

Pressemitteilung

504nis_intel, 20. September 2005

Neuer Symantec Sicherheitsreport: Immer mehr Hacker-Angriffe aus Profitgier

Trend zu Diebstahl, Betrug und Erpressung im Internet

München, 20. September 2005 – Der neue Sicherheitsbericht von Symantec hat neue Methoden ausgemacht, bei denen Schadprogramme im Internet für finanziellen Gewinn eingesetzt werden: Netzwerke ferngesteuerter Rechner (BotNets) werden zur Miete angeboten und maßgeschneiderter Code für Fernsteuerungsprogramme (Bots) können käuflich im Internet erworben werden. Die Kommerzialisierung cyberkrimineller Umtriebe findet ihren Niederschlag in Trojanern, die Spyware und Adware installieren, in Schadprogrammen, die vertrauliche Informationen ausspähen und in ausgefeilten Phishing-Methoden, die Anwendern sensible Daten wie Kontoinformationen entlocken. Im Zeitraum von Januar bis Juni 2005 beobachteten die Experten von Symantec im Schnitt 10.352 aktive bot-infizierte Computer pro Tag. Das ist eine Zunahme von mehr als 140 Prozent gegenüber dem vorherigen Untersuchungshalbjahr (4.348).

Da die finanziellen Gewinnmöglichkeiten durch Cyberverbrechen immer verlockender werden, werden Angreifer künftig wohl noch ausgefeiltere Methoden für BotNets und BotCode entwickeln – auch solche mit Tarnmechanismen, die darauf abzielen, Virenschutz, Firewalls und andere Sicherheitseinrichtungen außer Kraft zu setzen.

Im Zusammenhang mit BotNets ist auch die Zahl der Denial-of-Service-Attacken (DoS-Attacken) enorm gestiegen: Solche massiven Anfragen auf Server bringen diese letztlich zum Absturz. Webseiten, die über den Server laufen, sind dann zum Beispiel nicht mehr erreichbar. Symantec hat beobachtet, dass DoS-Attacken von durchschnittlich 119 auf 927 pro Tag angestiegen sind – das entspricht einer Zunahme von 680 Prozent in sechs Monaten. Neu ist, dass häufig kleine und mittlere Unternehmen ins Visier der Angreifer geraten.

Cyberschädlinge haben es stärker auf vertrauliche Informationen abgesehen – und auf deren Weitergabe an Dritte. Solche Bedrohungen können zu finanziellen Verlusten führen, insbesondere wenn Kreditkarteninformationen oder Bankdaten bloßgelegt werden.

Eine Besorgnis erregende Entwicklung, zumal Online-Shopping und Internetbanking immer beliebter werden. In der ersten Jahreshälfte 2005 machten Schadprogramme, die vertrauliche Informationen abschöpften, bereits 74 Prozent der 50 am häufigsten gemeldeten Cyberschädlinge aus.

„Der Trend geht weg von breit angelegten Angriffen auf Netzwerke hin zu kleineren, dafür aber zielgenauen Attacken auf Webanwendungen und Clients.“ So bringt Olaf Lindner, Sicherheitsexperte bei Symantec, die Verschiebung in der Bedrohungslandschaft auf den Punkt. „Unternehmen und Privatanwender müssen noch wachsamer sein, Rechner und Netzwerke mit Sicherheitslösungen schützen, aber auch Betriebssysteme und Anwendungen über Patches aktuell halten, damit Schwachstellen nicht ausgenutzt werden können.“

Außerdem greift ein neues Phänomen um sich: Modularer Schadcode, das sind Schadprogramme, die wie ein Baukasten nachrüstbar sind. Zunächst verfügen diese nur über limitierte Schadensfunktionen. Doch einmal auf dem Computer installiert, laden sie zusätzliche Funktionen herunter und rüsten sich so selbstständig zu gefährlichen Cyberschädlingen hoch. Diese Tendenz zu modularem Code wird sich nach Ansicht der Symantec-Experten noch verstärken und geht einher mit neuen Methoden zur Tarnung und zur Aushebelung von Sicherheitseinrichtungen auf befallenen Systemen.

Weitere wichtige Trends im ersten Halbjahr 2005 - eine Auswahl:

- Phishing greift weiter um sich. Die Anti-Phishing-Sensoren von Symantec haben im Schnitt 5,7 Millionen eigenständige Nachrichten pro Tag abgefangen, die mit betrügerischen Mitteln versuchten, an vertrauliche Daten zu gelangen (im Halbjahr zuvor waren es noch knapp drei Millionen täglich).
- Bei Schwachstellen hat sich die Situation weiter verschärft: Symantec dokumentierte 1.862 neue Schwachstellen, das ist die höchste Zahl, die bisher gemessen wurde. 59 Prozent befanden sich in Webanwendungen. Die Zeit zwischen der Bekanntgabe einer Schwachstelle und der Veröffentlichung von Exploit ist mit sechs Tagen weiterhin sehr kurz.
- Symantec verzeichnete 10.866 neue Varianten von Win32-Viren und -Würmern. Das ist eine Steigerung von 48 Prozent im Vergleich zum letzten Halbjahr 2004.
- Adware und Spyware stellen zunehmend eine Bedrohung für die Vertraulichkeit dar. Acht der zehn häufigsten Adware-Programme gelangten durch Web Browser auf den Rechner. Sechs der zehn häufigsten Spyware-Programme holten sich Anwender unwissentlich im Paket mit (kostenlosen) Downloads auf den Computer, andere installierten sich ebenfalls über den Web Browser.

505istr, 20. September 2005

WLANs werden, so die Prognose von Symantec, künftig häufiger im Fadenkreuz von Angreifern und Schadprogrammen stehen. Aber auch eine so selbstverständliche Tätigkeit wie das Telefonieren könnte künftig mit Risiken behaftet sein: Symantec befürchtet, dass Handy-Schädlinge ebenso einen Aufschwung erleben werden wie Sicherheitsprobleme für die Internettelefonie (Voice-over-IP).

Textumfang: 4.283 Zeichen (ohne Leerzeichen)

Über den Symantec Internet Security Threat Report:

Der Symantec Sicherheitsbericht liefert alle sechs Monate eine umfassende Analyse und Trendbewertung von Internetangriffen, Schwachstellen, Schadprogrammen und anderen Sicherheitsbedrohungen. Die Ergebnisse basieren auf umfassendem Datenmaterial aus Quellen wie dem DeepSight Threat Management System und der Symantec Managed Security Services mit 24.000 Sicherheitssensoren in über 180 Ländern; Reports zu böartigem Code, Spyware und Adware von über 120 Millionen Clients, Servern und Gateways mit Symantec Virenschutzlösungen; einer Schwachstellendatenbank mit etwa 13.000 Schwachstellen in 30.000 Technologien von mehr als 4.000 Herstellern; BugTraq, einem bekannten Forum zur Auflistung und Diskussion von Sicherheitslücken und 2 Millionen E-Mail-Konten, für die Analyse globaler Spam- und Phishing-Aktivitäten.

Weitere Details, Grafiken sowie den kompletten Sicherheitsbericht finden Sie im Symantec Online-Pressezentrum unter:

http://www.symantec.com/region/de/PressCenter/Threat_Reports.html

Über Symantec

Symantec ist weltweit führender Anbieter von Lösungen, die Privatpersonen und Unternehmen helfen, die Sicherheit, Verfügbarkeit und Integrität ihrer Informationen sicherzustellen. Das Unternehmen hat seinen Hauptsitz in Cupertino, Kalifornien und betreibt Niederlassungen in mehr als 40 Ländern.

Hinweis für Redakteure

Wenn Sie mehr über Symantec und seine Produkte erfahren möchten, dann besuchen Sie unser Online-Pressezentrum unter www.symantec.com/region/de/PressCenter. Dort liegt auch Bildmaterial von Personen und Produkten für Sie bereit.

Symantec und das Symantec Logo sind Warenzeichen oder eingetragene Warenzeichen der Symantec Corporation in den USA und ihrer Tochtergesellschaften einigen anderen Ländern. Andere Firmen- und Produktnamen können Warenzeichen oder eingetragene Warenzeichen der jeweiligen Firmen sein und werden hiermit anerkannt.

*Sitz der deutschen Firmenzentrale:
Symantec (Deutschland) GmbH, Lise-Meitner-Strasse 9, 85737 Ismaning
Telefon: +49 (0) 89 / 9458-3000
Telefax: +49 (0) 89 / 9458-3040*

*Ihr Ansprechpartner (NUR PRESSE) für Rückfragen:
Antje Weber
Pressereferentin
Telefon: +49 (0) 21 02 / 7453-892
Telefax: +49 (0) 21 02 / 7453-922
E-Mail: antje_weber@symantec.com*