



Hacking is professionele business geworden. Wat zal 2007 ons brengen?

Met de groei van het internet is ook de criminaliteit op het internet gegroeid. Er vindt steeds meer hacking plaats vanuit de georganiseerde misdaad. Wat zal 2007 ons brengen? Hier volgt een aantal ontwikkelingen in 2006 en voorspelde trends in 2007.

Identity theft

Volgens de cijfers van de Amerikaanse Federale Handelscommissie worden elk jaar zo'n 10 miljoen Amerikanen het slachtoffer van identiteitsfraude. Identity theft kan plaatsvinden via het bemachtigen van gegevens via ondermeer dierstal van laptops, USB-sticks en backup tapes.

Diefstal van wachtwoorden

Diefstal van wachtwoorden via nepsites zal naar verwachting toenemen. Nepsites zijn steeds professioneler. Phishing gaat vooraf met een email waarin de ontvanger wordt gevraagd om op een link te klikken. Het laatste kwartaal was ongeveer 1 op de 200 emails een phishing email. Ook deze emails zijn steeds professioneler, voorzien van de juiste logo's en stijl van de site die wordt nagebootst. Het is de verwachting dat phishers zich meer zullen gaan richten op sites voor goede doelen.

Aanvallen op Webapplicaties

Webapplicaties zijn steeds vaker doelwit van aanvallen. Bekende aanvalstechnieken op webapplicaties zijn code injection, cross site scripting, cross site request forgeries en directory traversal. Met het meer sophisticated en interactief worden van Webapplicaties, neemt ook de kwetsbaarheid toe. Gelet op de grote populariteit van webapplicaties is het de verwachting dat aanvallen op webapplicaties in 2007 zal toenemen.

Rootkits

Met de komst van Vista, is het moeilijk te voorspellen hoe snel virussen, en in het bijzonder rootkits om zich heen zullen grijpen in 2007 en hoe effectief deze zullen zijn. Overigens zijn in Vista de eerste exploits al gevonden. Cijfers van Microsoft over rootkits van 2006 (gebaseerd op 5.7 miljoen computers), geven aan dat in 14% van de gemeten computers een rootkit aanwezig was. Indien de bekende Sony rootkit niet wordt meegenomen, is dit ongeveer 9%.

Spam

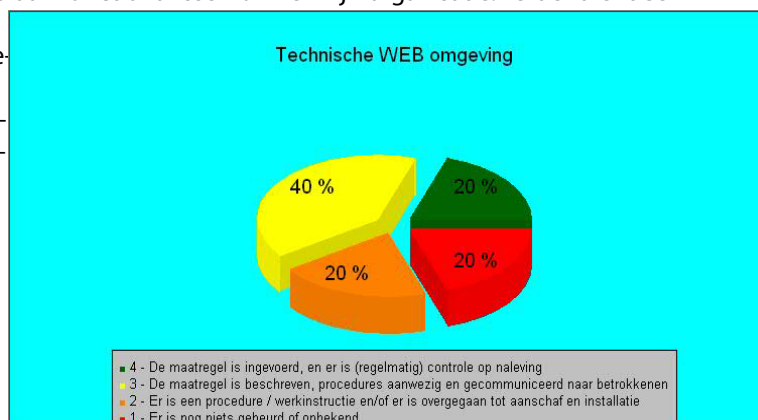
De hoeveelheid spam is al enige jaren hoog. Cijfers over Spam variëren van 65 tot ruim 80 procent van alle email. Een ontwikkeling dit jaar was de spam met de boodschap in een plaatje, waardoor filtering op tekst niet mogelijk was. Afgelopen November was ruim 40 % van alle spam van dit type. Vervelende bijkomstigheid van het gebruik van plaatjes is dat hierdoor de capaciteit die door spam wordt ingenomen toeneemt. De verwachting voor 2007 is dat Spam steeds specifiek op een branche zal worden toegespitst, met de daarbij behorende woordkeuze. Dit maakt het voor spamfilters nog lastiger om dergelijke email als spam te herkennen.

Secure Connection brengt Compliance SA2L builder uit.

Secure Connection heeft in aansluiting op de Systeemanalyse SA2L een nieuw object uitgebracht, waarmee door de klant zelf een Compliance kennisobject kan worden gemaakt. Dit builderobject maakt gebruik van de resultaten van een Systeemanalyse uit SA2L. De maatregeladviezen moeten door de klant worden gekoppeld aan functionarissen binnen zijn organisatie. Verder dient een

aantal gegevens m.b.t. de grafische weergave te worden opgegeven. Vervolgens wordt een kennisobject gegenereerd, waarmee de klant kan nagaan in hoeverre de organisatie voldoet aan de norm die via de Systeemanalyse is bepaald.

Op deze manier is voor het management zeer snel te zien waar de organisatie staat.



Actueel

Zero day exploit in MS Word

Deze maand werd door Mc Afee een nieuw lek ontdekt in Microsoft Word.

In dit geval ging het om een "geprepareerd" Microsoft Word document, gebruik makend van een exploit in MS Word (Exploit-MSWord.B). Dit bestand komt mee met een email of wordt via een WEBSITE gedownload. Indien het betreffende document wordt geopend, wordt er een buffer overflow gecreeerd. Hierdoor kan een password steler (PWS.j) worden geactiveerd. Deze wachtwoordsteler is in staat om wachtwoorden, onder andere uit de cash van het geïnfecteerde systeem te halen en deze via een ftp link of via email te sturen naar degene die binnen probeert te komen. Hoewel de kwetsbaarheid als ernstig werd gezien, is deze niet wijdverspreid geworden. Het stelen van wachtwoorden wordt steeds populairder. Zolang (alleen) wachtwoorden worden gebruikt voor authenticatie en zolang wachtwoorden relatief eenvoudig toegankelijk zijn, zullen deze type aanvallen doorgaan. U kunt zelf ook nagaan welke wachtwoorden er allemaal in uw computer "rondslingeren" door een (gratis) tool te downloaden. U kunt bijvoorbeeld het programma "Cain and Abel" van Oxid.it (<http://www.oxid.it/cain.html>) proberen.

Enkele tips:

- Gebruik geen wachtwoordmanagers (webrowsers maken hier ondermeer gebruik van).
- Wijzig uw wachtwoorden regelmatig
- Gebruik, waar het kan, een tweede authenticatiemiddel, zoals een token.

Bron: <http://us.mcafee.com>