'De Toekomst vaan Computervirussen

Verslag lezingavond, 17 juni jl.

Ernst J. Oud

Op 17 juni jl. ontving de afdeling Beveiliging in Utrecht bijna **100** leden voor de lezing "De toekomst van Computer Virussen". Sprekers waren uit Engeland Jan Hruska, technisch directeur van Sophos Plc., o.a. leverancier van SWEEP anti-virus software, en Albert Tuit, beveiligingsadviseur bij het Directoraat Generaal voor het Personenvervoer (DGP) van het Ministerie van Verkeer en Waterstaat.

De lezing van Jan Hruska schetste de geschiedenis van computer virussen waarbij duidelijk werd dat al een aantal jaren de vrijwel constante groei tussen de 200 en 300 nieuwe virussen per maand bedraagt. Het probleem is dus nog lang niet de wereld uit. Na een kort overzicht van de historie (met als belangrijkste herinnering de hype 'het eind van de IT industrie' in 1991 door het Michelangelo virus) schetste de heer Hruska de diverse typen virussen en maakte hij duidelijk dat tegenwoordig met name bootsector virussen en Word macro-virussen het meest bij gebruikers worden aangetroffen.

De heer Hruska noemde dat het Sophos onduidelijk is waarom bootsector virussen nog zo veel tot besmetting leiden daar elke moderne PC hier kosteloos tegen te beveiligen is door de volgorde voor schijfbenadering bij opstarten (in de BIOS setup) te veranderen van A:, C: naar C:, A:

Macrovirussen zijn in korte tijd enorm gegroeid, niet alleen qua aantal (er zijn vele honderden unieke exemplaren en varianten in omloop) maar ook qua aantal besmettingen op werkplekken. Door het uitwisselen van electronische documenten binnen grote groepen gebruikers, een normaal proces binnen organisaties, ligt het gevaar op de loer. De heer Hruska liet in een demonstratie zien dat een macrovirus altijd in broncode beschikbaar is waardoor kwaadwillenden bijzonder eenvoudig aanpassingen en daardoor nieuwe varianten kunnen maken. De tijd dat een virusprogrammeur machinetaal moest beheersen is ver achter ons.

Onder de moderne besturingssystemen, stilgestaan werd bij Windows NT, hebben veel 'oudere' computervirussen geen kans. Echter nieuwe kansen voor generaties virussen ontstaan door de opname van omgevingen waarin code uitgevoerd kan worden binnen applicaties. Een recente versie van een WWW browser bijvoorbeeld kent vele vormen van 'embedded objects', zoals Java, JavaScript, ActiveX Controls, binnen de browser met alle beveiligingsproblemen van dien.

De heer Hruska memoreerde de gevleugelde uitspraak dat "functionality always prevails over security". Macro's in documenten, automatische executie van macro's bij openen van een document, opname van executable code in web pagina's; het zijn allemaal voorbeelden van functies waarvan de beveiligingsaspecten (te) laat duidelijk worden. En wordt er van te voren goed nagedacht over beveiliging, de heer Hruska noemde Java en JavaScript als voorbeeld, dan wordt de software qua beveiliging niet sluitend geïmplementeerd, waardoor vele gaten in de beveiliging resulteren.

Als tweede voorbeeld kwam Microsoft's Office97 suite naar voren. De Visual Basic for Applications taal (VBA; opvolger van WordBasic) in alle componenten van deze suite converteert macro's automatisch van de oude naar de nieuwe syntax. Als het één van de bij Microsoft bekende macro-virussen is (en dat blijken er maar een paar te zijn; hoewel er nu meer dan 1000 bij virusresearchers bekend zijn), dan meldt Office97 dat er sprake is van een virus. Maar de ruim verspreide béta's van Office97 bevatte deze controle niet, dus de keurig naar Office97 geconverteerde virussen zijn al in omloop.

Uit het publiek kwam de vraag of het groeiende aantal virussen nu of in de toekomst zou betekenen dat de anti-virus industrie het niet meer aan kan of dat wellicht andere tools zoals heuristic scanning noodzakelijk worden. Op dit moment is de groei nog vrijwel lineair en kan de industrie de groei aan. Op diverse plaatsen wordt onderzoek gedaan of kunstmatige intelligentie en expert systems een computersysteem kunnen helpen virussen te detecteren.

Vooralsnog lijkt het er op dat deze gereedschappen het meest nuttig zijn voor de researchers zelf en leiden de neven-effecten (zoals foutieve melding van virusbesmetting) tot meer nadelen dan voordelen.

Na de pauze werd de heer Albert Tuit gevraagd duidelijk te maken hoe een grote instantie zich wapent tegen de geschetste gevaren. De heer Tuit introduceerde de manier waarop binnen DGP de virusproblematiek aangepakt is. Algemeen wordt voor beveiliging het VIR (Voorschrift Informatiebeveiliging Rijksoverheid) gevolgd. Het VIR schrijft voor dat beleid, coördinatie, verantwoordelijkheden, meldpunt voor inbreuken, en controle op naleving geïmplementeerd moeten zijn en dat een Afhankelijkheids- en Kwetsbaarheidsanalyse uitgevoerd is. Dit alles resulteert in een informatiebeveiligingsplan met maatregelen.

Qua virusprotectie zijn belangrijke criteria de eenvoud in gebruik, de kwaliteit van de leverancier en de regelmaat van updates. De gebruikers zijn middels een prijsvraag bewust gemaakt en ontvangen maandelijks diskettes met hulpmiddelen om de werkplek, vaak decentraal opgesteld, te controleren op virussen. Uit ervaring bij de migratie die DGP doormaakt naar het Windows 95/NT platform is gebleken dat voor kennisintensieve materie zoals anti-virus problematiek een goede partner waarop je kunt terugvallen bijzonder waardevol is. Andere tips: wed niet op één paard en neem een mix van maatregelen, met verschillende werking op de schaal van proactief-reactief. Maak iedereen betrokken en verantwoordelijk voor de problematiek. Laat maatregelen niet tegen je keren voor wat betreft acceptatie. Neem stappen die haalbaar zijn. Gebruik juiste momenten voor invoering van maatregelen, na een reeks van virusincidenten of bijvoorbeeld bij een grote technologische overgang.

Indien u de handout van deze sessie zoudt willen ontvangen met daarin veel achtergrondinformatie over virussen zoals het gevaar van Internet en macro-virussen, kunt u contact opnemen met Gert van de Nadort op telefoonnummer (0183) 624444 of per email: vandenadort@crypsys.nl

In de presentatie van de heer Hruska kwam een aantal nuttige informatiebronnen naar voren zoals:

http://www.virusbtn.com	(Virus Bulletin; het AV vakblad)
http://www.sophos.com/virusinfo/features/office97.html	(Virussen en Office97)
http://www.sophos.com/virusinfo/scares/javaviruses.html	(Java en virussen)