VIRUSPROTECTIE EN HET NETWERK

STAND VAN ZAKEN

Je zou als systeembeheerder geneigd zijn te denken dat het onderwerp 'virussen op het net' oud nieuws is. Aan de ene kant is het dat ook, maar alleen omdat het voorkomen (in beide opzichten) van virussen al wat langer dagelijkse praktijk is. En niet dat er patches beschikbaar worden gemaakt voor verouderde virussen, maar de ontwikkelingen staan ook op dat gebied, helaas, niet stil. Ernst Oud, in het dagelijks leven Security Consultant bij Crypsys Data Security, praat ons bij.

In relatief korte tijd zijn computervirussen een niet meer weg te denken fenomeen geworden, waartegen elke systeembeheerder maatregelen dient te nemen om de beschikbaarheid van het netwerk en de authenticiteit van daarin opgeslagen data te kunnen waarborgen. Hoewel inmiddels ruim 12.000 virussen circuleren en er maandelijks enkele honderden bijkomen, lijkt het alsof veel mensen het probleem als opgelost beschouwen. Gezien de stroom van nieuwe ontwikkelingen, zoals de opkomst van het internet, de macro-virussen en natuurlijk de zorgen rond Java(Script) en ActiveX en andere actieve componenten ingekapseld in bestanden, is het desalniettemin zinvol het probleem van computervirussen weer eens opnieuw te beschouwen.

Alvorens verder te gaan dienen we natuurlijk vast te stellen wat we onder een virus verstaan. Een computervirus bestaat uit executable code welke bij uitvoering één of meerdere replica's van zichzelf produceert en andere uitvoerbare code automatisch infecteert met deze replica's. Hoewel zeker niet als voorwaarde gesteld aan een virus, bevat deze soms een 'payload': code die onder een bepaalde voorwaarde, de 'trigger', geactiveerd wordt en acties onderneemt. De ondernomen acties zijn zeer divers en variëren van het laten horen van geluiden tot het verschijnen van boodschappen en het wissen van gegevens.

De definitie is met opzet ruim gekozen. Doordat vrijwel dagelijks nieuwe vormen van 'executable code' verschijnen, ontstaan regelmatig nieuwe families van virussen. Zo maakte de mogelijkheid tot het plaatsen van macro's in documenten en de kracht van de macro-taal de familie van macro-virussen in korte tijd de meest verspreide vorm van virussen van vandaag.

Historie

Voordat we echter direct naar de huidige problemen kijken is het nuttig kennis te vergaren uit de historie. Reeds in de jaren zestig toonde Fred Cohen aan dat een zichzelf reproducerend programma mogelijk was. Men vermoedde dat dergelijke programma's zelfs nuttig zouden zijn. Gedacht werd bijvoorbeeld aan 'agents', hoewel deze term veel moderner is, die in netwerken tijdelijke bestanden zouden kunnen opruimen zonder interventie van gebruikers. Net zoals bij biologische virussen is een bepaalde populatie noodzakelijk binnen de omgeving van het virus en spelen zaken als incubatietijd, eenvoud van overdracht van de infectie en dergelijke een belangrijke rol. Een computervirus geschreven voor een weinig voorkomende variant van een bepaald besturingssysteem zal zich moeilijk kunnen verspreiden. Simpelweg omdat de kans voor het virus een geschikte gastheer te vinden klein is. Het duurde dan ook feitelijk tot het midden van de tachtiger jaren voordat computervirussen een probleem werden. Rond die tijd waren er immers, door het succes van de personal computer, genoeg geschikte gastheren. Bovendien was een geschikte gastheer snel voorhanden door de toenemende uitwisseling van bestanden via netwerken en media zoals diskettes.

Doordat de populatie van gastheren, personal computers, zeer groot is en een relatief groot aantal daarvan nog steeds geen protectie kent, is de kans op een 'succesje' nog steeds groot en blijkt het voor sommigen kennelijk een intellectuele uitdaging om nieuwe virussen te ontwikkelen. De aanbieders van anti-virus produkten ontdekken nu tussen de vijf en tien nieuwe virussen of varianten per dag.

Overigens is deze groei vrij constant en kan de anti-virus industrie hierdoor het probleem nog steeds goed aan, hoewel de druk een aantal aanbieders uit de markt heeft doen verdwijnen.

Soorten virussen

Gezien het feit dat executable code binnen een personal computer op vele plaatsen voorkomt, is er voor een virus keuze bij het kiezen van de gastheer. Vandaar dat virussen in een aantal groepen worden ingedeeld, gebaseerd op het type gastheer. De meest belangrijke vormen zijn bootvirussen, welke actief worden door het uitvoeren van de code die een personal computer opstart, en parasitaire virussen, welke zich bijvoorbeeld nestelen in programmatuur. Ook combinaties komen voor, de zogenaamde multi-partite virussen. Virussen die zich zowel in bootcode als in programmatuur nestelen.

Een zeer veel voorkomende en een vorm met grote potentie vormen de macro-virussen waarover later meer. Naast computervirussen bestaat ook een aantal vormen van uitvoerbare code met kwade bijbedoelingen, die vaak verward worden met de term virus. Het betreft hier onder andere 'trojan-horses': programma's die een andere uitwerking hebben dan de gebruiker op het oog had. Een schoolvoorbeeld daarvan is het programma ARC513.EXE, dat de gebruiker doet vermoeden dat het een nieuwe versie van het bekende ARC archiverings-programma betreft. in werkelijkheid wist het programma bestanden. Tegen 'trojan-horses' helpt alleen isolatie: het gebruik van programmatuur op aparte hardware, totdat zeker is dat de software de gewenste functionaliteit bezit.

Programma's die zichzelf in zijn geheel repliceren, zonder infectie in een gastheer-programma, worden 'worms' genoemd. Deze vorm is voor verspreiding veelal afhankelijk van fouten in systeemsoftware. Een voorbeeld daarvan is de UNIX Internet-worm die in 1988 het Internet lam legde door gebruik te maken van fouten in sendmail en fingerd.

Doordat aan specifieke voorwaarden moet worden voldaan, is de verspreiding van worms doorgaans gering en daarmee ook het risico geïnfecteerd te raken. Tegen 'worms' helpt het up-to-date houden van je systeemsoftware met de laatste security patches die fabrikanten ter beschikking stellen.

Hoewel de media begin jaren negentig vaak suggereerden dat de wereld aan zijn einde kwam door een alles vernietigend computervirus, is het klaarblijkelijk mogelijk besmetting door een computervirus te voorkomen. De wereld is immers nog steeds niet aan zijn eind. Relevant is echter dat iemand die verantwoordelijk is voor de protectie, veelal de systeembeheerder, zich regelmatig afvraagt of het netwerk (server en werkstations) nog wel optimaal beveiligd zijn. Het zonder voorzorgsmaatregelen aansluiten van een modem aan een werkplek kan de tot dat moment perfecte protectie verlagen. Het overschakelen van een bedrijf van WordPerfect naar MS-Word stelt het bedrijf opeens bloot aan macro-virussen. Zelfs een nieuwe werknemer met als hobby computerspelletjes kan een bedreiging vormen. Volledige protectie is onmogelijk, maar gezond verstand en goede hulpmiddelen bieden, in combinatie met back-ups, dataverzekering en continuïteitsplanning, de zekerheid dat virussen geen kans krijgen.

Oplossingen

Strategische oorlogvoering begint met het onderzoeken van je tegenstander. Wil je dus goede protectie bieden tegen computervirussen, dan moet je weten waar je risico loopt. Pas dan kun je nadenken over het verminderen van dat risico. Een perfect anti-virus produkt gebruiken op de werkplekken heeft geen zin als het bedrijf afhankelijk is van informatie op een niet-beveiligde server waarop de systeembeheerder werkt met uitgeschakelde protectie. Omdat hij vindt dat het installeren van nieuwe software dan sneller gaat...

Duidelijk moet zijn dat virusbesmetting altijd veroorzaakt wordt door menselijk handelen. De anti-virus strategie is in essentie simpel: als je voorkomt dat werknemers acties ondernemen die kunnen leiden tot virusbesmetting dan ben je klaar. En voorkomen is altijd beter dan genezen. Het helpt dus als werknemers verteld wordt welke acties kunnen leiden tot virusbesmetting. Dat kan door regelmatige training waarbij het bewustzijn verbeterd wordt. Aangezien besmetting echter in veel gevallen volledig onbewust plaatsvindt, vormen hulpmiddelen een absolute noodzaak.

Virussen besmetten een werkplek en/of server, doordat uitvoerbare code met daarin een virus opgestart wordt.

Elke weg waarlangs uitvoerbare code ontvangen en uitgevoerd wordt, vormt dus in principe een risico.

Worden deze wegen geblokkeerd of gecontroleerd op virussen, dan is protectie bereikt. Te denken valt dus aan blokkeren of reguleren van diskette gebruik (sloten of gebruik maken van diskloze PC's), blokkeren of reguleren van internet gebruik en blokkeren of reguleren van e-mail attachments (die een virus kunnen bevatten).

Veel systeembeheerders beseffen niet dat zij een aantal eenvoudige hulpmiddelen ter beschikking hebben om virusbesmetting te voorkomen of verspreiding tegen te gaan. Zo veroorzaken bootvirussen, na macro-virussen, de meeste besmettingen. En dat terwijl vrijwel alle moderne PC's in de BIOS zo ingesteld kunnen worden dat de bootvolgorde C:, A: is en niet A:, C:. Door van alle werkstations het opstarten van diskette te voorkomen, heb je kosteloos en zonder maandelijkse updates bereikt dat deze grote groep virussen geen kans meer krijgen.

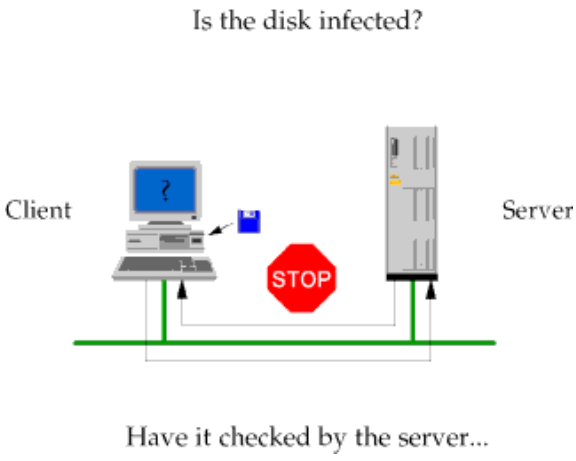
Veel systeembeheerders brengen de juiste toegangsrechten tot bestanden en directories niet aan. Nog altijd verspreiden virussen zich razendsnel in een netwerk omdat bijvoorbeeld LOGIN.EXE of CAPTURE.EXE voor de gebruikers niet tegen schrijven beveiligd is. Geen enkel virus kan 'toveren'. Als het netwerk een gebruiker geen schrijfrechten geeft in een bepaalde directory heeft geen enkel virus de kans om daar een besmetting te veroorzaken.

Controle

Is blokkeren niet wenselijk of mogelijk, dan blijft reguleren en controleren de enige mogelijkheid. Hiertoe dient alle dataverkeer via de desbetreffende weg, liefst transparant voor de gebruiker, op virussen gecontroleerd te worden. Wordt dus een diskette geplaatst en een programma van de diskette opgestart, dan dient een proces in te grijpen en transparant het programma te controleren voordat het uitgevoerd wordt. Hiertoe werd traditioneel onder DOS een TSR gebruikt, met een vervelend neveneffect: verminderde performance en verhoogd geheugengebruik - zeker in combinatie met de NetWare shell. Onder Windows3.x en Windows 95 vindt een dergelijke implementatie plaats via een VxD of DLL.

Op deze manier ontstaat een stand-alone viruscontrole met alle problemen van decentrale automatisering met betrekking tot onderhoud en support.

Het maandelijks updaten van vele werkstations met nieuwe software, al dan niet automatisch, vereist enige tijd. Een resource waar bij de systeembeheerder altijd schaarste aan is. Ideaal zou dus een anti-virus produkt op de werkplek zijn dat geen onderhoud vereist. Een aantal produkten in de markt kunnen controlegetallen (checksums) genereren van elk aanwezig bestand. Door interactief of real-time deze checksums te controleren wordt elke wijziging, al dan niet veroorzaakt door een virus, geconstateerd en gerapporteerd. Als normaal geen wijzigingen op een werkplek optreden dan kan deze software toegepast worden, anders ontstaan te veel meldingen die na verloop van tijd genegeerd worden. Met de moderne besturingssystemen - zoals Windows 95, waarbij diverse bestanden op schijf veranderen zonder dat de gebruiker zich dit bewust is, wordt checksumming software steeds minder bruikbaar. Wel kan een virusscanner checksumming gebruiken om te filteren welke bestanden gewijzigd zijn, om ze daarna te controleren zonder interventie van de gebruiker.



Een anti-virus oplossing volgens het client-server principe

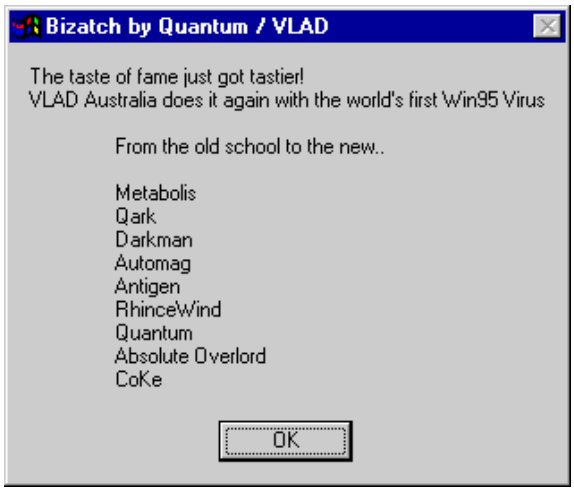
Een volledig client-server concept bestaat uit checksumming op de client en, bij constatering van verandering, controle op een anti-virus server in het netwerk. Hierdoor worden twee grote voordelen bereikt: de clients hoeven niet meer maandelijks onderhouden te worden (er is namelijk geen virus-specifieke software aanwezig) en de gehele anti-virus software staat op de server (de client wordt geladen vanuit de login procedure).

De anti-virus server kan natuurlijk onder NetWare een fileserver met een anti-virus NLM of onder NT een fileserver met een anti-virus service zijn. In dat laatste geval is van belang om na te gaan of het gebruikte produkt het security model van NT goed implementeert. Is dat niet het geval dan wordt bijvoorbeeld het door de gebruiker controleren van de bootsectoren van een diskette onmogelijk of onbetrouwbaar.

Ontwikkelingen

Bewezen kan worden dat elk besturings-systeem dat objecten (programma's, bestanden) vertrouwt en een open karakter kent, kwetsbaar is. Hieronder vallen alle bekende besturingssystemen.

Populaire besturingssystemen hebben een grote populatie en zijn goedkoop en vrij verkrijgbaar (waardoor ook de virusauteur er de beschikking over heeft) waardoor ze vaker het doelwit zijn van virusontwikkelaars. Uiteraard loopt MS-DOS hierin voorop.



Het eerste Windows 95 virus, een twijfelachtige eer

Er is slechts een beperkt aantal specifieke Windows 95 virussen en voor NetWare en Windows NT zijn slechts niet erg succesvolle pogingen gedaan. Helaas is het echter zo dat een groot deel van de MS-DOS virussen werkzaam zijn onder Windows 95 of NT. Dus ook indien alleen gebruik gemaakt wordt van moderne besturingssystemen blijft protectie nodig.

Helaas ontstaan de laatste tijd platform onafhankelijke, eenvoudig te programmeren, bijzonder populaire programmeeromgevingen binnen applicaties en besturingssystemen. De droom dus van elke kwade genius en een nieuwe intellectuele uitdaging.

Zonder compleet te willen zijn, kennen we nu Java, JavaScript en ActiveX als programmeertaal, binnen een Java of ActiveX engine, in een HTML browser of Office97, met in elke module Visual Basic for Applications. Een werkelijke doos van Pandora.

Links met nadere informatie

Virus Bulletin; het vakblad
http://www.virusbtn.com

Virussen en Office97
http://www.sophos.com/virusinfo/features/office97.html

Virussen en Internet
http://www.sophos.com/virusinfo/features/virusesintemet.html

Macro-virussen
http://www.sophos.com/virusinfo/techreports/macropro.html

Virussen en email
http://www.sophos.com/virusinfo/techreports/internet.html

Vermeende virussen
http://www.sophos.com/virusinfo/scares/

Java en virussen
http://www.sophos.com/virusinfo/scares/javaviruses.html

Computer Virus Helpdesk
http://iw1.indyweb.net/~cvhd/

Virus Test Center (duits)
http://agn-www.informatik.uni-hamburg.de/vtc/dt.htm

NetWare security workshop
http://www.sophos.com/productinfo/workshops/

Top 10 virussen deze maand
http://www.sophos.com/virusinfo/topten/

Gesteld kan worden dat op dit moment geen virus in Java geschreven is en dat virussen geschreven in JavaScript of ActiveX mogelijk en gedemonstreerd zijn. Voor de voorloper van Office97 zijn nu ruim 1000 virussen en veel daarvan werken onder Office97. Ook specifieke Office97 virussen bestaan reeds. Virussen in uitvoerbare objecten die de gebruiker niet als zodanig herkent, hebben gezien de enorm snelle verspreiding van Word macro-virussen een grote kans hun werk te doen zonder opgemerkt te worden. Realiseert u zich bijvoorbeeld dat dubbel klikken op een Word document betekent dat Word eventuele macro's in het document direct uitvoert? Protectie met een recent anti-virus product en regelmatige update daarvan is absolute noodzaak.

Zolang bedrijfskritische applicaties geen gebruik van Java(Script) of ActiveX vereisen, is het zeer de vraag of gebruikers eigenlijk wel de beschikking moeten hebben over browsers met ondersteuning van Java(Script) of ActiveX. Als dat al zo is, blijft isolatie van die werkplekken (dus losnemen uit het netwerk) de meest veilige keuze.

Een virusvrije toekomst is wellicht een utopie, maar dat hoeft niet te betekenen dat er nu geen goede oplossingen zijn. Kies een goede oplossing op basis van je eisen en wensen, je vertrouwen in de leverancier, de geboden support, de minimaal maandelijkse updates en een implementatie die je maandelijkse inspanningen minimaliseert. Grote kans dat je dan weinig last van virussen zult hebben.