DIE SCHWEIZER IT-PLATTFORM

Neu auch als E-Paper
www.computerworld.ch/service/epaper

Computerworld

Nr. 13/2007 30. März Fr. 5.80 / € 3.90

IDG COMMUNICATIONS

Fokus: Steigern Sie die Sicherheit

Lesen Sie alles über die neuen **Hacker-Strategien**, wie Sie **Würmer effizient jagen** und weshalb Sie **Webapplikationen wirksam absichern** sollten.

Sparen mit Thin Clients

Terminalrechner sind dem normalen PC zweifach überlegen: ökonomisch und ökologisch.

Sicher ins Firmennetz

Die neuesten VPN-Appliances in der grossen Marktübersicht.

Fünf Gratiswerkzeuge

Diese Netzwerk-Management-Tools entlasten Ihr IT-Budget.

Candid Wüest, Security-Experte von Symantec

«Geldgier beflügelt die Hacker-Szene»

Der Schweizer Virenjäger erläutert im Exklusiv-Interview, wie professionell Hacker heutzutage vorgehen und welche Gefahren sich hieraus ergeben.

DOWNLOAD-TIPP: IE7-Pro, das Ergänzungskit für Microsofts Browser, unter **www.computerworld.ch**

BILD: DOROTHEA MÜLLER

«Es gibt schon Hacker mit Arbeitsverträgen»

Phishing, Spam und Viren sind eine Landplage. Zudem werden ihre Urheber immer professioneller. Im Exklusiv-Interview mit Computerworld erläutert Security-Spezialist Candid Wüest von Symantec die derzeitige Bedrohungslage. INTERVIEW: JENS STARK

Die Hackerszene hat sich weiter professionalisiert und verfolgt fast ausschliesslich finanzielle Interessen. Dies geht aus dem jüngst von Sicherheits-Spezialistin Symantec vorgelegten «Internet Security Threat Report» über das zweite Halbjahr 2006 hervor. Computerworld Schweiz hat mit Candid Wüest, Software-Ingenieur in Symantecs Threat Analysis Team und einer der prominentesten Schweizer Virenjäger, die gegenwärtige Bedrohungslage analysiert und diskutiert.

Lesen Sie hier...

- warum Hacker vor allem End-User angreifen
- welche neuen Methoden Phisher austüfteln
- welche Virenarten derzeit im Trend liegen

COMPUTERWORLD: Nach Ihrem jüngsten Sicherheitsbericht erfolgen 99,4 Prozent der Angriffe in Europa auf Endanwender zuhause am PC. Warum ist das so?

CANDID WÜEST: Es gibt zwei Gründe: Erstens sind Heimanwender exponierter als Firmenanwender. Nehmen wir das Beispiel einer Wurm-verseuchten Mail. Diese gelangt viel einfacher auf den Rechner des Heimanwenders, weil er sie über einen Webmaildienst erhält, der oft ungenügend abgeschirmt ist. Viele Firmennetze filtern hingegen die eintreffende E-Post. Zweitens sind Heimanwender interessant für den Aufbau sogenannter Bot-Netze, mit denen Denial-of-Service-Attacken (DoS) ausgeführt werden. Die Chance ist gross, dass der PC-Nutzer mit Breitbandanschluss lange nicht merkt, dass er für DoS-Angriffe missbraucht wird. In einem mit Firewalls bestückten Firmennetz fallen solche Anomalien sofort auf.

Heisst das also, dass Unternehmensanwender aus dem Schneider sind?

Leider nein. Zwar mögen die verbleibenden 0,6 Prozent klein anmuten. Dahinter verbergen sich aber immer noch Millionen von Angriffen. Zudem sind die Attacken sehr viel gezielter. Unternehmen werden angegriffen, um ganz konkret Wirtschaftsspionage zu betreiben. Dafür reicht der Angriff auf wenige Systeme. Diese fallen zwar in unserer Statistik nur wenig ins Gewicht. Was jedoch das Ausmass und den wirtschaftlichen Scha-

den anbetrifft, sind sie viel schwerwiegender als die Attacken auf Privatanwender.

Sie haben in Ihrem Bericht die Angriffe auf die einzelnen europäischen Länder heruntergebrochen. Ich vermisse allerdings die Schweiz. Leben wir auf einer Insel der Glückseligen?
Keineswegs. Aber das Datenmaterial aus der Schweiz ist so gering, dass eine Auswertung statistisch zu ungenau wird. Allerdings lässt sich sagen, dass die Schweiz in Sachen Phishing-Versuche – auch wenn sie grösser wäre – nicht oben ausschwingen würde. Dafür sind beispielsweise unsere Online-Banking-Systeme viel zu sicher. In den USA reicht vielerorts die Eingabe von Benutzername und Passwort, um auf ein Bankkonto zuzugreifen, während in der Schweiz Zusatzsysteme im Einsatz sind. Auch Hacker versuchen aber erst einmal dort zu ernten, wo die Früchte relativ tief hängen.

Eine Aussage im Threat-Report hat mich erstaunt: Demnach haben Hacker und Phisher heutzutage «geregelte Arbeitszeiten». Wie kommt das?
Tatsächlich haben wir festgestellt, dass an Wochenenden 30 Prozent weniger Phishing-Mails verschickt werden als an Werktagen. Das hat zum einen ganz strategische Gründe: Wenn Sie eine solche Mail am Samstag losschicken, werden viele Adressaten diese erst am Montag lesen. Bis dahin könnte die darin verwendete Webadresse aber bereits gesperrt worden sein.

Andererseits sind die «geregelten Arbeitszeiten» aber auch darauf zurückzuführen, dass die Hacker einen enormen Grad an Professionalisierung erreicht haben. So wird die «Arbeit» beispielsweise geteilt. Es gibt schon Gruppen von mehreren Hackern, bei denen beispielsweise der erste die Phishing-Seite aufschaltet, der zweite die Mails verschickt und ein dritter die Inhalte professionell in mehrere Sprachen übersetzt. Uns sind sogar Fälle bekannt, in denen Hacker ganz konkret Arbeitsverträge unterschrieben haben, in denen Dinge wie Gewinnbeteiligung und Ferienansprüche geregelt werden. Es ist eine regelrechte Marktwirtschaft, die hier in den letzten Jahren aufgebaut wurde.

Welche Länder sind hier besonders aktiv?
Ich kenne Fälle aus Russland und auch aus Brasilien. Dies hängt aber auch mit der gesetzlichen Lage zusammen. Hier in der Schweiz tritt beispielsweise ab 1. April ein Anti-Spam-Gesetz in Kraft. Dieses sieht für das Versenden von Werbe- und Phishing-Mails Strafen von bis zu fünf Jahren Gefängnis vor. Es ist klar, dass man sich als Phisher eher ein Land aussucht, in dem die Gefahr der Aufdeckung und Bestrafung geringer ist. Schliesslich muss das ergaunerte Geld ja in Umlauf gebracht und gewaschen werden. Auch hierfür gibt es in besagten Ländern grössere Schlupflöcher.

Gibt es bestimmte Zeiten, in denen sich Phishing- und Spam-E-Mails häufen?
Klassisch sind die Tage vor Weihnachten oder vor dem Valentinstag. Wir beobachten aber auch Zunahmen vor speziellen Events. So nahm die Spam-Aktivität kurz vor dem Finale der Fussballweltmeisterschaft im letzten Jahr um 27 Prozent zu. Diese Anlässe können zudem einen sehr lokalen Charakter haben. So fielen mir in der Zeit, als in Bülach der Swissair-Prozess verhandelt wurde, diverse Spam-Mails auf, in denen für Silberbesteck und sonstige Souvenirs aus den Swissair-Beständen geworben wurde.

Die Leute reagieren also nach wie vor auf diese Mails. Sonst gäbe es sie ja nicht ...
... ja, das ist leider so. Spammer untersuchen die Erfolgsrate ihrer Mails sehr genau und ändern sofort die Strategie, wenn etwas nicht mehr funktioniert. So ist zum Beispiel der Anteil der Werbepost, die Erotikinhalte bewirbt, auf sechs Prozent geschrumpft, während Spam-Mails, die Aktien anpreisen und dadurch deren Preis in die Höhe treiben, auf 30 Prozent gestiegen sind.

Auch die Techniken verändern sich. So werden immer häufiger Spams verschickt, welche aus Bilddateien bestehen. Wie sieht diesbezüglich der Trend aus?
Der Versand von Bildern, welche zudem jeweils um wenige Bits abgeändert werden, damit sie nicht von Systemen zur Mustererkennung wahrgenommen werden, liegt nach wie vor stark im Trend. Ebenfalls auf dem Vormarsch sind beispielsweise auch animierte Grafiken. Dabei baut sich der Inhalt erst langsam auf oder Text wandert von einem Bildrand zum nächsten. Der Filter, der entscheiden soll, ob es sich um Spam handelt, analysiert nur das erste, noch ganz schwarze Bild der Serie.

Haben Sie ganz neue Methoden beobachtet, die noch nicht verbreitet sind?
Ja. So ist mir etwa aufgefallen, dass auch Newsletter gekapert werden. Dabei fangen die Spammer einen legitimen Newsletter ab, fügen diesem eine Werbebotschaft samt URL ein, und schicken ihn unter Beibehaltung des Absenders weiter. Das Problem an dieser relativ neuen Methode ist natürlich, dass Newsletter bei den Sicherheitsdiensten auf der weissen Liste stehen und deshalb selbst mit Anomalien nicht abgefangen werden. Auch die Empfänger sind weniger skeptisch, wenn ihnen in einem Schreiben von einem ihnen wohl bekannten Absender ein Link präsentiert wird.

Des weiteren werden öfters Suchanfragen «entführt». Man gibt bei Google einen Begriff ein, und Spammer mischen unter die Antworten der Suchmaschine Links zu den eigenen Firmen und Angeboten.

Was passiert derzeit in Sachen Schädlingen? Der Symantec-Report erwähnt einige neue Familienmitglieder. Was hat es mit diesen auf sich?
Die jüngste Schädlingsgeneration unterscheidet sich durch die Art und Weise, wie sie sich verbreitet und wo sie sich einnistet. So verwenden einige Rootkit-Techniken, um sich sozusagen unter dem Radarschirm des Betriebssystems zu installieren. Hier werden sie oft lange nicht wahrgenommen. Neue Verbreitungswege sucht dabei etwa auch «Peacom». Dieser Wurm baut ein Peer-to-peer-Netzwerk auf, also eine Art Mini-Napster. Dieses dient dann aber nicht dazu, MP3-Dateien herunterzuladen. Vielmehr wird es genutzt, um weitere Schädlinge oder Updates zu verteilen. Das Problem für uns Virenjäger ist, dass es keinen zentralen Server gibt, also keinen Kopf, den wir abhacken könnten.

Der Virus feiert derzeit seinen 25. Geburtstag. Denken Sie, dass er auch 50 wird? Und wie wird ein Virus im Jahr 2032 aussehen?
Man muss die Definition des Virus weiter fassen und von einem Schadprogramm sprechen. Eine solche Applikation, die etwas tut, was der Anwender nicht möchte und was ihm Schaden zufügt, wird wohl ihren 50. Geburtstag feiern können. Denn mit neuen Medien und neuen Techniken wird es immer Möglichkeiten geben, um etwas Bösartiges einzuschleusen. Wie ein Virus in 25 Jahren aussehen wird, ist schwer zu sagen. Dazu ist die weitere technische Entwicklung einfach zu schwer vorhersehbar. ■

ZUR PERSON

Candid Wüest, der Virenjäger

Candid Wüest hat sich der Jagd nach Computer-Schädlingen verschrieben. Nach seinem Informatikstudium an der ETH Zürich war der heute 30-Jährige am IBM-Forschungslabor in Rüschlikon am Global Security Analysing Lab tätig. 2003 heuerte er bei Symantec an. Hier analysierte er zunächst im Virenforschungslabor in Dublin bösartigen Code, um Virendefinitionen und Entfernungstools zu erstellen. Seit 2006 ist Wüest Mitglied des Threat Analysis Teams und befasst sich unter anderem mit neu auftretenden Sicherheitsrisiken im Internet.