

# Pressemitteilung

## Symantec Sicherheitsreport: Deutschland mit den meisten Phishing-Webseiten in Europa

32 Prozent aller Phishing-Webseiten befinden sich in Deutschland/  
Identitätsdiebstahl und Wiederverkauf der Daten über das Internet  
wächst weiter/ Spam beeinflusst Aktienkurse

**München, 19. März 2007 – Von Deutschland gehen 19 Prozent aller Internet-Sicherheitsrisiken in Europa aus, dazu gehören Spam, Phishing oder die Verteilung von Schadcode über das Internet. Das zeigt die elfte Ausgabe des Internetsicherheitsreports von Symantec, der alle sechs Monate erscheint und dieses Mal einen gesonderten Report zur Region EMEA (Europa, Mittlerer Osten, Afrika) umfasst. Insbesondere der Bereich Phishing fällt in diesem Zusammenhang auf: 32 Prozent aller Phishing-Webseiten in der Region sind in Deutschland ermittelt worden, selbst weltweit steht das Land damit an zweiter Stelle nach den USA. Diese Zahlen unterstreichen deutlich, wie der Identitätsdiebstahl über das Netz weiter wächst. Die dort gesammelten Daten wie Passwörter, PINs und Kreditkartendaten werden häufig über so genannte Underground Economy Server von Kriminellen zum Weiterverkauf angeboten – schon für weniger als 10 US-Dollar können Kreditkartendaten online erworben werden, wie Symantec im Beobachtungszeitraum (1. Juli 2006 bis 31. Dezember 2006) ermittelt hat.**

„Auch Spam wird ganz gezielt eingesetzt, um finanziellen Gewinn zu erlangen – im letzten Halbjahr haben wir deutliches Wachstum von „Pump-and-Dump-Spam“ festgestellt, der Aktienkurse manipulieren soll“, erklärt Candid Wüest, Sicherheitsexperte bei Symantec. „Die Urheber kaufen schwach notierte Aktien und verschicken anschließend falsche Prognosen als Spam-E-Mails – der Aktienkurs steigt und sie können ihre Papiere mit Gewinn verkaufen.“ Insgesamt 30 Prozent betrug der Anteil finanzorientierter Spam-Mails in der zweiten Jahreshälfte 2006, gefolgt von 23 Prozent Spam zu Gesundheitsprodukten und 21 Prozent zu weiteren Produkten.

### **Bot-Rechner nehmen Überhand – 130 Prozent Zuwachs in EMEA**

Ein gängiges Verbreitungsmittel von Spam sind so genannte Bot-Netze. Mehr als sechs Millionen Bot-PCs, also Rechner, die ohne Wissen der Betroffenen „ferngelenkt“ werden können, existierten weltweit in der zweiten Jahreshälfte 2006. Das bedeutet einen Anstieg um ganze 29 Prozent gegenüber dem ersten Halbjahr. Im gleichen Zeitraum ging die weltweite Anzahl der „Command-and-Control“-Server, von denen aus die gekaperten Rechner gesteuert werden, um 25 Prozent zurück. Das heißt: mehr Bot-Netze werden von weniger Servern aus gesteuert. Hier zeigt sich insbesondere ein Trend zur länderübergreifenden Vernetzung der virtuellen Angreifer, beispielsweise um die finanzielle Effizienz der Attacken zu steigern. In Europa sind die meisten Bot-Rechner in Deutschland und Frankreich zu finden, was an der hohen Rate von Breitband-Anschlüssen in beiden Ländern liegt. Die Region EMEA zeigt die größte Steigerungsrate in der Anzahl an Bot-Rechner: Es wurde ein Zuwachs von 130 Prozent im Beobachtungszeitraum registriert.

### **Schattenwirtschaft im Internet**

Generell nehmen die Versuche zu, über das Internet an vertrauliche Daten zu gelangen. Von den 50 weltweit am meisten entdeckten Schadprogrammen zielen 66 Prozent auf vertrauliche Informationen ab – 48 Prozent mehr als im ersten Halbjahr 2006. Den Informations- und Identitätsdieben wird ihr Handwerk durch Hackerangriffe, Verlust von Hardware, wie Laptops und Smartphones, sowie unzureichenden Sicherheitsrichtlinien in Unternehmen erleichtert. Vertrauliche Daten stellen für Internetkriminelle die lukrativste Möglichkeit dar, sich auf Kosten der Bestohlenen zu bereichern. Doch auch die Daten selbst sind eine attraktive Einnahmequelle: Zum ersten Mal nimmt der Report den illegalen Handel mit gestohlenen Online-Identitäten unter die Lupe. Dazu Candid Wüest: „Gehandelt werden unter anderem Kreditkartennummern, PINs und E-Mail-Adressen – eine regelrechte Schattenwirtschaft auf speziellen Servern, den so genannten Underground Economy Servern, von denen 51 Prozent in den USA stehen. Eine Kreditkarte einschließlich Authentizitäts-Nachweisnummer kostet dort maximal sechs Dollar, eine komplette Identität einschließlich aller relevanten Daten wie der Ausweisnummer ist für 18 Dollar und weniger zu haben.“

### **Deutschland ist europäische Phishing-Hochburg**

Eine der bevorzugten Methoden, um an vertrauliche Informationen zu kommen, ist nach wie vor Phishing. Im zweiten Halbjahr 2006 entdeckte Symantec weltweit insgesamt 166.248 verschiedene Phishing-E-Mails, das sind durchschnittlich 904 pro Tag.

Insgesamt wurden über 1,5 Milliarden Phishing-E-Mails abgefangen, was einem Zuwachs von 19 Prozent im Vergleich zum vorigen Halbjahr entspricht. Dabei häufen sich die Phishing-Attacken unter der Woche, um am Wochenende deutlich abzunehmen. Auch Großereignisse wie beispielsweise die FIFA Weltmeisterschaft führen ebenfalls zu einem Anstieg betrügerischer Aktivitäten. Europäische Hochburg mit 32 Prozent aller Phishing-Webseiten ist Deutschland. Das zweitplatzierte Land Großbritannien folgt mit deutlichem Abstand (neun Prozent). „Einer der möglichen Gründe dafür ist die Anzahl an Web-Domains, bei denen Deutschland nach den USA an zweiter Stelle steht“, erklärt Sicherheitsexperte Candid Wüest. „Die Mehrzahl der Webseiten wird nur von einigen wenigen großen Internet-Providern verwaltet. Das kommt den Absendern von Phishing-E-Mails zugute, denn große Provider können aufgrund der Menge verwalteter Seiten weniger schnell auf illegale Webseiten reagieren.“

#### **Schadprogramme: Trojaner auf dem Vormarsch**

Die zahlenmäßig bedeutendsten bösartigen Aktivitäten im Internet – weltweit wie in EMEA – sind Angriffe durch Trojaner. Von den 50 am häufigsten auftretenden Schadcodes waren 45 Prozent Trojaner. In EMEA haben Trojaner einen Anteil von 54 Prozent aller Schadprogramme, Würmer – darunter auch der am meisten verbreitete W32.Stration-Wurm – haben einen Anteil von 43 Prozent.

#### **'Von Null auf Hundert' – Zero-Day-Attacken**

Der Internetsicherheitsreport verzeichnet einen deutlichen Anstieg bei den „Zero-Day-Angriffen“. Dies ist besonders kritisch, da diese Art von Attacke jeweils immer erst dann bekannt wird, wenn sie bereits ausgeführt wurde und noch kein Patch vorhanden war. Weltweit wurden in der zweiten Jahreshälfte 2006 ganze 12 Schwachstellen, die sich durch eine Zero-Day-Attacke ausnutzen ließen, registriert – in der ersten Jahreshälfte war es lediglich eine einzige. Die Angreifer werden gerade hier immer raffinierter, um der Entdeckung durch Schutzprogramme zu entgehen. Entdeckt werden solche Schwachstellen ausschließlich durch hoch qualifizierte Experten oder dann, wenn sie schon auf dem Schwarzmarkt zum Kauf angeboten werden.

Abschließend hat der Internet Security Threat Report für das zweite Halbjahr 2006 zum ersten Mal diejenigen Länder identifiziert, die den höchsten Anteil an kriminellen Internet-Aktivitäten aufweisen. Die USA stehen dabei mit einem weltweiten Anteil von 31 Prozent klar an der Spitze. Als Standort von Bot-Rechnern steht China ganz weit vorne – 26 Prozent sämtlicher Bots weltweit befinden sich dort.

*Textumfang: 7.099 Zeichen*

### **Weiterführende Informationen zur Datenerhebung**

Die analysierten Daten wurden im Zeitraum vom 1. Juli 2006 bis zum 31. Dezember 2006 erhoben und stammen aus der weltgrößten Ressource für Datensicherheit:

- Symantec DeepSight Threat Management System und Symantec Managed Security Services – mehr als 40.000 Sensoren, die die Netzwerkaktivitäten in 180 Ländern überwachen.
- Symantec Virenschutzlösungen – mehr als 120 Millionen Installationen auf Clients, Servern und Gateways erfassen Schadcodes, Spyware und Adware.
- Schwachstellen-Datenbank – mehr als 20.000 erfasste Sicherheitslücken aus mehr als 45.000 Technologien von über 7.000 Anbietern seit mehr als zehn Jahren.
- BugTraq – Forum mit über 50.000 Abonnenten, die täglich neue Gefahrenpotenziale diskutieren und Lösungsansätze austauschen.
- Symantec Probe Network – ein System mit mehr als zwei Millionen E-Mail Accounts, als Köder in 20 Ländern installiert, um weltweite Spam- und Phishing-Aktivitäten zu analysieren.
- Symantec Phish Report Network – eine umfangreiche Community, deren Mitglieder, Unternehmen und Endkunden, betrügerische Webseiten aufdecken, indem sie Informationen zu Phishing-Webseiten an das Netzwerk weiterleiten und im Gegenzug weiterführende Daten zu aktuellen Phishing-Aktivitäten erhalten.

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

[http://www.symantec.com/de/de/about/theme.jsp?themeid=threat\\_report](http://www.symantec.com/de/de/about/theme.jsp?themeid=threat_report)

Umfassendes Hintergrundmaterial zum Symantec Global Intelligence Network ist unter folgendem Link erhältlich:

[http://www.symantec.com/about/news/resources/press\\_kits/securityintelligence/](http://www.symantec.com/about/news/resources/press_kits/securityintelligence/)

### **Über den Symantec Internet Security Threat Report**

Der Symantec Internet Security Threat Report bietet eine komplette Übersicht der aktuellen Gefahrenpotenziale aus dem Internet. Neben detaillierten Ergebnissen werden auch die Methoden der Datenerhebung und Analyse vorgestellt. Unternehmen und Endanwender erhalten damit notwendige Informationen, um ihre Systeme entsprechend abzusichern.

Der Report, der im Turnus von sechs Monaten veröffentlicht wird, ist nunmehr in der elften Ausgabe verfügbar. Behandelt wird der Zeitraum vom 1. Juli 2006 bis zum 31. Dezember 2006.

### **Über Symantec**

Symantec ist ein weltweit führender Anbieter von Software, mit der sich Unternehmen und Privatpersonen sicher und vertrauensvoll in einer vernetzten Welt bewegen können. Das Unternehmen unterstützt Kunden mit Software und Dienstleistungen beim Schutz ihrer Infrastrukturen, Informationen und Interaktionen. Symantec hat seinen Hauptsitz in Cupertino, Kalifornien und betreibt Niederlassungen in 40 Ländern. Mehr Informationen unter [www.symantec.de](http://www.symantec.de)

### **Hinweis für Redakteure**

Wenn Sie mehr über Symantec und seine Produkte erfahren möchten, dann besuchen Sie unser Online-Pressezentrum unter [www.symantec.com/presse](http://www.symantec.com/presse)  
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.

*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:*

*Christiane Dellmann*

*Pressereferentin*

*Symantec (Deutschland) GmbH*

*Telefon +49 (0) 89-94302-619*

*Fax: +49 (0) 89-94302-450*

*E-Mail: [christiane\\_dellmann@symantec.com](mailto:christiane_dellmann@symantec.com)*

*Suemer Cetin*

*PR Consultant*

*Trimedia Communications Deutschland GmbH*

*Telefon +49 (0) 211-96485-54*

*Fax +49 (0) 211-96485-45*

*E-Mail: [suemergetin@dus.trimedia.de](mailto:suemergetin@dus.trimedia.de)*