

Pressemitteilung

Symantec Sicherheitsreport: Renommierte Webseiten im Visier der Cyberkriminellen

Untergrundwirtschaft zunehmend professionalisiert / Zwei Drittel aller bekannten Schadcodes stammen aus 2007

München, 8. April 2008 – Etablierte, häufig besuchte Internetportale sowie Social Networking-Seiten rücken ins Visier der Cyberkriminellen. Das ist eine der Kernaussagen der 13. Ausgabe des Symantec Internetsicherheitsreports. Zwar ist der Computer immer noch Angriffsziel Nummer eins, um an finanziell verwertbare Daten der Anwender zu gelangen – doch das Vertrauen in etablierte Webseiten und der unbedarfte Umgang mit persönlichen Informationen ermöglichen immer gezieltere Phishing-Attacken. Dementsprechend ist die Zahl der Server, auf denen betrügerische Webseiten gehostet werden, im zweiten Halbjahr 2007 weltweit um 167 Prozent auf 87.963 gestiegen. Darüber hinaus nutzen die Angreifer seitenspezifische Schwachstellen aus, um über Shotgun-Angriffe (mehrere, zeitgleiche Attacken über verschiedene Schwachstellen) Trojaner und Spionagetools in den Computer einzuschleusen. In den meisten Fällen ist es nicht einmal notwendig, dass der Anwender bewusst etwas herunterlädt oder anklickt. Solche Drive-by-Downloads gehören mittlerweile zum Standard-Repertoire der Angreifer.

„Professionell, organisiert und hochflexibel sind die Attribute, die den Wandel der Cyberkriminalität zu einer globalen Untergrundwirtschaft am besten beschreiben“, sagt Candid Wüest, Sicherheitsexperte bei Symantec und Co-Autor des aktuellen Sicherheitsreports. „Outsourcing und Spezialisierung bei der Erstellung von Schadcode, das sind neue Trends, die sich fortsetzen werden. Hier hat sich bereits etwas grundlegend verändert. Wir haben es nicht mehr mit Amateuren zu tun, sondern mit kriminellen Geschäftsleuten.“

Auf das Jahr 2007 entfallen zwei Drittel der insgesamt 1,1 Millionen Schadcode-Exemplare, die Symantec bisher insgesamt erfasst hat. Der Zuwachs liegt bei 468 Prozent. Die Masse an neuen Bedrohungen basiert dabei auf der zunehmenden Vernetzung und Arbeitsteilung der Cyberkriminellen untereinander. So werden weltweit je nach Bedarf die Angriffswerkzeuge

modifiziert und die erfolgversprechenden Entwicklungen zu Toolkits zusammengeführt, die dann auf Untergrundservern für jedermann angeboten werden. Beispielsweise gehen 26 Prozent aller weltweiten Phishing-Seiten auf nur drei Toolkits zurück. Diese Entwicklung ist besonders in Rumänien zu beobachten, das innerhalb weniger Monate Deutschland als Phishing-Hochburg Europas abgelöst hat.

Deutschland immer noch Spitzenreiter in der EMEA-Region

18 Prozent der bösartigen Aktivitäten in der Region Europa, Mittlerer Osten und Afrika (EMEA) wurden von Rechnern in Deutschland aus durchgeführt – damit ist Deutschland wie auch im Vorberichtszeitraum Spitzenreiter in der Region. Der Grund für die führende Position liegt in der hohen Zahl der vorhandenen Breitbandanschlüsse sowie in der weiterhin hohen Zuwachsrate. Da bei den meisten Internet Service Providern (ISP) für Sicherheitsmaßnahmen weitere Kosten für den Anwender anfallen, verzichten viele auf diese Schutzmaßnahmen und gefährden dadurch sich – und andere. In Deutschland befinden sich mit 18 Prozent immer noch die meisten Bot-infizierten Rechner in EMEA. Unter einem Bot (Abkürzung für Robot) versteht man ein heimlich installiertes Computerprogramm, welches Angreifern den Fernzugriff auf das System über einen Kommunikationskanal (wie z.B. Internet Relay Chat, kurz IRC) ermöglicht. Dabei infiziert in der Regel ein Angreifer zahlreiche Rechner mit einem Bot und verbindet diese dann zu einem Netzwerk (Botnet). Dieses Netzwerk kann zentral von einem Command-and-Control-Server aus gesteuert werden, um koordinierte Aktionen – wie beispielsweise den millionenfachen Versand von Spam-Mails – zu starten. „22 Prozent der Command-and-Control Server in der Region EMEA sind in Deutschland zu finden“, so Candid Wüest weiter. „So ist es nicht verwunderlich, dass 71 Prozent des E-Mail-Verkehrs in Deutschland aus Spam besteht – soviel wie in keinem anderen Land.“

Kernaussagen des 13. Symantec Internet Security Threat Reports

Schwachstellen auf Webseiten:

- Im zweiten Halbjahr 2007 wurden insgesamt 11.253 seitenspezifische Cross-site-scripting-Schwachstellen registriert – gegenüber 6.961 registrierten seitenspezifischen Schwachstellen im ersten Halbjahr 2007.
- Von diesen 11.253 Schwachstellen wurden lediglich 473 durch den Administrator der jeweiligen Seite behoben.
- Von den zehn wichtigsten Schadcode-Familien, die im zweiten Halbjahr 2007 entdeckt wurden, sind zwei darauf spezialisiert, Webseiten zu manipulieren. Sieben Prozent der 50 bedeutendsten Schadcode-Beispiele manipulierten ebenfalls Websites.
- Es ist sehr wahrscheinlich, dass gerade in letzter Zeit Toolkits wie MPack besonders das Interesse von Angreifern wecken, die Webseiten attackieren und dort Schadcode installieren wollen. MPack ist ein Toolkit, das in der ersten Jahreshälfte 2007 entdeckt

wurde und in der Lage ist, Exploits für Browser- und Client-Schwachstellen einzusetzen, die sich gegen alle Besucher einer infizierten Website richten.

Der Markt für gestohlene Daten und Informationen

- Daten mit finanzieller Relevanz machten im zweiten Halbjahr 2007 insgesamt 53 Prozent sämtlicher Angebote auf Servern der Untergrundwirtschaft aus, während dieser Zeit waren Bankkonten mit 22 Prozent des Gesamtaufkommens die am häufigsten angebotenen Güter.
- Der Rückgang bei der Bewerbung von Kreditkarten von 21 auf 13 Prozent ist maßgeblich auf die verstärkte Beobachtung der Szene durch die Kreditkarteninstitute sowie die größeren Hürden bei der Einlösung von Kreditkarten zurückzuführen.
- Die Preise in der Schattenwirtschaft richten sich zunehmend nach „normalen“ Marktgesetzen wie Angebot und Nachfrage. So begründet sich der Preis für eine Kreditkartennummer in der Lage der Bank und der Seltenheit der Karte.
- Insbesondere Zugangsdaten für Konten mit hohen Guthaben, wie beispielsweise Geschäftskonten oder Konten der EU sind kontinuierlich teurer geworden. Dasselbe gilt für Kontoinformationen, die auch persönliche Daten wie Namen, Adressen und Geburtsdaten enthielten.
- Nicht nur der Diebstahl durch kriminelle Handlungen ist beim Schutz persönlicher Informationen ein Problem. Diebstahl oder Verlust eines Computers oder eines vergleichbaren Speichergeräts verursachten 57 Prozent aller Datenverluste im zweiten Halbjahr 2007.

Flexibilisierung als Erfolgsgarant

- Angreifer aus dem Internet reagieren inzwischen immer schneller und präziser auf neue Sicherheitsmaßnahmen. Sie werden mobiler, adaptieren neue Taktiken und versuchen so, neu implementierte Sicherheitsmechanismen auszuhebeln.
- Immer häufiger ziehen sich Angreifer in Regionen zurück, in denen die Sicherheitsmaßnahmen noch nicht so ausgereift und Administratoren sowie Anwender mit Best Practices in Sachen Sicherheit nicht so vertraut sind.

Statements zum aktuellen ISTR

Dr. Andreas Knaebchen, Leiter der IT-Sicherheitsberatung von Accenture:

„In immer mehr Unternehmen wird IT zum Kern des Geschäfts, also werden auch Lücken und verkannte Risiken in der IT-Sicherheit immer bedrohlicher für das Geschäft. Besonders gefährdet sind Unternehmen, die Internetanwendungen wie Online-Buchungen und Online-Banking anbieten: Sind ihre Dienste einmal nicht verfügbar, kommen viele Kunden nicht wieder und wechseln zum Wettbewerber.“

Günther Ennen, Leiter des Referats Beratung des Bundesamtes für Sicherheit in der Informationstechnik (BSI):

„Der Marktplatz Internet stellt völlig neue Anforderungen daran, das Eigentum zu schützen und Bösewichte zu stellen. ‚Haltet den Dieb!‘ war gestern. Internetnutzer müssen heute risikobewusst sein und aktuelle, effiziente Sicherheitsmaßnahmen umsetzen.“

Dr. Mathias Tötzke, Department Head Trust and Safety bei eBay:

„Der aktuelle Internetsicherheitsbericht von Symantec zeigt einmal mehr, dass sich die Kriminalität im Internet ständig weiterentwickelt. Für uns bedeutet dies, dass wir unsere Sicherheitsmaßnahmen kontinuierlich überprüfen und anpassen müssen, um den Nutzern größtmögliche Sicherheit beim Handeln auf eBay zu bieten. Parallel legen wir großen Wert darauf, unsere Mitglieder über die wichtigsten Schutzinstrumente und Regeln zum sicheren Kaufen und Verkaufen auf unserem Marktplatz aufzuklären.“

Textumfang: 8.112 Zeichen (inkl. Leerzeichen)

Symantec Internet Security Threat Report

Der Symantec Internet Security Threat Report bietet eine umfassende 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 seit sieben Jahren im halbjährlichen Turnus erscheint, ist nunmehr in der 13. Ausgabe verfügbar. Die Daten wurden im Zeitraum vom 1. Juli 2007 bis zum 31. Dezember 2007 erhoben.

Um dem neuen Trend zu regionalen Bedrohungsmustern Rechnung zu tragen, gibt Symantec neben dem genannten Hauptbericht drei weitere Berichte heraus:

- den "EMEA Internet Security Threat Report" (für die Region Europa, Mittlerer Osten und Afrika)
- den "APJ Internet Security Threat Report" (für die Region Asien/Pazifischer Raum/Japan)
- den "Government Internet Security Threat Report", der sich in erster Linie mit Bedrohungen und Trends befasst, die speziell für Regierungsorganisationen und Behörden sowie kritische Infrastrukturbereiche interessant sind.

Weiterführende Informationen zur Datenerhebung

Die im 13. Internet Security Threat Report analysierten Daten stammen aus verschiedenen Informationsquellen von Symantec und sind zusammen genommen die weltgrößte Ressource für Datensicherheit:

- Symantec DeepSight Threat Management System und Symantec Managed Security Services – mehr als 40.000 Sensoren, die die Netzwerkaktivitäten in mehr als 180 Ländern überwachen.
- Symantec Virenschutzlösungen – mehr als 120 Millionen Installationen auf Clients, Servern und Gateways erfassen Schadcodes, Spyware und Adware.
- Schwachstellen-Datenbank – mehr als 25.000 erfasste Sicherheitslücken aus mehr als 55.000 Technologien von über 8.000 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 30 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

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

http://www.symantec.com/about/news/resources/press_kits/securityintelligence/

Über Symantec

Symantec ist ein weltweit führender Anbieter von Sicherheits-, Storage- und Systemmanagement-Software, mit der Unternehmen und Privatpersonen ihre Informationen sichern und verwalten können. Symantec hat seinen Hauptsitz in Cupertino, Kalifornien und betreibt Niederlassungen in mehr als 40 Ländern. Mehr Informationen unter 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. 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, Humboldtstraße 6, 85609 Aschheim-Dornach

Telefon: +49 (0) 89 / 94302 - 100

Telefax: +49 (0) 89 / 94302 - 950

Ihr Ansprechpartner (NUR PRESSE!) für Rückfragen:

Corinna Spohr

Sr. PR Manager Zentraleuropa

Symantec (Deutschland) GmbH

Telefon +49 (0) 89-94302-620

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

E-Mail: corinna_spohr@symantec.com

Suemer Cetin

Senior PR Consultant

Trimedia Communications Deutschland GmbH

Telefon +49 (0) 211-96485-54

Fax +49 (0) 211-96485-45

E-Mail: suemergetin@dus.trimedia.de