Attacken im Internet : immer raffinierter

Autor(en): **Hogan, Kevin**

Objekttyp: **Article**

Zeitschrift: **Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology**

Band (Jahr): **83 (2005)**

Heft 4

PDF erstellt am: **10.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-877133

Attacken im Internet – immer raffinierter

Zu den altbekannten Cyber-Plagen, wie Viren, Würmer und Trojaner, haben sich neue gesellt: Der Sicherheitsreport von Symantec verzeichnete im Jahresverlauf eine Besorgnis erregende Zunahme von BotNets, Phishing-Attacken und Spionageprogrammen. Auch Schadprogramme für Smartphones sind im Kommen und fordern die Wachsamkeit von Privatnutzern wie Unternehmen.

Im folgenden Gespräch gibt Kevin Hogan, Leiter des Symantec-Virenforschungszentrums in Dublin, eine Einschätzung der aktuellen Bedrohungslage.

Herr Hogan, aus vormals 2000 neu entdeckten BotNets sind 30 000 geworden – und das Tag für Tag. Was sind BotNets überhaupt?
BotNet ist ein Kürzel für Robot Network: Damit sind grosse Gruppen von Computern im Internet gemeint, die mithilfe von speziellen Backdoor-Programmen (so genannte Bots) es Hackern ermöglichen, einen fremden Rechner fernzusteuern. Das Interesse der Hacker ist hier nicht auf Zerstörung ausgerichtet. Vielmehr geht es um die Rechnerleistung jedes einzelnen Computers. So werden PCs über die Bots zu einem leistungsfähigen Rechnernetzwerk verknüpft.

Was genau können Hacker mit BotNets anfangen und warum sind sie gefährlich?
Hacker können infizierte Rechner nach Belieben für ihre Zwecke einsetzen. BotNets dienen als riesige Plattformen für systematische Attacken auf andere Computer oder Netzwerke. Mit BotNets können Angreifer verletzliche Systeme noch leichter ausmachen und diese für ihre konzertierten Aktionen missbrauchen, zum Beispiel für massive Denial-of-Service-Attacken, also gezielte, massenweise Anfragen, welche die Server zum Absturz bringen. Darüber hinaus sind sie die Vorposten für die Eroberung neuer ungesicherter Rechner, mit denen sich das bestehende BotNet erweitern und seine Schlagkraft erhöhen lässt. Häufig werden die gekaperten Rechner auch zum Versenden von Spam, als Host für illegale Webseiten, zum Beispiel mit kinderpornografischem Inhalt, oder zum Speichern von Raubkopien missbraucht; und zwar so, dass der Computerbesitzer nichts davon merkt.

Die Vorstellung, plötzlich festzustellen, dass auf dem eigenen Rechner illegales Material gespeichert ist, wirkt bedrohlich.
Verantwortliches Handeln im Cyberspace schliesst auch ein, dass man seinen Computer vor Missbrauch mit geeigneten Sicherheitslösungen schützt.

Sehen Sie einen Trend zum Ausspionieren sensibler Daten, speziell von finanziellen Informationen?
Alle Anzeichen sprechen dafür. Allein die Zahl an Phishing-

Symantec
Symantec ist weltweit marktführend auf dem Gebiet der Informationssicherheit. Die umfangreiche Angebotspalette umfasst Software- und Appliance-Lösungen sowie Services. Diese sollen Privatanwendern, Unternehmen und Internet-Dienstleistern helfen, ihre ITInfrastruktur zu sichern und zu verwalten. Die Konsumentenmarke Norton ist weltweit marktführend auf dem Gebiet der Sicherheits- und Systempflegeprodukte für Endanwender. Das Unternehmen hat seinen Hauptsitz in Cupertino, Kalifornien und ist in mehr als 35 Ländern vertreten.

Attacken nahm zwischen Juli und Oktober 2004 um 25% zu. Online-Betrug, ob per E-Mail oder mithilfe von spezieller Software, ist vor allem zu einem Problem für Finanzdienstleister, Internet-Händler und deren Kunden geworden. Je mehr finanzielle Transaktionen online vorgenommen werden, umso sensibler sind die auf dem Computer gespeicherten Informationen. Dies an sich ist zwar keine neue Entwicklung, doch das Abzielen auf spezielle Informationen auf einem einzelnen Computer ist ein Trend, der in dieser Form vor wenigen Jahren noch nicht existierte.

Worauf sind die Datendiebe aus und wie gehen sie vor?
Es gibt Trickbetrüger im Internet, die sich auf die Wirkung des Social Engineerings verlassen. Das heisst, sie verleiten Anwender durch eine geschickte Ansprache, sensible Angaben zu machen. Techniken wie das Webspoofing erlauben es Kriminellen, Webseiten täuschend echt nachzumachen. Zusammen mit gefälschten E-Mails «phishen» sie im Internet nach vertrauensseligen Online-Kunden, denen sie sensible Informationen entlocken.

Welche Methoden wenden Cyber-Kriminelle sonst noch an?
Es gibt nach wie vor Betrüger, die auf soziale Interaktion verzichten und mithilfe von Spyware versuchen, an lohnende Informationen zu kommen. Mittlerweile gibt es eine Reihe von Attacken, bei denen sich eine unheilvolle Kombination von Phishing und Spyware abzeichnete. So werden Nutzer über Phishing Mails zwar auf echte Internet-Seiten geführt, doch beim Öffnen schaltet sich eine gefälschte Seite auf, die sensible Angaben wie Kontodaten, PIN- und TAN-Nummern abfragt.

Wie funktioniert Spyware?
Spyware sind Spionage-Programme, die Informationen von einem befallenen Rechner übers Internet an den Hersteller der Spyware senden. Zu diesem Zweck zeichnet das Schadprogramm Passwörter, Kontonummern und Ähnliches während einer Online-Sitzung auf. Spyware kann mit eindeutig krimineller Absicht eingesetzt werden, um die Sicherheit eines Systems zu unterhöhlen und sensible Daten herauszugreifen. Daneben gibt es kommerzielle Motive: In diesem Fall sprechen wir von Adware, die das Online-Verhalten des Nutzers aufzeichnet und für zielgruppengerechte Werbung auswertet. Die Grenzen zwischen Adware und Spyware sind fliessend, technologisch sind sie im Prinzip gleich.

Ist das Problem tatsächlich so akut?
Ich will Ihnen ein Beispiel zur Verdeutlichung geben: Einer meiner Kollegen hat kürzlich einen PC für einen Test konfiguriert. Der Rechner, eine Version ohne Schutz-Software, war für drei Stunden online. Nach dieser kurzen Zeit hatten sich rund achtzig Spionageprogramme auf dem Computer installiert.

Wie hoch ist denn der Anteil an Spionageprogrammen?
Bereits 20% aller «Virenmeldungen» beim Virenschutzzentrum von Symantec gehen auf Spyware zurück. 80% der Schädlinge, die wir als Spyware bezeichnen, sind eigentlich Adware, verfolgen also kommerzielle Ziele und dienen meist Marketingzwecken. Diese Programme zeichnen das Nutzerverhalten auf, beispielsweise welche Webseiten besucht werden. Nichtsdestotrotz verletzen sie das Recht des Anwenders auf Privatsphäre, die Vertraulichkeit seiner Daten und Surfgewohnheiten.

Wie können sich Anwender vor Spionageprogrammen schützen?
Um das Risiko deutlich herabzusetzen, sollten Internet-Nutzer Sicherheitsmassnahmen ergreifen. Dazu gehören restriktive Browser-Einstellungen sowie die Verwendung einer leistungsfähigen Firewall und Virenschutzlösung.

Kevin Hogan, Leiter des Symantec-Virenforschungszentrums in Dublin.

Wie gefährdet sind denn mobile Endgeräte wie Handys?
Der Funktionsumfang mobiler Kommunikationsgeräte nimmt ständig zu und somit auch die Zahl der Angriffsvektoren. Im Juni 2004 wurde der erste Handy-Wurm «Cabir» entdeckt. Im Oktober traten manipulierte Java-Anwendungen auf, die sämtliche Sicherheitsfunktionen auf einem Handy aushebeln konnten. Im November 2004 machte der Trojaner «Skulls» Geräte vom Typ Nokia 7610 unbrauchbar. Die Netzwerke der dritten Generation (wie GPRS und UMTS) ermöglichen Smartphones die ständige Verbindung mit dem Internet. Dieser Fortschritt hat einen Pferdefuss, denn so haben auch Hacker jederzeit Zugriff.

Mit welchen Entwicklungen rechnen Sie in der nahen Zukunft?
Wir werden mit zusätzlichen komplexen Bedrohungen konfrontiert werden, etwa mit weiteren Massenmailern. Auch die Zahl der Open-Source-Schadprogramme wie «Gaobot», dessen Quellcode im Internet veröffentlicht wurde, wird vermutlich weiter steigen. Dies könnte dazu führen, dass es zwar immer weniger Familien von Würmern oder Viren gibt, dafür aber unzählige Varianten.

In Zukunft werden vermutlich ausserdem häufiger Schadprogramme auftreten, die sich auch über Schnittstellengeräte wie Drucker verbreiten können. Einige wenige sind bereits aufgetreten. Im Moment ist das noch keine ernsthafte Bedrohung, doch immer mehr dieser Geräte sind webfähig und damit auch über Sicherheitslücken attackierbar. Auch durch die zunehmende Vernetzung und veränderte Nutzung von Computern im privaten Bereich könnte sich dies in den nächsten zwei bis drei Jahren zu einem grösseren Problem auswachsen. ■

Info: Symantec (Deutschland) GmbH, Lise-Meitner-Strasse 9, D-85737 Ismaning, Tel. +49 (0)89 945 830-00, Fax +49 (0)89 945 830-40