

Het groene boekje over **internetbeveiliging**



NORMAN

www.norman.nl

Het groene boekje over **internetbeveiliging**

Hier vindt u informatie over veel voorkomende hedendaagse IT-bedreigingen en leert u hoe u deze kunt aanpakken, zowel op vaste als draadloze netwerken.

Norman is niet aansprakelijk voor enige vorm van verlies of schade die is ontstaan door het gebruik van de documentatie of door fouten of gebreken hierin, inclusief maar niet beperkt tot inkomstenderving.

De informatie in dit document kan zonder kennisgeving worden gewijzigd. Zonder de expliciete schriftelijke toestemming van Norman mag geen enkel deel van deze documentatie worden gereproduceerd of worden verzonden in welke vorm of op welke wijze dan ook, elektronisch of mechanisch, waaronder het maken van fotokopieën en het gebruik van opname- of gegevensopslag- en opzoeksysteem, voor welk doel dan ook, met uitzondering van persoonlijk gebruik door de koper.

Het Norman logo is een gedeponeerd handelsmerk van Norman ASA. Namen van producten die in deze documentatie worden genoemd, zijn handelsmerken of gedeponeerde handelsmerken van hun respectievelijke eigenaren. Deze worden alleen genoemd voor identificatiedoeleinden.

Copyright © 2010 Norman ASA.

Alle rechten voorbehouden.

Inhoudsopgave

Veilig op het internet	7
Hoe veilig te blijven op het internet - 10 adviezen	9
Voor gebruikers van draadloze netwerken	12
Veel voorkomende bedreigingen	14
Andere soorten bedreigingen	18
Verspreidingsmethodes	20
Proactieve vs. traditionele antivirusoplossingen	21

Veilig op het internet

Het is niet eenvoudig om de ontwikkelingen op het gebied van IT-beveiliging en criminaliteit bij te benen. Er is echter overduidelijk behoefte aan effectieve bescherming en daarom is enige kennis van de meest voorkomende bedreigingen onontbeerlijk. In deze brochure worden actuele en veel voorkomende bedreigingen beschreven, worden de effecten van malware op gebruikers toegelicht en wordt aangegeven welke maatregelen u kunt treffen om u te beschermen.

Computervirussen en andere bedreigingen voor IT-beveiliging zijn al geruime tijd een bekend probleem. Meer dan 25 jaar geleden werd het eerste computervirus ontdekt en sindsdien heeft het probleem zich in een alarmerend tempo verspreid.

De eerste virussen waren gericht op het vernietigen van computers en het veroorzaken van computercrashes, terwijl hedendaagse makers van kwaadaardige software veel graf-fineerder te werk gaan en vaak uit zijn op financieel voordeel.

De meest actieve virusmakers zijn vaak goed georganiseerd en passen geavanceerde methoden voor de verspreiding van malware (verzamel-naam voor virussen, trojans, wormen. etc.) toe.

Hackers kunnen uw privé-gegevens met financieel oogmerk stelen of uw surfgewoonten op het internet volgen om u aangepaste reclame te kunnen aanbieden. Sommige hackers verzamelen e-mailadressen op uw systeem om deze vervolgens aan andere bedrijven te verkopen.

OPMERKING

IT-criminelen zijn steeds beter georganiseerd en produceren steeds geavanceerdere bedreigingen.





Beveiliging van gebruiker

Op het internet loeren vele gevaren. Gebruikers van WLAN's (draadloze netwerken) en Bluetooth devices lopen meer gevaar dan anderen. Gebruikers van mobiele technologie moeten zich extra bewust zijn van de mogelijke gevaren die hun beveiliging in de weg staan. Mobiele gebruikers dienen hun Bluetooth-verbinding uit te schakelen wanneer deze niet wordt gebruikt. Het eerste waar een potentiële hacker naar zoekt is de SSID (Service Set Identifier), die niet te vinden is wanneer de verbinding is uitgeschakeld.

Een ander mogelijk gevaar betreft het risico van fysiek gegevensverlies. Nu steeds meer mensen thuis en buiten kantoor werken, wordt de kans op fysieke diefstal steeds groter. U dient voorzichtig te zijn met waar u uw laptop of externe memory sticks achterlaat.

Kwetsbaarheden en malware die deze exploiteert zijn inmiddels aangetroffen op mobiele telefoons en pinautomaten. Een voorbeeld is het Cabir virus dat zich via mobiele telefoons verspreidt.

Men kan verwachten dat apparatuur die steeds complexer wordt in de gebruikte computertechnologie, steeds kwetsbaarder wordt voor malware aanvallen.

Zie ook de aparte sectie op pagina 12, voor gebruikers van draadloze netwerken.



Hoe veilig te blijven op het internet - 10 adviezen

1 Laat nooit vreemden binnen

Zorg dat de pc goed is beveiligd voordat u verbinding maakt met internet. Het is van groot belang dat u zich bewust bent van gedeelde mappen of bronnen. Het is niet waarschijnlijk dat u uw persoonlijke gegevens wilt vrijgeven aan de gehele internetgemeenschap. Dit gebeurt echter wel wanneer u uw gegevens op een onveilige manier opslaat. Dit is een van de grootste beveiligingsrisico's van Windows-systemen waarvan door indringers veelvuldig misbruik wordt gemaakt. Ook dient u de pc uit te schakelen wanneer deze niet wordt gebruikt.

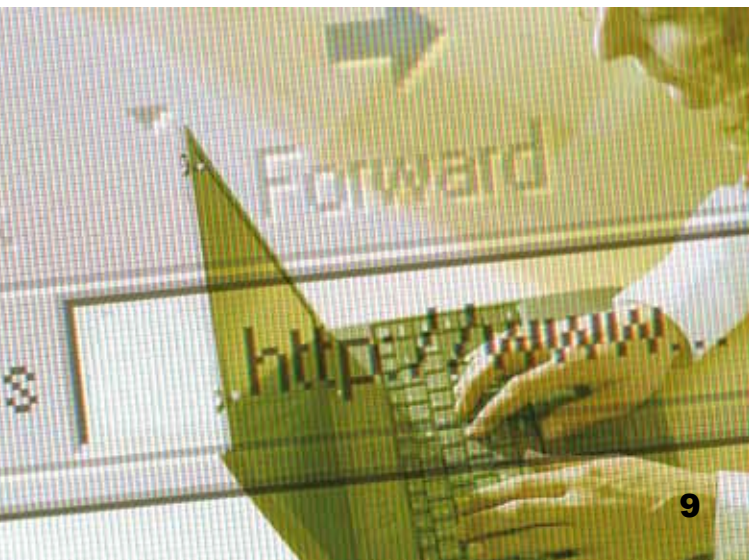
2 Gebruik professionele 'opschoners'

De installatie van antivirussoftware is een verplichte beveiligingsmaatregel. Het is echter al even belangrijk dat de antivirussoftware regelmatig wordt bijgewerkt, bij voorkeur automatisch zodra verbinding wordt gemaakt met internet.

De installatie van producten voor het verwijderen van spyware en adware kan u helpen om uw systemen ervan te vrijwaren. Ook is het verstandig uw inkomende e-mailberichten te laten scannen door een antivirusproduct voordat deze uw systeem binnenkomen.

3 Werk het besturings-systeem coninu bij

Het besturingssysteem vormt de kern van alle activiteiten op een pc. Een besturingssysteem dat volledig vrij is van softwarefouten bestaat niet. Virusschrijvers/ontwikkelaars doen vaak hun voordeel met dergelijke fouten. Het is dan ook van belang dat alle belangrijke beveiligingsupdates continu worden gedownload en geïnstalleerd zodra deze beschikbaar zijn. Bij de modernere besturings-systemen (o.a. Windows 7, XP met SP2) is het mogelijk automatisch beveiligingsupdates te laten ophalen en installeren. Het is verstandig deze functionaliteit te activeren.



4 Beoordeel ingekomen berichten kritisch

Gebruik uw gezond verstand. Als een van de volgende omschrijvingen van toepassing is, verwijderd u het e-mailbericht.

- De afzender is niet bekend.
- De tekst in het veld 'Onderwerp' zegt u helemaal niets.
- Het e-mailbericht bevat een koppeling, maar u weet niet precies naar welke internetlocatie deze u zal leiden.
- Het e-mailbericht zelf is verdacht.
- Het e-mailbericht bevat een verdachte bijlage.
- Het e-mailbericht lijkt afkomstig te zijn van een software leverancier en bevat als bijlage een programma dat een beveiligings-update zou zijn. Software leveranciers verzenden nooit beveiligingsupdates als groot-schalige mailings!

OPMERKING

Softwareleveranciers verzenden nooit beveiligingsupdates als grootschalige mailings.

- Gebruik van de voorbeeldweergave in e-mailclients vormt een beveiligingsrisico. U dient deze dus uit te schakelen, zodat u ongewenste e-mails kunt verwijderen zonder dat deze worden geopend.
- Een spamfilter kan u een aanzienlijke hoeveelheid tijd en frustratie besparen bij het opschonen van ongewenste e-mailberichten die vaak kwaadaardige software bevatten. U dient spamberichten nooit te beantwoorden. Beantwoorden van deze spam bevestigt de spamverspreider dat het e-mailadres gebruikt wordt, actief is en dus misbruikt kan worden.
- U moet vertrouwelijke informatie coderen voordat u deze verzendt.

5 Gebruik een betrouwbare 'portier'

Een computer heeft vele poorten (ingangen) voor verschillende taken. Open poorten kunnen worden gebruikt voor onbeperkte toegang tot bronnen op de computer. Zo wordt poort 25 bijvoorbeeld doorgaans voor e-mail gebruikt. De meeste spammers gebruiken dan ook deze poort. Poort 80 is de standaardpoort voor webtoegang. Het voornaamste doel van een personal firewall is het beschermen van de computer tegen 'bezoekers' (met andere woorden, aanvallen) via internet. De meeste firewalls kunnen ook worden geconfigureerd om toegang voor bepaalde adressen te blokkeren.

6 Sluit 'archiefkasten' met gevoelige informatie af

Sla vertrouwelijke gegevens veilig op. Dit is met name van belang waar het gegevens op draagbare computers betreft die in verkeerde handen terecht kunnen komen. De beste oplossing is om gebruik te maken van coderings-toepassingen die zowel mappen als afzonderlijke bestanden kunnen verwerken.

7 Geef niet iedereen toegang

Stel uw internetbrowser zodanig in dat wordt gevraagd of u 'actieve inhoud' toestaat. Vele websites maken gebruik van scripts en andere typen programma's om uw surfervaring te verbeteren. Dit vormt echter een beveiligingsrisico doordat hiervoor programmacode wordt uitgevoerd op de computer. Wees kritisch voor wat betreft de websites die u toegang geeft tot uw eigen computer en voor wat betreft programma's die u downloadt via het web en via P2P-programma's (peer-to-peer) zoals Kazaa.



8 Volg de raad op van ervaren IT medewerkers

Wanneer u een kantoor aan huis heeft of een draagbare computer gebruikt voor uw dagelijkse werkzaamheden, moet u eerst goed op de hoogte zijn van de regels van de werkgever met betrekking tot IT-beveiliging. Door de IT-medewerkers van het bedrijf te raadplegen, vermijdt u mogelijk vele problemen in de toekomst.

OPMERKING

Wees voorzichtig met het vrijgeven van privé-gegevens op het internet.

9 Geef zo min mogelijk persoonlijke gegevens door

Geef nooit persoonlijke gegevens door, tenzij dit absoluut noodzakelijk is. Het is raadzaam voor verschillende aanvragen verschillende e-mailadressen te gebruiken.

10 Maak een reservekopie van relevante gegevens

Gegevens kunnen per ongeluk, door een virus, door andere kwaadaardige codes of door kwaadwillenden met toegang tot uw gegevens, worden gewist.

Maak regelmatig reservekopieën van essentiële gegevens.

De bestanden waarvan het maken veel tijd en moeite heeft gekost, vormen de belangrijkste gegevens. Software en andere systeembestanden kunnen opnieuw worden geïnstalleerd wanneer deze zijn beschadigd.



Voor gebruikers van draadloze netwerken

Gebruikers van WLAN's (draadloze netwerken) moeten extra voorzorgsmaatregelen treffen om optimaal beschermd te zijn. Een draadloos netwerk is handig en effectief voor gebruikers, maar is tegelijkertijd gemakkelijk toegankelijk en dus kwetsbaar voor indringers en onrechtmatige gebruikers. Als u uw draadloze netwerksysteem niet beschermt of vergrendelt, kan men er heimelijk toegang toe verkrijgen om het vervolgens bijvoorbeeld te gebruiken voor illegale downloads of voor de distributie van spam. In het ergste geval kunnen indringers toegang tot uw computer krijgen.

Hier volgt een aantal adviezen voor gebruikers van draadloze netwerken:

Beveilig uw netwerk met een autorisatiesleutel

In de gebruikersdocumentatie kunt u lezen hoe u dit doet. Het is een eenvoudige procedure die door iedereen kan worden uitgevoerd: u hoeft alleen maar de juiste code voor toegang tot het netwerk in te voeren. Als u een autorisatiesleutel inschakelt, weet u zeker

dat alleen computers met de juiste sleutel toegang tot uw privé-netwerk kunnen krijgen, en dat het verkeer op het netwerk wordt gecodeerd. De meest gebruikte coderingsmethoden zijn WEP en WPA.

OPMERKING

Schakel de computer altijd uit als deze niet in gebruik is.

Gebruik antivirusprogramma's

Net als andere netwerkgebruikers, hebben ook gebruikers van draadloze netwerken de bescherming van een antivirusprogramma nodig. Draadloze netwerken zijn extra kwetsbaar, en antivirussoftware beschermt u tegen virussen, worms, trojans en andere kwaadaardige software (malware).

De beste programma's zijn proactieve antivirusoplossingen die niet afhankelijk zijn van traditionele technologie op basis van signatures. Proactieve antivirusoplossingen detecteren nieuwe en onbekende virussen en zorgen daarmee voor effectievere bescherming van uw computer.



Gebruik programma's voor het verwijderen van spyware en adware

Deze programma's verwijderen spyware en voorkomen dat uw internet-activiteiten kunnen worden bijgehouden.

Codeer uw privé-gegevens

U wilt uw gegevens niet zo maar met iedereen delen. De beste manier om uw privacy te waarborgen is door uw bestanden te coderen.

U kunt een coderingsprogramma installeren en e-mailberichten, privé-bestanden, bedrijfsinformatie, vertrouwelijke dossiers en e-mailbijlagen coderen.



Veel voorkomende bedreigingen

U kunt als gebruiker schade ondervinden van verschillende bedreigingen. Dit zijn de meest voorkomende bedreigingen:

Malware

Malware is de algemene benaming voor kwaadaardige code die erop is gericht om een computersysteem te storen of te vernietigen.

Hieronder vindt u korte beschrijvingen van een aantal veel voorkomende typen malware.

1 Virus

Een computervirus is een programma dat erop is gericht zichzelf te kopiëren en te verspreiden, meestal door zich aan toepassingen te hechten. Wanneer een geïnfecteerde toepassing wordt uitgevoerd, kan deze andere bestanden infecteren. Voor de verspreiding van een virus over computers en systemen is actie van een gebruiker nodig. Dit kan bijvoorbeeld gaan om het downloaden van bestanden, het verwisselen van diskettes en USB-sticks, het kopiëren van bestanden van en naar bestandsservers of het verzenden/openen van geïnfecteerde e-mail bijlagen.

Een virus kan verschillende verschijningsvormen hebben:

Bestandsvirus:

Een bestandsvirus is aan een programmabestand gehecht. Het gebruikt uiteenlopende technieken om andere programmabestanden te infecteren. Dit type virus kan van/naar allerlei typen opslagmedia (alleen naar devices die beschrijfbaar zijn) en via het netwerk worden overgebracht.

Systeemvirus:

Systeemvirussen, ook wel bootvirussen genoemd, staan vaak op USB sticks en CD's zonder dat de

gebruiker zich hiervan bewust is. Wanneer een gebruiker de computer (opnieuw) opstart, worden de master-bootsector en systeembootsector door het systeemvirus geïnfecteerd als de computer wordt opgestart van een opstart device (zoals bijvoorbeeld USB sticks en CD's).

Droppervirus:

Een dropper is een programma dat is gemaakt of aangepast om een virus op de doelcomputer te "installeren". De dropper is in feite de verpakking waarin het virus zit. De infectie is een feit wanneer het virus op de computer is geïnstalleerd. Het virus zelf wordt verspreid, niet de dropper. De dropper kan een naam zoals README.exe hebben, waarmee de nieuwsgierigheid van de gebruiker wordt gewekt en deze eerder geneigd zal zijn het bestand te openen. Een dropper is eigenlijk een trojan, bedoeld voor de installatie van een virus.

Macrovirus:

Macrovirussen kunnen worden opgenomen in typen bestanden waarbij een macrotaal wordt gebruikt, zoals Word, Access en Excel. Het virus wordt van het ene naar het andere document overgebracht. De infectie vindt plaats wanneer het document wordt geopend.



Enkele jaren geleden waren macro-virussen een “populaire” malware soort. De laatste tijd worden deze minder vaak wijd verspreid en nieuwe varianten verschijnen minder frequent als andere soorten malware.

2 Worms

Een netwerkworm infecteert andere computers en verspreidt zich automatisch over een netwerk, zonder dat daarvoor actie van gebruikers nodig is. Aangezien er voor de verspreiding geen actie van gebruikers nodig is, verloopt de verspreiding veel sneller dan bij een virus. Een netwerkworm kan geïnjecteerd worden met behulp van bijvoorbeeld een USB-stick of via een e-mail bijlage.

Wormen kunnen ook via e-mail worden overgebracht, vaak zonder dat de geïnfecteerde gebruiker zich hiervan bewust is. Een typische e-mailworm verzendt zichzelf naar alle e-mail adressen die op de geïnfecteerde pc te vinden zijn. De e-mail lijkt dan afkomstig te zijn van de geïnfecteerde gebruiker, die u dus mogelijk kent, zodat u wellicht niet op uw hoede zult zijn.

3 Trojan

Een trojan (Trojaans paard/Trojan horse) is een programma dat op het eerste gezicht onschuldig lijkt. Het kan zelfs nuttig lijken, zodat u in verleiding wordt gebracht het programma te gebruiken. Terwijl het programma vervolgens wordt uitgevoerd, zou de trojan backdoor(s) kunnen openen zodat uw computer bloot wordt gesteld aan hackers. De onmiddellijke schade is doorgaans niet noemenswaardig, maar de computer is nu onbeschermd, zodat criminelen gevoelige informatie kunnen stelen en/of op afstand de controle over de computer overnemen voor kwaadaardige doeleinden.

4 Spyware

Onder spyware verstaan we elke vorm van technologie die wordt gebruikt om informatie over een persoon of organisatie te verzamelen zonder medeweten of toestemming van de betreffende persoon of organisatie. Spyware wordt vaak heimelijk geïnstalleerd, wanneer er een bestand wordt gedownload of wanneer u op pop-up reclame klikt. Er kan ook spyware in uw hardware geïmplementeerd zijn.

OPMERKING

De meeste spywareprogramma's zijn niet eenvoudig te verwijderen.

Spyware programma's kunnen de auto-signatures resetten en/of verwijderen, voorkeuren veranderen, ze kunnen de toetsaanslagen monitoren, zichzelf toegang verschaffen tot applicaties, websites veranderen, met als doel reclame materiaal online of offline te plaatsen.

Er bestaan diverse categorieën spyware:

Adwarenetwerken:

De meest wijdverspreide spyware vertrouwt op adwarenetwerken die uitgevers van spelletjes, hulp-programma's en muziek-/videospelers een vergoeding per download betalen om hun adware-programma's erin op te nemen.

Stalking horses:

Een aantal programma's die adwarenetwerken in staat stellen op het bureaublad van een computer te werken. Soms worden deze gebundeld met populaire toepassingen en tijdens installatie aangeboden als interessante uitbreiding van de toepassing. Deze programma's verzamelen allemaal informatie.

Backdoor Santa's:

Zelfstandige programma's met een soortgelijke aanpak, die echter geen koppelingen naar adwarenetwerken gebruiken, maar wel informatie van gebruikers verzamelen.

Cookies:

In sommige browsers is het mogelijk dat informatie uit bestaande cookies nog steeds wordt

verzonden, zelfs als cookies in de browserinstellingen zijn uitgeschakeld. U dient alle cookie-bestanden op het systeem handmatig te verwijderen om te voorkomen dat uw activiteiten kunnen worden bijgehouden door adware-netwerken van derden of door providers van spyware of adware.

Spywareprogramma's kunnen uw automatische handtekening opnieuw instellen, uw installatiefuncties uitschakelen of omzeilen, uw toetsaanslagen bijhouden, bestanden op het station scannen, toegang krijgen tot toepassingen, startpagina's veranderen en zowel on line als off line reclame weer geven.

Zij kunnen bestanden lezen, schrijven en verwijderen en zelfs het vasteschijfstation opnieuw formatteren, terwijl er tegelijkertijd continu gegevens stromen naar degene die de spyware bestuurt.

Als deze programma's eenmaal zijn geïnstalleerd, kunnen deze meestal niet gemakkelijk via standaardmethoden van het systeem worden verwijderd. Zij laten vaak onderdelen achter die doorgaan met het bijhouden van uw activiteiten en zichzelf opnieuw installeren. Spyware kan niet alleen in legitieme software-producten zijn opgenomen, maar kan ook op uw computer worden geïnstalleerd terwijl u op internet surft.

OPMERKING

De beste programma's zijn proactieve antivirusoplossingen die niet afhankelijk zijn van traditionele technologie met signaturen.

5 Adware

Adware is nauw gerelateerd aan spyware, en veel spywareprogramma's worden geïnstalleerd met de bedoeling om adware-programma's uit te voeren. Met adware software wordt reclame weergegeven, meestal in de vorm van pop-ups. Deze zijn specifiek aan u als gebruiker aangepast, voornamelijk op basis van uw activiteiten (gedrag) op internet die door Spyware "bekenen" worden.

6 Backdoor

Een backdoor is een programma dat uw computer openstelt voor toegang waarvoor u geen toestemming hebt gegeven. Dergelijke backdoors kunnen dus externe toegang mogelijk maken, waarbij de verificatieschema's die u mogelijk ter beveiliging hebt ingesteld, worden omzeild. De backdoorprogramma's openen doorgaans bepaalde poorten waarmee de maker verbinding probeert te maken. Als een hacker erin slaagt diverse computers met backdoors te infecteren, kan deze hele series computers scannen om deze te identificeren en voor

speciale taken te gebruiken, bijvoorbeeld als zombiecomputers (zie hierna).

7 Combinaties van malware

Recentelijk is er sprake van een snel stijgende tendens waarbij meerdere van de bovengenoemde bedreigingen tot malware worden gecombineerd. Wormen worden gebruikt voor de verspreiding van virussen die backdoors en spyware installeren, terwijl spyware-programma's worden gebruikt om aangepaste reclame naar u te leiden en zelfs om uw pc als e-mail server te gebruiken voor de verzending van spam (zie hierna).

Het meest zichtbaar echter, is de eigenschap dat malware zichzelf update door downloaden van nieuwe componenten via het Internet. Deze nieuwe modules kunnen van alles zijn, variërend van introductie van nieuwe type malware, tot nieuwe functionaliteit. Het onderscheid tussen deze verschillende soorten dreigingen wordt steeds minder duidelijk. De malware schrijvers worden nu gedreven door commerciële





belangen en beschikken over substantiële middelen.

Andere soorten bedreigingen

1 Spam

Spam kan worden gedefinieerd als ongewenste e-mailberichten die willekeurig op grote schaal worden verzonden. Dit vormt een bijzonder efficiënte en goedkope manier om producten onder de aandacht te brengen. De meeste gebruikers worden blootgesteld aan spam, wat wordt bevestigd door enquêtes die uitwijzen dat meer dan 95% van alle e-mailberichten uit spam bestaat.

OPMERKING

Enquêtes wijzen uit dat meer dan 95% van alle e-mailberichten uit spam bestaat.

Spam vormt geen directe bedreiging, maar het hoge aantal gegeneerde e-mailberichten en de tijd die organisaties en individuele gebruikers kwijt zijn aan het identificeren en verwijderen ervan, leiden tot ergernis en hoge kosten bij internetgebruikers. Spam wordt tevens gebruikt voor verzending van diverse soorten malware die hiervoor zijn beschreven.

2 Phishing

Phishing is het op frauduleuze wijze verwerven van gevoelige privé gegevens zoals wachtwoorden en creditcardgegevens, door vermomming als bijvoorbeeld een officieel aandoend e-mailbericht dat bedoeld is om over te komen als een betrouwbaar iemand die om legitieme redenen om gegevens vraagt. Als doelwit wordt vaak gekozen voor gebruikers van diensten voor internetbankieren en veiling-sites.

OPMERKING

Als doelwit voor phishing wordt vaak gekozen voor gebruikers van diensten voor internetbankieren.

Phishers gaan doorgaans te werk middels verzending van spam naar een groot aantal potentiële slachtoffers. Dergelijke e-mailberichten verwijzen de ontvanger naar een webpagina die bijvoorbeeld deel lijkt uit te maken van diens internetbank, maar waarop in werkelijkheid de accountgegevens worden vastgelegd met het oog op onrechtmatig gebruik door de phisher. Een speciale phishing variant is de zogenaamde “spear phishing”, deze richt zich

op een kleine groep bijvoorbeeld 'bedrijfsleiders'. Dit toont aan dat de phishing pogingen nog meer toegespitst en daarmee nog geavanceerder zijn geworden.

3 Pharming

Pharming is een geraffineerdere vorm van phishing. Pharmers maken misbruik van het DNS-systeem, het systeem vertaald een computeradres en probeert het om te zetten naar een IP-adres. Zo kunnen de pharmers bijvoorbeeld een onechte website presenteren die eruit ziet als de echte versie, bijvoorbeeld van de website van een bank, om vervolgens gegevens te verzamelen die de gebruikers aan hun echte bank denken te verstrekken. Pharming werd voorheen ook wel DNS-poisoning genoemd.

4 'Distributed Denial of Service'-aanvallen

Diverse toonaangevende websites zijn het slachtoffer geweest van zogenaamde 'Distributed Denial of Service'-aanvallen (DDoS attacks). Dergelijke aanvallen worden vaak uitgevoerd door meerdere robots die tegelijkertijd grote aantallen verzoeken naar een gegeven computer of netwerk verzenden. Hierdoor ondervindt het netwerk of de computer overmatige belasting, waardoor legitieme bewerkingen niet meer kunnen worden verwerkt. De aanvallende computers (robots) zijn vaak computers met open backdoors, zodat deze voor dit specifieke doel kunnen worden ingezet.

Waarschijnlijk zijn de meeste eigenaars van dergelijke computers zich niet bewust van dit bedrog en om deze reden worden de geïnfecteerde computers vaak 'zombies' genoemd. Deze 'zombies' worden door een hacker op afstand ingesteld en geactiveerd. Uw computer kan dus worden gebruikt voor het uitvoeren van illegale activiteiten.

5 Keyloggers

Keyloggers zijn erop gericht de toetsaanslagen van de gebruiker vast te leggen, voor een specifieke toepassing dan wel voor het gehele systeem. Keylogging stelt criminelen in staat specifieke gegevens op te sporen die kunnen worden gebruikt voor diefstal van legitimatie, diefstal van intellectueel eigendom of andere frauduleuze acties. Creditcardnummers, wachtwoorden en andere gevoelige gegevens kunnen op deze wijze worden gestolen.

6 Browser Helper Objects

Browser Helper Objects (BHO's) zijn plug-ins voor Internet Explorer. Een BHO heeft volledige toegang tot alles wat er in de huidige browsersessie gebeurt: een BHO kan zien welke pagina's worden weergegeven en hoe deze worden weergegeven en kan bovendien sites veranderen voordat deze worden weergegeven. Ondanks hun slechte reputatie worden BHO's vaak gebruikt voor legitieme doeleinden, zoals voor downloaden, knopinfo en pop-upverwijdering.

OPMERKING

Norman heeft diverse producten ontwikkeld die uw veiligheid op internet zeker stellen. Voor meer informatie kunt u terecht op www.norman.com

7 Valse beveiligingssoftware

Een speciaal soort dreiging wordt gevormd door software die claimt beveiligingssoftware te zijn, maar in feite malware is, die gebruikers die de software installeren probeert over te halen om geld

te laten betalen om volledig beschermd te zijn (wat ze ook na betaling niet zijn). Er zijn vele voorbeelden hiervan, in het bijzonder van software die zich manifesteert als antispyware en antivirus programma's.

Verspreidingsmethodes

In de vroege dagen van computervirussen, waren diskettes het voornaamste verspreidingsmechanisme. Dit type mediadrager wordt inmiddels nauwelijks meer gebruikt, en nieuwe en effectievere verspreidingstechnieken zijn ontwikkeld.

Tegenwoordig gebruikt malware vaak bekende kwetsbaarheden in verschillende applicaties en operating systemen om zich te verspreiden. Het is ook niet ongewoon dat malware probeert verschillende kwetsbaarheden in verschillende applicaties probeert te gebruiken.

E-mail bijlagen

Malware in e-mailbijlagen was de meest populaire verspreidingsmethode rond de eeuwwisseling. Bij deze gebruikte techniek waren e-mailbijlagen besmet en gebruikers werden verleid de bijlage te openen. Wanneer de bijlage geopend werd, werd de computer geïnfecteerd. Malware verspreiding via e-mail wordt vaak bereikt via mailwormen die zichzelf automatisch versturen zonder dat de (geïnfecteerde) gebruiker dit merkt.

Netwerkverspreiding

De meest gevaarlijke malware verspreiders binnen organisaties zijn degenen die zich verspreiden over netwerken, daarbij netwerkdrives infecterend. Eén geïnfecteerde computer kan een groot netwerk binnen enkele seconden infecteren.

Deze verspreidingsmechanismen via netwerken zijn zo snel en efficiënt, dat het extreem moeilijk is zulke besmettingen weer kwijt te raken.

USB sticks

Deze kunnen beschouwd worden als de opvolger van de diskette. Eenvoudig te vervoeren, met voldoende opslagcapaciteit, als het doel is om gegevens van de ene naar de nadere computer te verplaatsen. Helaas zijn het ook efficiënte malware verspreiders, speciaal als de autorun van computers is geactiveerd.

Omdat USB sticks zo klein zijn en op individuele computers ingeplugd worden, worden ze vaak niet opgenomen in de beveiligingsbeleid van organisaties betreffende het installeren van nieuwe apparatuur op het netwerk.

Geïnfecteerde websites

Een van de populairste verspreidingsvectoren op dit moment, zijn geïnfecteerde websites. De meeste van deze infecties zijn gedaan zonder toestemming of wetenschap van de website eigenaar- bijvoorbeeld door het exploiteren van een software kwetsbaarheid in de web server applicaties.

Onschuldige websurfers worden met een verscheidenheid aan technieken misleid om een geïnfecteerde website te bezoeken. Het resultaat is dat de surfers zelf besmet raken. Deze vorm van infectie wordt vaak "Drive-by-infection" genoemd.

Proactieve vs. traditionele antivirusoplossingen

Het verschil tussen traditionele, op signaturen gebaseerde antivirusoplossingen en de nieuwe, proactieve antivirustechnologie kan doorslaggevend zijn voor het welzijn van uw computersystemen.

Proactieve oplossingen kunnen nieuwe bedreigingen detecteren die oplossingen op basis van signaturen niet aan kunnen. Nu virusmakers steeds geraffineerder worden en nieuwe virusvarianten het net overspoelen, zijn traditionele oplossingen niet langer afdoende. Er is dringend behoefte aan proactieve oplossingen.

Hieronder volgt een korte beschrijving van de twee technologieën.

Traditionele oplossingen

Bij traditionele antivirusoplossingen op basis van signaturen, moet een virus door iemand worden ontdekt, als virus worden herkend en worden geanalyseerd voordat antivirusbedrijven de juiste bescherming kunnen bieden. Pas na deze noodzakelijke eerste stappen kan er een virus-signatuurbestand worden gepubliceerd. Het duurt gemiddeld 6 tot 24 uur voordat er een bijgewerkt signatuurbestand wordt gedistribueerd. Dit bestand wordt gebruikt om het antivirusprogramma van alle klanten bij te werken, zodat de pogingen tot virusinfectie vanaf dat moment kunnen worden gestopt. De periode tussen het moment waarop het virus wordt uitgebracht en het moment waarop er een bijgewerkt signatuurbestand wordt gedistribueerd, is uiteraard cruciaal voor gebruikers die nog steeds het risico lopen van infectie door het virus.

Proactieve oplossingen

Een proactieve antivirusoplossing detecteert nieuwe en onbekende virussen zonder bijgewerkte signatuurbestanden.

Norman SandBox®

Dit is in feite een volledig gesimuleerde computeromgeving die is geïsoleerd van de feitelijke verwerkingsomgeving.

Alle inkomende bestanden komen de gesimuleerde computer (de SandBox) binnen. Hier worden de bestanden in de gaten gehouden en als er verdachte actie wordt waargenomen, wordt het betreffende bestand gestopt en wordt het de toegang tot de feitelijke computer ontzegd. Als het bestand zich conform verwachting gedraagt, krijgt het toegang tot de feitelijke computer. Zogenaamde 'Day Zero'-aanvallen (aanvallen die plaatsvinden op de dag waarop een zwakheid in software bekend wordt en er een kwaadaardig programma wordt gemaakt dat misbruik maakt van deze zwakheid) vormen een steeds grotere bedreiging. Alleen proactieve oplossingen kunnen afrekenen met deze bedreiging.

OPMERKING

U kunt uw bestanden gratis op virussen controleren via Norman SandBox Center. U kunt hiervoor terecht op <http://sand-box.norman.no>

Norman DNA Matching

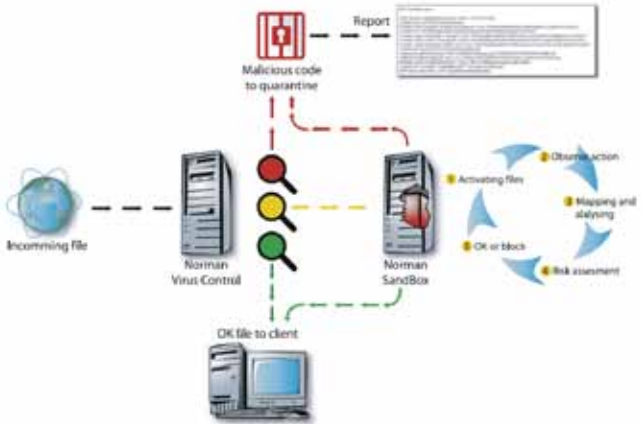
Computer code en instructies kunnen worden gezien als de sequenties van het 'DNA profiel' van een programma. Norman gebruikt deze benadering om nieuwe malware te stoppen, waarvoor nog geen signature is. Indien nieuwe malware een mutatie lijkt van een bekende soort, doordat het dezelfde of gelijksoortige kwaadaardige code gebruikt, kunnen

we concluderen dat dit waarschijnlijk malware van dezelfde familie is. Als nieuwe onbekende programma's gemaakt en verspreid worden, gebruikt Norman de NDA Matching technologie om te bepalen of deze programma's kwaadaardig, verdacht of legaal gedrag vertonen. Als het nieuwe programma veel kwaadaardig DNA bevat, is het programma zelf waarschijnlijk ook kwaadaardig.

Norman Exploit Detection

Is een technologie om malware te detecteren die kwetsbaarheden uitbuit in veelgebruikte documenttypes zoals OLE2 (Office documenten), MDB (Access), WMF (Windows Meta File), JPEG (foto's), RIFF (Windows media meta-formaat) en SWF (Flash).





Oases:

Met een virtuele pc met toeters en bellen zijn we er echter nog niet. Waar virussen zich vroeger verspreiden door zich in de boot-sector van een diskette of exe-bestand te nestelen, wordt tegenwoordig steeds vaker internet gebruikt. De meest succesvolle virussen van de laatste jaren verspreiden zichzelf gewoon per mail.

Het is voor een virus namelijk helemaal niet zo ingewikkeld om op een besmette pc e-mailadressen bij elkaar te sprokkelen en daar dan zonder dat de gebruiker het merkt berichten naartoe te sturen. Als die mailtjes weer het virus bevatten en door de geadresseerden worden geopend, kan de verspreiding erg snel gaan!

De Norman SandBox® is dan ook meer dan een zandbak. Het is een enorme woestijn met naast de virtuele pc nog veel andere oases. Zo is er een compleet netwerk, waardoor een virus dat e-mail gaat versturen net als in de buitenwereld het ip-nummer van de juiste mailserver kan achterhalen. Alleen krijgt hij die informatie natuurlijk niet van een echte, maar van een virtuele DNS-server in de SandBox. En dat ip-nummer zelf zal natuurlijk

ook van een virtuele mailserver in diezelfde SandBox zijn. Kortom: een virus kan zich lekker uitleven en terwijl het zich denkt te verspreiden, komt het in werkelijkheid de zandbak niet uit. En de virusscanner kijkt rustig toe wat er gebeurt. Een ander geintje dat virussen gebruiken, is het ophalen van een stukje programmacode van een website om dat vervolgens uit te voeren. Op die manier hoeft schadelijke code niet in het virus zelf te zitten. Bovendien kan de maker van het virus die natuurlijk ook die website onder controle heeft zo nog op het allerlaatste moment bepalen wat het virus precies moet gaan doen, of wanneer. Ook dat soort trucs worden door de SandBox genadeloos blootgelegd. Een virus in de zandbak krijgt natuurlijk niets van de echte site, maar van een virtuele site. En de gegevens die op die manier door het virus worden opgehaald, kunnen natuurlijk eenvoudig worden gevolgd. Zodra het virus er dingen mee doet die niet door de beugel kunnen, valt het onmiddellijk door de mand.

bron: Oases, geschreven door: Robbert Wetmar voor PC-Active

Norman productenoverzicht voor de thuisgebruikers

Norman Security Pack

Norman Antivirus & AntiSpyware gedurende 1 jaar voor 2 gebruikers.

Norman Security Suite

Norman Antivirus & AntiSpyware gedurende 1 jaar voor 3 gebruikers.

Personal Firewall, Parental Control, Screensaver scanner

Norman Security Suite

Norman Antivirus & AntiSpyware gedurende 3 jaar voor 3 gebruikers.

Personal Firewall, Parental Control, Screensaver scanner

Norman Security Suite PRO

Norman Antivirus & AntiSpyware gedurende 1 jaar voor 5 gebruikers.

Personal Firewall, Parental Control, Screensaver scanner, Antispam,

Intrusion Guard & Privacy Tools

Norman Security Suite PRO

Norman Antivirus & AntiSpyware gedurende 3 jaar voor 5 gebruikers.

Personal Firewall, Parental Control, Screensaver scanner, Antispam,

Intrusion Guard & Privacy Tools

Norman SOHO (Norman Small Office Home Office)

Licentie voor Windows Home Server of een SBS server met max. 5 werkstations.

Voor meer info zie onze website: <http://www.norman.com/support/53590/nl>

Producten portfolio voor MKB/KMO of groter zie onze website: <http://www.norman.nl>

Norman ASA is in 1984 opgericht in Oslo Noorwegen en is een wereldleider en pionier in proactieve beveiligingsoplossingen en forensische malware tools. Miljoenen gebruikers vertrouwen op de Norman oplossingen zoals bijvoorbeeld netwerkbeveiliging, endpoint beveiligingsoplossingen en malware analyse tools, om hun waardevolle data te beschermen.

Norman biedt als technologisch leverancier- proactieve antim malware technologie die wereldwijd wordt gebruikt door verschillende beveiligingsoplossingen en services. Norman's proactieve antim malware oplossingen worden gedreven door gepatenteerde technologie: de Norman SandBox[®].



Notities

Norman Data Defense Systems B.V.

Diamantlaan 4, 2132 WV Hoofddorp, www.norman.nl
Tel: 023-78 90 222 | Fax: 023-56 13 165 | info@norman.nl

Norman ASA is in 1984 opgericht in Oslo Noorwegen en is een wereldleider en pionier in proactieve beveiligingsoplossingen en forensische malware tools. Miljoenen gebruikers vertrouwen op de Norman oplossingen zoals bijvoorbeeld netwerkbeveiliging, endpoint beveiligingsoplossingen en malware analyse tools, om hun waardevolle data te beschermen.

Dealerstempel

ref: 2010-150200002



NORMAN®

www.norman.nl