Inhoud

Hoofdstuk 1

Computer-beveiliging

Beveiliging is een wedloop tussen aanvaller en verdediging. De aanvaller wil schade aanrichten, iets van waarde stelen of de verdediging verzwakken terwijl de verdediging dit wil voorkomen. Computers en andere informatie- en communicatie-technologie zijn hierop geen uitzondering.

Je leert in dit hoofdstuk:

De nood aan beveiliging is alomtegenwoordig.

Waarom zijn computers kwetsbaar? Hoe worden deze zwakheden uitgebuit?

Wat is voor een aanvaller de waarde van je computer?

Het belang van goede gewoontes.

Wie zijn de aanvallers? Wie komt je ter verdediging?

Wat is een 'hacker'?

Achtergrond

De wedloop tussen aanvaller en verdediger heeft altijd bestaan: primitieve oermensen verschansten zich in grotten en maakten vuur om zichzelf tegen roofdieren te beschermen; middeleeuwse kastelen dienden om het land tegen indringers te beveiligen; de Tower of London diende om de kroonjuwelen van het Britse koningshuis te beveiligen tegen dieven; en goed-geoefende voetballers kunnen hun goal beveiligen tegen welgemikte doelschoten van de tegenstand.

Telkens wanneer technologie evolueerde, evolueerde ook de behoefte aan beveiliging. De eerste textielfabrieken in Groot-Brittannië, die voor het eerst menselijke spinners en wevers door stoomkracht vervingen, werden opzettelijk in dunbevolkte gebieden in het noorden van Engeland gebouwd, om te voorkomen dat de machines vernield zouden worden door jaloerse concurrenten, of dat hun industriële geheimen zouden worden gestolen. Het waren echte kastelen van de industriële revolutie, inclusief dikke muren en schietgaten voor musketten.

Deze gebouwen waren natuurlijk niet goedkoop, en hun afgelegen locatie maakte het moeilijker en duurder om producten te transporteren. Maar de eigenaars vonden dat de prijs het waard was, want de nieuwe technologieën zorgden voor een enorme winst, en zo lang zij de enigen waren met dit voordeel was er meer dan voldoende geld om de kosten van de beveiliging te dragen.

Zo is beveiliging altijd een compromis tussen kosten en waarde. Een bank zal over het algemeen beter beveiligd zijn dan een huis, en het zal moeilijker zijn in een huis in te breken dan in een tuinhuisje. Goede deuren, sloten en alarmsystemen kosten geld, en dat zal het niet waard zijn voor een ladder en een grasmaaier, maar wel voor de persoonlijke eigendommen en het geruste gemoed van de bewoners van het huis, en zeker voor de rijkdom die in een bank opgeslagen kan zijn.

En deze norm geldt ook voor computers. Zij kunnen veel digitale waarde bevatten, soms waar je het niet zou verwachten. Computerchips en netwerkverbindingen zijn nu zo goedkoop te maken, en zo veelzijdig, dat ze overal in onze maatschappij te vinden zijn. Niet alleen als PC’s, laptops of mobiele telefoons, maar ze zijn ook ingebouwd in allerhande toestellen: televisies, netwerkcamera’s, zelfs wasmachines en koelkasten kunnen ermee zijn uitgerust.

Daarenboven zijn we allen steeds meer afhankelijk van het internet, waar we online boodschappen kunnen doen, kunnen bankieren, of gewoon sociaal zijn met vrienden, kennissen en collega's. Daarom zijn meer en meer computers dan ook rechtstreeks met het internet verbonden. Jammer genoeg betekent dit soms dat ze niet alleen ons toegang verzorgen tot de informatiesnelweg, maar ook dat anderen, om het even waar ter wereld, diezelfde elektronische snelweg kunnen gebruiken om onze computers aan te vallen en te misbruiken.

De beveiliging van je IT- (Informatie Technologie) of ICT- (Informatie- en Communicatie Technologie) bezittingen is dan ook belangrijker dan ooit.

Het doel van dit boek is je te informeren zodat je je eigen IT-veiligheid kunt verhogen. We helpen je te begrijpen hoe, en vooral waarom, je best met je computers, netwerken en gegevens omgaat, en hoe je zelf inspanningen kunt afwegen tegenover risico's. Soms kan dit het leven wat moeilijker maken, net als je sneller je huis in en uit kunt als je geen slot op de deur hebt, maar het is dan ook wel heel wat minder veilig! Na het lezen van dit boek kun je zelf afwegen welke digitale sloten voor jou, of voor je bedrijf, de moeite waard zijn, en welke minder noodzakelijk zijn.

Kwetsbaarheid en aanval

In een ideale wereld zouden computersystemen altijd veilig zijn, met onkwetsbare software die door niets of niemand kan worden uitgebuit om ongeoorloofd toegang te krijgen.

Jammer genoeg leven we niet in een ideale wereld, en zijn computers wel kwetsbaar. Vaak manifesteren deze kwetsbaarheden zich in de programma's die de computer draait (*software*), maar er zijn ook aanvallen die het rechtstreeks op de elektronische chips in je computer gemunt hebben (dat is de *hardware*), of de programmatuur die in de hardware is ingebakken om basisfuncties te vervullen (de *firmware*).

Zo'n kwetsbaarheid (of *vulnerability* in het Engels, we zullen beide woorden in dit boek gebruiken), kan ertoe leiden dat informatie die door het systeem bewerkt en/of opgeslagen wordt niet langer betrouwbaar of toegankelijk is. Dat gebeurt wanneer zo'n vulnerability in een systeem wordt uitgebuit door een tegenpartij, zeg maar een aanvaller die hier de kans toe heeft. De manier waarop een vulnerability wordt uitgebuit is een *exploit*, ook weer uit het Engels. Het duurt meestal enige tijd nadat een kwetsbaarheid is ontdekt voordat een succesvolle exploit wordt gevonden die kan worden gebruikt om er een aanval mee uit te voeren.

Zo'n aanval kan tot gevolg hebben dat het systeem niet langer werkt, of dat informatie wordt vernield, of dat het overbelast wordt en niet langer normaal dienst kan doen. Maar zelfs als een aanval geen directe schade aanricht, dan kan die toch negatieve gevolgen hebben, bijvoorbeeld wanneer in computersystemen wordt ingebroken en geheime gegevens (bijvoorbeeld compromitterende privéfoto's, bedrijfsgeheimen of bankinformatie) worden gekopieerd. Dan is er geen onmiddellijke schade, maar kan dit toch nefaste gevolgen hebben.

Waarom zijn computersystemen of netwerken kwetsbaar? Meestal is de boosdoener de complexiteit: computersystemen worden alsmaar ingewikkelder, en dat vergroot de kans op foutjes. In complexe systemen is het ook moeilijker alle mogelijke combinaties van instellingen te testen, en deze kunnen aanleiding geven tot zwakheden die gebruikt kunnen worden om het systeem aan te vallen.

Om een aanval uit te voeren zal de aanvaller een combinatie van de volgende elementen gebruiken: toegang tot de computer of het netwerk; expertise (kennis van zaken) in het uitvoeren van de aanval; tijd en mankracht om de aanval uit te voeren; en de wil om een zekere hoeveelheid risico op zich te nemen. Het spreekt voor zich dat aanvallers met meer middelen, zoals rijke firma's of overheden, meer geld kunnen besteden om aanvallen te versterken.

Besturingssystemen van moderne computers gebruiken een uitgebreid systeem van permissies en trachten zo te voorkomen dat verkeerde acties worden ondernomen (zij het door een aanvaller, of door slechte software). Hierbij worden verschillende gebruikersrollen op de computer gecreëerd door het besturingssysteem, waarbij iedere gebruiker een verschillend toegangsniveau kan worden toegekend, van een almachtige *administrator* tot een gewone gebruiker of tijdelijke bezoeker. Iedere gebruiker krijgt zo een bepaald toegangsniveau tot de bestanden en diensten van de computer. Zo kunnen, in theorie, essentiële delen van het besturingssysteem beschermd worden tegen vergissingen of aanvallen. Hoewel de verleiding soms groot is om alle handelingen op de computer in de almachtige administrateur-rol uit te voeren, zodat je acties nooit verboden zullen worden door de ingebouwde beveiliging van het besturingssysteem, is dit ten zeerste af te raden. Een eenvoudige handeling als het bekijken van een gecompromitteerde webpagina kan dan al onmiddellijk leiden tot een computer die besmet is met kwaadaardige software, bijvoorbeeld een virus, waar dit mogelijk zou gestopt zijn door de beperktere toegang van de gewone gebruikersrol. Moderne besturingssystemen maken het ook steeds gemakkelijker om de gewone gebruikersrol te gebruiken, en zullen automatisch om een wachtwoord vragen als toch meer toegang vereist is. Wanneer dit gebeurt is dit dan ook een sterke waarschuwing dat iets of iemand ingrijpende wijzigingen aan het systeem wil maken, en kun je indien nodig deze activiteit

een halt toeroepen (door eenvoudigweg de vraag om een wachtwoord te annuleren).

Catalogus van kwetsbaarheden

Er bestaan verschillende databanken van vulnerabilities, die als doel hebben het publiek te informeren over mogelijke kwetsbaarheden in de software die ze gebruiken, en het risico dat ermee gepaard gaat. De bekendste is zonder twijfel de CVE-database van de Amerikaanse organisatie MITRE (die gefinancierd wordt door verschillende armen van de Amerikaanse overheid). CVE betekent hier 'Common Vulnerabilities and Exposures'. Elke kwetsbaarheid krijgt een nummer toegewezen, en zal door MITRE geverifieerd worden voordat ze publiek wordt gemaakt. Grote softwarebedrijven als Apple, Google of Microsoft zullen het CVE-nummer van kwetsbaarheden soms ook vermelden in de details van een software-update die ze oplost.

Hoewel ze Amerikaans is, is dit toch de standaard databank voor kwetsbaarheden in allerhande software geworden, dank zij de wereldwijde natuur van het internet.

Als je security bulletins leest, dan zie je soms ook de naam 'CERT'. Hier gaat het dan om een Computer Emergency Response Team. Oorspronkelijk opgezet aan de Amerikaanse Carnegie Mellon Universiteit ging het om een groep IT-specialisten wiens taak het was het computernetwerk te bewaken, te beveiligen tegen dreigingen, en te reageren op eventuele aanvallen. Door de jaren heen is de naam generisch overgenomen door vele organisaties wereldwijd, die in een nationale of zakelijke context deze taken vervullen.

De waarde van je computer

Zoals we al zagen, ga je beveiliging altijd afwegen tegen het mogelijke risico. De computersystemen van een bank hebben meer behoefte aan sterke beveiliging dan een spelconsole thuis. Beveiliging van computers kost tijd en vaak ook geld, dus is het best goed af te wegen wat nodig is. Er zijn jammer genoeg geen officiële cijfers van hoeveel schade er jaarlijks wereldwijd wordt geleden door cyberaanvallen, en schattingen variëren van tientallen tot honderden miljarden euro per jaar.

Het lijkt logisch dat de computersystemen van grote banken waardevol zijn, maar de waarde van een computer in een kleiner bedrijf, of thuis, is moeilijker in te schatten. En toch hebben ook die systemen een verrassende waarde, zeker als er duizenden van dergelijke systemen automatisch kunnen worden aangevallen en overgenomen. Zelfs al zou je denken dat je niets van waarde bezit.

De informatie op de computer(s) kan worden gestolen, gewist of zelfs gegijzeld. Financiële en inloggegevens kunnen worden gestolen en misbruikt, of verhandeld op de zwarte markt. Zij worden gebruikt om je identiteit te stelen zodat je bankrekeningen kunnen worden geplunderd, of om valse aankopen te doen op online winkel- en veilingwebsites. Je e-mail en adresboek kunnen worden misbruikt om andere elektronische aanvallen authentieker te maken. Als iemand actief en bekend is op sociale media, dan heeft een dergelijke reputatie ook waarde. Populaire personen op Facebook of Twitter kunnen beïnvloeden welke berichten vaak door andere gebruikers gezien zullen worden, en dit kan misbruikt worden om betaalde advertenties te tonen, of virussen en kwaadaardige software te verspreiden.

Wordt de computer gebruikt om online spellen te spelen, dan heeft zelfs die informatie een waarde: het gebeurt vaak dat 'bezittingen' binnen dergelijke online spellen, die vaak slechts met moeite kunnen worden verkregen, worden gestolen om dan voor 'echt' geld verkocht te worden.

Als het gaat om bedrijfscomputers dan zijn er natuurlijk een hele hoop financiële en personeelsgegevens die gestolen kunnen worden, en die waarde hebben op de zwarte markt. En gestolen intellectueel eigendom kan enorm veel geld waard zijn wanneer dit aan concurrenten wordt aangeboden.

Een computer die onder controle staat van aanvallers kan ook ingeschakeld worden als een pion in een *bot*-netwerk. Een afgekorte versie van 'robot', waarbij het hier gaat om duizenden gehackte computers die onder de controle staan van een enkele organisatie of individu. Ze worden gebruikt om spam e-mails te sturen, massale aanvallen op websites of andere infrastructuur uit te voeren, of om illegaal netwerkverkeer te verbergen. Omdat dergelijke aanvallen, waarbij computers worden overgenomen voor later gebruik, gemakkelijk te automatiseren zijn komen ze het vaakst voor.

De computers worden, ook zonder dat de eigenaar er weet van heeft, gebruikt als server op het internet, waardoor illegale software of andere gegevens inclusief malware, illegale software, illegale pornografie enzovoort, worden uitgewisseld.

Je ziet: er kan bijzonder veel van waarde in een bescheiden computer gevonden worden. Het is onmogelijk in te schatten wat de exacte waarde is op de zwarte markt voor deze aspecten, en dit is vaak ook niet van belang. Wat wel telt is hoeveel schade jij zelf oploopt wanneer je het slachtoffer zou worden van deze aanvallen. Dit is het risico dat je moet afwegen om te besluiten in welke beveiligingstechnieken je tijd en geld wil investeren.

Geautomatiseerde aanvallen zijn het meest voorkomend, bijvoorbeeld wanneer een website elke kwetsbare computer die ze bezoekt kan aanvallen en overnemen. Dit kost een opportunistische aanvaller immers niets, en zij zullen geen scrupules hebben over wiens computer het gaat, en hoeveel schade er wordt aangericht. Scholen en ziekenhuizen worden net zo vaak aangevallen als banken en koffieshops, iedereen is een mogelijk doelwit. Gelukkig zijn dit soort aanvallen ook relatief gemakkelijk af te weren, voornamelijk door je computersoftware altijd up-to-date te houden (meer over dit heel belangrijke onderwerp in een later hoofdstuk!).

Beleid en policies

Goede computerbeveiliging is in de eerste plaats afhankelijk van een goed beleid en goede gewoontes. Voor bedrijven is het dan ook heel belangrijk een beleid uit te werken dat aangeeft hoe computers en computernetwerken in het bedrijf moeten of mogen worden gebruikt, en ervoor te zorgen dat alle werknemers hiervan op de hoogte zijn en dat ook blijven.

Dit boek zal een overzicht geven van de meest belangrijke goede gewoontes die men dient op te bouwen, en de slechte gewoontes die vermeden moeten worden. Wat geldt voor de bedrijfswereld is vaak ook van toepassing in het persoonlijke leven, zij het dan op kleinere schaal. Je hoeft dan ook geen persoonlijk IT Policy-document te schrijven, maar je zult wel dezelfde goede gewoontes opbouwen en eventueel delen met anderen in je onmiddellijke omgeving.

Bij het opstellen ga je beoordelen hoe belangrijk beveiliging is voor jezelf of je bedrijf, en ga je dit afwegen aan de verwachte weerslag hiervan op de activiteiten die op je computers en netwerk worden uitgevoerd.

Heb je bijvoorbeeld vastgesteld dat virussen of andere malware je netwerk zijn binnengedrongen omdat gebruikers onvoldoende voorzichtig waren bij het browsen van het worldwide web, dan zou je volledig de toegang tot het WWW kunnen verbieden. In sommige omstandigheden kan dit aanvaardbaar zijn, maar het web is vaak zo ingeburgerd, en zo'n nuttige bron van informatie, dat enige toegang toch gewenst is. Dus besluit je dan misschien om enkel toegang te geven tot bekende 'goede' websites, of om een lijst van bekende slechte sites te weren. Je kunt hiervoor bijvoorbeeld proxy servers gebruiken op het netwerk, en die behandelen we nog in een later hoofdstuk.

Wanneer het beleid verandert kunnen heel wat mensen dit als negatief ervaren, en zul je tegenwind krijgen. Maar houd dan toch het been stijf: als je besluit dat je beveiligingspolicy sterker gemaakt moet worden, voer deze dan volledig uit op het moment van implementatie. Het zal een tijdelijke invloed hebben op de productiviteit, en men kan klagen, maar over het algemeen zal men snel oplossingen vinden om weer even productief te zijn met het nieuwe beveiligingsregime. Enkel als er echte showstoppers zijn kun je een uitzondering maken op de regels tot je policy is aangepast om ook in dit geval effectief te werken.

Wie valt aan?

Tegen wie moet je je computers beschermen? Als een misdaad in de fysieke wereld een tegenhanger heeft in *cyberspace* (de cyberwereld), dan zal die worden begaan. Waar banken vroeger geld in zwaar bewaakte konvooien of treinen transporteerden, gebeurt dat nu allemaal via computernetwerken: miljarden euro worden elke dag tussen banken verhandeld, eenvoudigweg door het manipuleren van getallen in databanken. De meeste bankfilialen hebben dan ook vaak slechts weinig contant geld ter beschikking, waardoor fysieke bankovervallen vaak niet meer de moeite lonen. Maar wie kan inbreken in de computernetwerken die door diezelfde banken overal en altijd worden gebruikt, kan miljoenen bijeenrapen, soms jarenlang zonder ontdekt te worden. In 1995 slaagde de Rus Vladimir Leonidovitch Levin erin om 10,5 miljoen Amerikaanse dollar van Citibank frauduleus over te hevelen naar rekeningen van samenzweerders in Finland, de VS, Nederland en Israël. Drie van de samenzweerders werden opgepakt toen de fraude aan het licht kwam, en uiteindelijk werd het merendeel van de fondsen (10,1 miljoen dollar) herwonnen, maar het duurde verscheidene jaren voordat Levin kon worden gearresteerd: hij kon door de Russische wet niet worden uitgeleverd, en werd pas opgepakt door de Britse politie toen hij overstapte tussen twee vluchten in een luchthaven in het Verenigd Koninkrijk, waarna hij aan Amerika kon worden overgeleverd. Daar werd hij in 1998 tot 3 jaar cel en een boete van 240,000 dollar veroordeeld.

Nu het internet computers overal ter wereld met elkaar verbindt, leeft iedereen digitaal in dezelfde buurt. Een aanvaller in de Benelux kan nu dus net zo gemakkelijk computers aanvallen in Rusland als in het thuisland, en vice versa. Vaak zullen aanvallers buitenlandse computers verkiezen, omdat het dan veel moeilijker wordt voor de gerechtelijke diensten om de daders te pakken, zoals in het geval van de Citibank-fraude van 1995. Hoewel het overgrote deel van de mensen geen criminele intenties heeft en je computer niet zal aanvallen, is zelfs een klein percentage van de wereldbevolking nog steeds een aanzienlijk aantal. De cybercriminaliteit groeit dan ook hand in hand met het toenemende gebruik van computers in de samenleving.

En omdat computers gemaakt zijn om snel automatische handelingen te verrichten, worden misdrijven die de moeite niet loonden in het verleden nu plots wel lucratief. Zogenaamde 'salami-aanvallen', bijvoorbeeld, waarbij slechts een miniem bedrag wordt buitgemaakt (te vergelijken met een dun plakje salami) kunnen door computers automatisch duizenden tot honderdduizenden keren worden uitgevoerd, waardoor de buit plots wel heel aantrekkelijk wordt—als het ware een enorme salami-worst, opgebouwd uit duizenden dunne schijfjes.

Vaak zijn cyberaanvallen erop uit om geld of gegevens te stelen, soms kan het erom gaan je computer van afstand te kunnen bedienen om in de toekomst te gebruiken voor andere aanvallen, soms gaat het de aanvaller gewoon om schade aan te richten. Soms wil de aanvaller bekendheid verwerven, soms is men erop uit de reputatie van het slachtoffer te ruïneren. Het kan dan gaan om een individu (bijvoorbeeld politici: zo slaagden Russische hackers in de Amerikaanse presidentsverkiezingen van 2016 erin om in te breken in de e-mailserver van de Democratische Conventie, en werden aldus verkregen e-mails gebruikt om de reputatie van de Clinton-campagne bij de Republikeinse kiezers te schaden). Maar het gaat vaak ook om bedrijven, al dan niet opzettelijk: de reputatie van Citibank kelderde na de fraude van 1995, omdat die door de media wijd werd besproken. In 2014 werd Sony Pictures het slachtoffer van een grootschalige cyberaanval, die schijnbaar enkel tot doel had hun reputatie te schaden, onder meer door vertrouwelijke e-mails van de filmafdeling publiek te maken.

Men zou kunnen denken dat het uitvoeren van aanvallen op computers in cyberspace een gegronde technische kennis vereist, en dat ze enkel door specialisten kunnen worden uitgevoerd. Dat is zo voor de ontwikkeling van nieuwe aanvallen, maar wanneer een techniek gebruiksklaar is kan deze geautomatiseerd en verspreid worden, en kan ze vaak door iedereen met slechts enkele klikken van een computermuis worden uitgevoerd. Deze informatie zal zich snel verspreiden langs het internet, en dan vooral via websites en discussieforums waar men het niet nauw neemt met de letter van de wet.

De ultieme uiting hiervan zijn zogenaamde *script kiddies*, een denigrerende Engelstalige term voor amateurs (oorspronkelijk teenagers) die op z'n best over weinig expertise beschikken. Zij kopiëren en wijzigen programmacode van internet, wat meestal resulteert in een vrij amateuristisch, cru stukje malware (kwaadaardige software). Dit brengt anderen echter vaak op ideeën, en zo'n malware wordt vaak verder verfijnd en verspreid, en wordt dus toch beter niet onderschat.

Echt geavanceerde cyberaanvallen vereisen dikwijls een enorme investering, en de combinatie van het kunnen van meer dan één expert. Hoewel er commerciële (en vaak criminele) organisaties bestaan die zich in dit soort kennis specialiseren, is dit vaak iets dat op nationale schaal wordt uitgevoerd: een intelligentiedienst en/of een geheime dienst, iets waarover de meeste landen beschikken. Bij grootmachten hebben die diensten een enorm budget, en een enorme capaciteit om aanvallen tegen computersystemen uit te voeren wanneer nodig. Men noemt dit dan *cyber warfare*, of cyberoorlogvoering. Vooral de Verenigde Staten, het Verenigd Koninkrijk, Rusland, Israël en China zijn berucht vanwege de enorme middelen die ze kunnen inschakelen om online aanvallen uit te voeren en informatie te verzamelen, vervalsen of verspreiden. Sommige landen hebben echte *cyber armies*: legers van computerhackers die ingezet worden om gigantische hoeveelheden informatie in te zamelen, strategisch elektronische doelwitten aan te vallen, valse campagnes op sociale media te ondersteunen of vernietigen enzovoort. Als individu of KMO je hiertegen beschermen is heel moeilijk, zelfs bijna onmogelijk, tenzij je computers volledig losstaan van het internet om ze onbereikbaar te maken.

Geavanceerde aanvallers kunnen schade aanrichten met een heel doelgericht offensief. Zo lanceerde een geavanceerde anonieme organisatie in 2010 een cyberaanval tegen het Iraanse nucleaire programma. Iran gebruikte speciale centrifuges om uranium te verrijken met nucleaire isotopen, zodat het in kernreactoren tot grondstof voor atoomwapens kan worden verwerkt. De aanval gebeurde door een heel gerichte infectie met een specifiek computervirus. Het virus heette StuxNet, en was volgens onderzoekers waarschijnlijk ontwikkeld door een samenwerking van de Amerikaanse en Israëlische geheime diensten, hoewel dit nooit officieel is bevestigd. Het virus was gebaseerd op twee kwetsbaarheden in Microsoft Windows, die voor de aanvallers bekend waren maar geheim werden gehouden, opdat Microsoft deze achterpoortjes niet zou afsluiten en hen de toegang zo ontnemen. Ondanks het feit dat de computers die deze centrifuges beheerden volledig losstonden van het internet, werden zij toch met een virus besmet: het virus besmette eerst één of meerdere USB-opslagmedia, en wanneer die werden gebruikt kon de besmetting zich over de centrifuge-controlecomputers verspreiden langs het lokale netwerk. Kwam het virus terecht op een computer waar mogelijke centrifuge-hardware aan verbonden was, dan beschadigde het de centrifuge door er instructies naartoe te sturen die de snelheid verkeerd instelden. Het virus zorgde er ook voor dat het bewakingssysteem de indruk gaf dat alles normaal was, zodat meer schade werd aangericht voordat de fout werd ontdekt. Kwam het virus op een computer terecht zonder centrifuge, dan ging het in ‘digitale winterslaap’ en trachtte het zich alleen verder te verspreiden over het netwerk en over USB. Men schat dat een vijfde van de Iraanse centrifuges hierdoor zwaar beschadigd raakte. Om het geheim van de worm te bewaren was het programma zo ingesteld dat het zich vanaf 2012 automatisch zou uitwissen.

Een foutje in de software om het virus te updaten zorgde er in 2010 echter voor dat het zich toch verspreidde buiten Iran, en zo ontmaskerd werd door Amerikaanse en Russische computerspecialisten.

Hoewel overheden nog steeds de krachtigste wapens bezitten, ook in cyberspace, loopt de commerciële (zij het dan criminele) wereld niet ver achter. Zij ontwikkelen nieuwe aanvallen en zoeken nieuwe vulnerabilities, en verkopen deze informatie dan voor miljoenen euro. De nieuwste technieken, die eerst door hen worden gebruikt, zullen dan na verloop van tijd ook door de 'modale' hacker gebruikt worden. Zo werd, 5 jaar na StuxNet, een virus ontdekt dat dezelfde technieken gebruikt om de computernetwerken van banken te infiltreren. De boosdoener die het creëerde is bij dit schrijven nog niet gepakt.

Zelfs kleine firma's kunnen ten prooi vallen aan hacking, bijvoorbeeld door concurrenten. Zo werd een klein linnenbedrijf in Amerika gedurende twee jaar bespioneerd door een concurrerende firma, die hun klantengegevens en prijsoffertes kopieerde om er zo klanten van af te snoepen. Ze konden dit doen omdat ze het online websysteem van de andere firma kenden, en het standaard wachtwoord niet was veranderd. Uiteindelijk werd de tweede firma betrapt en moest deze na een rechtszaak een zware schadevergoeding betalen.

Wie verdedigt?

Gelukkig worden gewone computergebruikers, geconfronteerd met computeraanvallen van alle hoekjes van de wereld, niet aan hun lot overgelaten. Specialisten in het analyseren van computeraanvallen, virussen en andere kwaadaardige software werken overal ter wereld aan middelen om de schade van deze aanvallen in te perken en gebruikers (en hun gegevens) veilig te houden.

Deze specialisten, *security researchers*, kunnen in dienst zijn van overheidsdiensten, universiteiten, grote softwarebedrijven, of gespecialiseerde IT-beveiligingsbedrijven. Voor overheden komt het eropaan te zorgen dat de veiligheid van computersystemen verzekerd is voor de bevolking en natuurlijk vooral voor de verschillende overheidsdiensten. Bij IT-bedrijven wordt de expertise van deze onderzoekers gebruikt voor de bescherming van de (betalende) klanten, en de infrastructuur van de bedrijven zelf. Dit kan ook worden uitbesteed aan andere bedrijven die zich specialiseren in de computerbeveiliging. Een groot deel van het onderzoek wordt ook verricht aan universiteiten in de afdeling computerwetenschappen. De resultaten van al dit werk worden vaak uiteindelijk gratis met iedereen gedeeld via internet, soms na een korte exclusiviteitsperiode.

Natuurlijk zijn de makers van kwaadaardige software op de hoogte van het bestaan van security researchers, en zij zullen in sommige van hun creaties trachten de netwerklocaties en hulpprogramma's te identificeren die vaak door deze specialisten worden gebruikt. Zo worden virussen en andere kwaadaardige software vaak getest in virtual machines: virtuele, gesimuleerde computers die niets van waarde bevatten en enkel dienen om de effecten van slechte software te onderzoeken. Indien dit het geval is kan de software zichzelf wissen, om de kans op ontdekking te verkleinen.

Hacker!

Het woord 'hacker' heeft niet altijd negatieve connotaties. Het werd voor het eerst gebruikt bij MIT in de jaren 60, en verwees naar een technisch aangelegde enthousiast met aanzienlijke vaardigheden. Tijdens de thuiscomputerrevolutie van de volgende decennia begon men het ook te gebruiken voor mensen die bijzonder goed waren met computers. Later werd deze terminologie gebruikt voor mensen die over de kennis, ervaring of middelen beschikken om vulnerabilities uit te buiten en in te breken in computersystemen. Dit is beduidend negatiever dan de originele betekenis van het woord.

Er wordt druk naar nieuwe vulnerabilities gezocht, door mensen met goede of slechte bedoelingen. De eerste categorie omvat onderzoekers en programmeurs die de digitale wereld veiliger willen maken, en/of die erop uit zijn zichzelf een naam te verwerven als security-specialist, zogenaamde 'white hat' hackers (hackers met witte hoed, dus). Zij zoeken kwetsbaarheden zodat ze opgelost kunnen worden, soms door de hacker zelf, en ze zijn vaak in dienst van grote computerfirma's. Sommige softwarebedrijven, zoals Apple, Google en Microsoft, loven ook beloningen uit voor dergelijke hackers wanneer ze op een verantwoorde manier een kwetsbaarheid in hun producten kunnen aantonen en deze bedrijven een kans geven om de fout op te lossen alvorens de kwetsbaarheid publiek te maken. (De reden voor de publiciteit is tweevoudig: het doet de reputatie van de hacker goed, en het kan mensen informeren dat ze zich moeten beschermen. Meestal wordt aan bedrijven een bepaalde periode, nu meestal 8 weken, gegeven waarin zij de enigen zijn die over de kwetsbaarheid geïnformeerd worden. Dat zou voldoende moeten zijn om het probleem aan te pakken, en naar men hoopt onvoldoende voor andere, kwaadwillige aanvallers om dezelfde kwetsbaarheid te ontdekken.)

De tweede categorie zijn de zogenaamde 'black hat' hackers (met zwarte hoed); deze zoeken kwetsbaarheden om ze te kunnen misbruiken om toegang te krijgen tot systemen of netwerken. Deze zijn soms ook in dienst van firma's - zij het dan wel met een heel dubieuze reputatie. Deze firma's bieden soms ook kennis van kwetsbaarheden aan op de zwarte markt, zodat aanvallers ze

kunnen misbruiken. Het gaat hier dan vaak om heel grote sommen geld, en het is een markt die ook door intelligentiediensten van rijke landen gretig in het oog wordt gehouden. Zogenaamde 'zero-day exploits', de meeste kwetsbare aanvalspunten die nog niet door de softwarefirma's ontdekt en gerepareerd zijn, kunnen op deze zwarte markt zeer veel geld opbrengen, en worden zowel door overheden als door kartels van computercriminelen aangekocht.

Ten slotte identificeert men soms ook 'grey hat' hackers (grijs, dus), die hacken voor hun eigen plezier, en die eerder grapjes uithalen. Praktisch gezien leunen zij eerder aan tegen de black hat hackers dan de white hat hackers. Zij zullen de eigenaars van de software die ze hacken niet inlichten over de kwetsbaarheid, maar die gebruiken voor hun eigen entertainment.

Het woord 'hacking' is in recentere jaren ook meer en meer gebruikt voor simpelweg het gebruik van slimme trucjes, bijvoorbeeld 'lifehacking', het bedenken en verspreiden van trucjes om dagelijkse taken in het leven op te lossen. In de media gebruikt men het woord 'hacker' ook wel voor iedereen die tracht in computers of computernetwerken in te breken, ook al hebben ze daarover slechts beperkte kennis en gebruiken ze enkelweg computersoftware die door anderen is geschreven. Dit kan tot verwarring leiden met de traditionele definitie.

Vragen

1. Computers zijn kwetsbaar. Wat is de veelgebruikte Engelse naam voor een kwetsbaarheid?
2. Wat is de Engelse naam voor een aanval die zo'n kwetsbaarheid uitbuit?
3. Hoe beperken moderne besturingssystemen de schade die een aanvaller kan aanrichten?
4. Je hebt net een nieuwe computer gekocht en aangezet, maar nog niet gebruikt. Heeft het toestel dan waarde voor een aanvaller?
5. Goede computerbeveiliging is iets dat je één keer regelt, en daarna niet meer aan denkt. Juist of fout?
6. Goede computerbeveiliging heeft geen nadelen. Juist of fout?
7. Nationale intelligentiediensten hebben de meeste middelen om geavanceerde cyberaanvallen uit te voeren. Zijn zij de grootste dreiging voor je IT-infrastructuur?
8. Het woord 'hacker' heeft veel connotaties. Kan een hacker je ook behulpzaam zijn?