarige breekt in op duizenden computers', NRC NEXT, zaterdag 14 december 2013. Zie http://www.nrc.nl/next/van/2013/december/14/18-jarige-breekt-in-op-duizenden-computers-1324070.
36.	'Vrijspraak oud-buurman Manon Thomas', RTL Nieuws, 20 maart 2012. Zie http://www.rtlnieuws.nl/nieuws/vrijspraak-oud-buurman-manon-thomas.
37.	'Wat is grooming?' Zie http://www.vraaghetdepolitie.nl/sf.mcgi?240.
38.	'INTERNET SERVICE PROVIDERS AND BOTNET MITIGATION -A Fact-Finding Study on the Dutch Market', Van Eeten et al., januari 2011. Zie http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2011/01/13/internet-service-providers-and-botnet-mitigation/tud-isps-and-botnet-mitigation-in-nl-final-public-version-07jan2011.pdf In deze publicatie wordt middels drie bronnen afgeleid dat in de anderhalf jaar periode januari 2009 – juni 2010 er ongeveer 675.000 particuliere PCs besmet zijn geweest. Dus op jaarbasis betekent dit dat volgens deze publicatie een half miljoen particuliere PCs besmet zijn geweest met malware. Uit persoonlijke communicatie met Van Eeten (3 december 2013, email) blijkt dat de getallen uit de periode 2009 – 2010 ook nog van toepassing zijn op het jaar 2013. De aantallen van Van Eeten zijn gebaseerd op drie datasets (Spam Dataset, DShield Dataset, Conficker Dataset) gerelateerd aan de uitingsvormen van drie specifieke malware vormen, m.n. botnets. Om te compenseren voor de andere vormen van malware en niet gedetecteerde malware (cf. [44.]) schat ik het aantal Nederlandse particuliere PC besmettingen op jaarbasis op 1 miljoen.
39.	'Laat die ladder daar niet staan', NRC, 3 januari 2013.
40.	De schatting is dat ongeveer 10-15% van de mensen over de hele wereld per jaar griep krijgen. Zie http://www.nivel.nl/griep-veel-gestelde-vragen
41.	Zie www.nvb.nl. De gepresenteerde cijfers zijn als geheel bevestigd vanuit de Nederlandse Vereniging van Banken in een email van 22 december 2013.
42.	'Scherpe daling fraude internetbankieren', Nederlandse Vereniging van Banken, 2 april 2013. Zie http://www.nvb.nl/nieuws/2013/1812/scherpe-daling-fraude-internetbankieren.html.
43.	'Effective detection of sophisticated online banking fraud on extremely imbalanced data', Wei Wei et al, World Wide Web, Springer, July 2013, Volume 16, Issue 4, pp 449-475. Zie http://www-staff.it.uts.edu.au/~lbcao/publication/Jwww-12.pdf.
44.	'Expertos de UE alertan de que los antivirus solo funcionan en 30% de ataques', Expansión.com, 25 september 2012. Zie http://www.expansion.com/agencia/efe/2012/09/25/17646563.html. In een email van 27 december 2013 is de persvoorlichting van ENISA gevraagd of dit cijfer het officiële standpunt van ENISA is. De persvoorlichting geeft aan niet te weten wat er tijdens de betreffende bespreking is aangegeven door de directeur van ENISA maar bestrijdt niet dat dit cijfer is genoemd.
45.	'Antivirus software versus Malware', Bachelorscriptie door Anne Westerhof, 2011. Zie http://www.cs.ru.nl/bachelorscripties/2011/Anne_Westerhof___0815012___Antivirus_software_versus_Malware.pdf.
46.	'Assessing the Effectiveness of Antivirus Solutions', IMPERVA, december 2012. Zie

	http://www.imperva.com/docs/HII_Assessing_the_Effectiveness_of_Antivirus_Solutions.pdf.
47.	https://www.botfrei.de/
48.	'A Threat Case Study: Rogue Security Software', ENISA Quarterly Review, ENISA, Vol. 4, No. 4, Oct-Dec 2008. Zie http://www.enisa.europa.eu/publications/eqr-archive/issues/eqr-q4-2008-vol.-4-no.-4/at_download/issue.
49.	'Hoe doen ze het toch? Modus Operandi Woninginbraak', DSP-groep, 23 november 2009. Onderzoek uitgevoerd voor het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Zie http://www.dsp-groep.nl/projecten/p1/2711/.
50.	http://police-trojan.com/.
51.	'Microsoft Security Intelligence Report', Volume 15, Microsoft. Zie http://download.microsoft.com/download/5/0/3/50310CCE-8AF5-4FB4-83E2-03F1DA92F33C/Microsoft_Security_Intelligence_Report_Volume_15_English.pdf. Hierin wordt CCM waarde 3.3 gegeven voor Q1 2013 en 2.7 voor Q2 2013.
52.	In de eerdere versies van het Microsoft Security Intelligence Report worden de volgende CCM cijfers genoemd: Q1 2012: 6.3, Q2 2012: 4.8, Q3 2012: 5.6, Q4 2012: 2,6 (Volume 14) Q1 2011: 4,6, Q2 2011: 5.3, Q3 2011: 6.6 , Q4 2011: 13,1 (Volume 12, 13) Zie http://www.microsoft.com/security/sir/archive/default.aspx.
53.	De geschatte besmettingsduur van 36,5 dagen is in lijn met het onderzoek uitgevoerd door SurfRight. SurfRight heeft onderzoek gedaan naar de besmettingsduur van bepaalde malware (Zeus, Citadel, SpyEye and Tinba). Deze duur was 81 dagen voor computer zonder up-to-date anti-virus software en 25 dagen voor computers met up-to-date anti-virus software. Zie 'Antivirus shortens the life-time of financial malware', hitmanpro.Blog. http://hitmanpro.wordpress.com/2012/10/23/antivirus-shortens-the-life-time-of-financial-malware/
54.	'Security Operations Center: Een inrichtingsadvies', Platform voor Informatiebeveiliging Expertbrief – februari 2011. Zie https://www.pvib.nl/download/?id=17670673.
55.	'Post mortem report on the sinowal/nu.nl incident', Fox-IT, 16 maart 2012. Zie http://blog.fox-it.com/2012/03/16/post-mortem-report-on-the-sinowallnu-nl-incident/.
56.	'Persbericht AbuseHUB', 14 november 2013. Zie http://www.abuseinformationexchange.nl/mm_uploads/AbuseHUB_van_start_botnets_aangepakt-1.pdf
57.	'Using Trusted Execution Environments in Two-factor Authentication: comparing approaches', Erik Poll, Roland van Rijswijk-Deij. Zie http://www.cs.ru.nl/E.Poll/papers/TEE.pdf.
58.	Veel PCs (laptops of desktops) zijn al uitgerust met de Trusted Execution Technology van Intel IPT genaamd. Zie http://ipt.intel.com/Home/devices-with-intel-ipt.