

## Security

### Cisco Halbjahres-Sicherheitsbericht:

#### Was Cyberkriminelle von der realen Geschäftswelt gelernt haben

- *Professionalität, Kooperationen und Einfallsreichtum charakterisieren die Vorgehensweise der Online-Betrüger in 2009*
- *Kriminelle nutzen immer geschickter Strategien aus der realen Geschäftswelt*
- *Rückgang betrügerischer Attacken um 25 Prozent gegenüber dem ersten Halbjahr in 2008*
- *Barack Obama hat Internetsicherheit zur Chefsache erklärt*

Wien, 16. Juli 2009 – Cisco stellt heute seinen Halbjahresbericht zur Sicherheitslage 2009 vor. Der Report zeigt neue technische und geschäftliche Strategien auf, mit denen Kriminelle derzeit Unternehmensnetzwerke angreifen und Webseiten kompromittieren, um Malware zu verbreiten und persönliche Daten oder Geld zu stehlen. Dabei wird offensichtlich, dass Internetkriminelle immer mehr zu erfahrenen Geschäftsleuten werden: Sie orientieren sich an erfolgreichen Strategien seriöser Unternehmen und gehen Allianzen ein, um ihre illegalen Machenschaften noch lukrativer zu gestalten.

Mit dem Halbjahresbericht gibt Cisco Anregungen, wie sich Organisationen durch das Zusammenspiel von Mitarbeitern, Prozessen und Technologien wirksam vor neuen Angriffsmethoden schützen können. "Besonderes Augenmerk ist aber nach wie vor auf alte, bekannte Bedrohungen, die genauso verbreitet und gefährlich sind wie die neuen Verfahren, zu legen", warnt Achim Kaspar, General Manager Cisco Austria.

#### Die wichtigsten Erkenntnisse des ersten Halbjahres

Die guten Nachrichten zuerst: Im Vergleich zum ersten Halbjahr 2008 sind die Aktivitäten der Cyberkriminellen in den ersten sechs Monaten dieses Jahres um 25 Prozent zurückgegangen. Dies spricht zum einen für den Erfolg von Sicherheitsanbietern, zum anderen sind in den letzten Monaten mehrere Drahtzieher identifiziert und verhaftet worden. Doch Entwarnung ist nicht angesagt: Statt auf Masse setzen die verbleibenden Verbrecher vermehrt auf ausgefeiltere und gezielte Angriffsmethoden. Der Conficker-Wurm, der seit Ende 2008 Computer durch eine Windows-Sicherheitslücke infiziert, verbreitet sich weiter. Im Juni 2009 waren noch geschätzte drei Millionen Computer in über 150 Ländern unter seiner Kontrolle, die meisten davon in Brasilien, China und Russland.

Die Kriminellen sind verstärkt auf der Suche nach aktuellen Ereignissen, um sie für ihre Zwecke zu missbrauchen. So wurde nach Ausbruch der Schweinegrippe im April das Web schnell mit Spam zu angeblich helfenden Medikamenten und mit Links zu gefälschten Pharmaseiten überschwemmt. Zeitweise machte der "Schweinegrippe-Spam" bis zu vier Prozent des gesamten Spamaufkommens aus. Während viele Spammer immer noch auf den massenhaften Versand setzen, versenden andere nur eine kleine Anzahl von Nachrichten, aber diese dafür häufiger. Davon versprechen sie sich, von gängigen Sicherheitssystemen nicht erfasst zu werden. Cisco geht davon aus, dass die Gesamtaufkommen von Spam im Jahresverlauf weitere Rekordniveaus erreicht.

US-Präsident Barack Obama hat die Stärkung der Internetsicherheit in den Vereinigten Staaten zur Chefsache erklärt. Dabei arbeitet seine Regierung eng zusammen mit der Staatengemeinschaft und dem privaten Sektor, um Technologien gegen die Bedrohungen voranzutreiben. Dieses Vorhaben wird die Entwicklung der Sicherheitsindustrie in den kommenden Monaten stark positiv beeinflussen. John Stewart, Chief Security Officer bei Cisco und Mitwirkender beim Bericht des Center for Strategic and International Studies (CSIS) für die Obama-Regierung, gibt in einem aktuellen Video-Blog tiefere Einblicke.

### **Spezifische Bedrohungen im Überblick:**

Botnetze: Diese Netzwerke von infizierten Computern dienen als effiziente Werkzeuge, um eine Attacke zu starten. Immer häufiger vermieten die Botnetz-Besitzer die Infrastruktur als Software-as-a-service (SaaS)-Modell an Gleichgesinnte, die darüber weiteren Spam und Malware verbreiten. Damit verdienen sie zwischen 5.000 und 10.000 US-Dollar pro Woche.

Spam: Der „Mail-Müll“ ist einer der am stärksten etablierten Wege, um Millionen von Computern mit fragwürdigen Verkaufsoffensiven oder Links zu verseuchten Websites zu erreichen. Mit der Verbreitung von Würmern und Malware ist und bleibt Spam ein Hauptproblem, dass zunehmend auch den Internetverkehr verstopft: erstaunliche 180 Milliarden Spam-Nachrichten werden jeden Tag verschickt - das sind etwa 90 Prozent des gesamten E-Mail-Verkehrs.

Würmer: Die Popularität und Zunahme von Social Networking Sites erleichtert die Verbreitung von Wurmattaken erheblich. Mitglieder von Online-Communities klicken eher auf Links und Downloads von vermeintlich bekannten und vertrauenswürdigen Personen.

Spamdexing: Viele Unternehmen nutzen seit langem Suchmaschinenoptimierung, um bei Suchen auf Google & Co besser platziert zu sein. Die Taktik, eine Webseite mit relevanten Schlüsselwörtern oder Suchtermini zu versehen, haben auch die Cyberkriminellen für die Maskierung ihrer Malware als legitime Software entdeckt. Zahlreiche Anwender, die den Rankings von Suchmaschinen vertrauen und sie nicht

hinterfragen, laden bereitwillig solch heimtückische Software und damit gleich den darin versteckten Trojaner herunter.

SMS-Scam: Seit Anfang 2009 zielen im Schnitt mindestens zwei oder drei Kampagnen wöchentlich auf Mobiltelefone und Smartphones ab. Cisco sieht die schnell wachsende mobile Zielgruppe als neues, unwiderstehliches Ziel für betrügerische Cyberkriminelle. Mit mehr als 4,1 Milliarden Handyverträgen weltweit bieten sie eine große Angriffsfläche, so dass die Kriminellen selbst dann genügend Profit machen, wenn sie nur bei einem kleinen Teil erfolgreich sind.

Insider: Die globale Rezession führt dazu, dass viele Personen bereits ihren Job verloren haben oder zumindest um ihn fürchten. Folglich wird die Herausgabe von vertraulichen Informationen durch Betriebszugehörige in den kommenden Monaten zu einer ernst zu nehmenden Bedrohung für Unternehmen. Betrügerische Insider müssen nicht immer derzeitige oder frühere Mitarbeiter sein - auch Vertragspartner oder Dritte können Interna weitergeben.

Patrick Peterson, Cisco Fellow und Chief Security Researcher bei Cisco fasst zusammen: "Das Internet sicher zu machen ist seit langem eine enorme Herausforderung, denn die Kriminellen entdecken immer neue, verschlungene Wege, um Unternehmensnetzwerke zu knacken und an wertvolle persönliche Daten zu gelangen. Das Interessante an unseren aktuellen Untersuchungen: Neben den technischen Fähigkeiten, mit denen sie ihr Aktionsfeld ausweiten und Sicherheitsmaßnahmen umgehen, entwickeln sie zunehmend auch einen scharfen Geschäftssinn. Sie arbeiten mit anderen zusammen, nutzen sowohl die größten Ängste als auch die Interessen ihrer Opfer aus und greifen zunehmend auf herkömmliche Internet-Tools wie Suchmaschinen oder Software-as-a-Service-Modelle zurück. Manche sind erfolgreich, indem sie bewährte Betrugsmethoden anwenden, die in den letzten Jahren durch das Aufkommen neuer Bedrohungen heruntergespielt wurden. Bei Betrügern, die so schnell die Schwächen in Online-Netzwerken und der menschlichen Psyche aufspüren, müssen Unternehmen wachsam sein gegenüber allen Arten von Attacken und neue Wege beschreiten, um Cybercrime zu bekämpfen."

In einem Video-Blog erklärt Peterson einige der neuen Bedrohungen der Internetsicherheit, die im ersten Halbjahr 2009 bedeutend waren: <http://tools.cisco.com/cmn/jsp/index.jsp?id=89479>

#### **Quellen:**

- Cisco Halbjahres Security Report 2009
- Cisco Security Intelligence Operations – Cisco Security Intelligence Operations (SIO) sammelt Daten zu Angriffen von mehr als 700.000 Cisco-Sicherheitslösungen weltweit, aus verschiedenen Cisco-Abteilungen und über 600 externen Quellen. Diese Bedrohungen und Sicherheitslücken werden für neue Schutzmaßnahmen analysiert und korreliert. Da sich die Gefahren ständig weiterentwickeln, verbessert auch Cisco SIO permanent seine Fähigkeit, globale Bedrohungspotenziale und Trends

aufzuspüren. Mit einem weltweiten Team von Forschungsingenieuren, ausgeklügelten Technologien und automatischen Update-Systemen, bietet Cisco SIO Expertenanalysen und Services für einen umfassenden Schutz.

- Cisco Sicherheits-Blog auf The Platform

Aktuelle Informationen von Cisco Austria sind über die Kurznachrichten-Plattform „Twitter“ ([www.twitter.com/Cisco\\_Austria](http://www.twitter.com/Cisco_Austria)) abrufbar.

Weitere Informationen:

Cisco Systems Austria GmbH, Millennium Tower, Handelskai 94-96, A-1200 Wien, [www.cisco.at](http://www.cisco.at)  
Wolfgang Fasching-Kapfenberger, Tel. 01-240 30-6247, Fax 01-240 30-6300, [wfaschin@cisco.com](mailto:wfaschin@cisco.com)  
The Skills Group, Christiane Fuchs-Robetin, Tel. 01-505 26 25-66, [fuchs-robotin@skills.at](mailto:fuchs-robotin@skills.at)

---

Über Cisco

Cisco (NASDAQ: CSCO), weltweit führender Anbieter von Networking-Lösungen, verändert die Art und Weise wie Menschen miteinander in Kontakt treten, kommunizieren und zusammenarbeiten. Weitere Informationen zu Cisco finden Sie unter <http://www.cisco.at>. Cisco-Produkte werden in Europa von der Cisco Systems International BV geliefert, eine Tochtergesellschaft im vollständigen Besitz der Cisco Systems, Inc.

Cisco, Cisco Systems und das Cisco Systems-Logo sind eingetragene Marken oder Kennzeichen von Cisco Systems, Inc. und/oder deren verbundenen Unternehmen in den USA und in anderen Ländern. Alle anderen in diesem Dokument enthaltenen Marken sind Eigentum ihrer jeweiligen Inhaber. Die Verwendung des Worts "Partner" bedeutet nicht, dass eine Partnerschaft oder Gesellschaft zwischen Cisco und dem jeweils anderen Unternehmen besteht. Dieses Dokument ist eine Veröffentlichung von Cisco.