

## Technologien

### **Cisco Security Report: Spam-Flut steigt weiter, Sicherheitsprobleme in Social Media**

- *Social Media, zunehmende Mobilität, Collaboration und Virtualisierung lösen Neugestaltung in der Sicherheitslandschaft aus*
- *Unternehmen müssen ihre Denkweise zu Sicherheitsfragen ändern, um sicherzustellen, dass ihre Netzwerke geschützt werden*
- *Cisco-Report gibt klare Handlungsempfehlungen zur Gefahrenabwehr*

Wien, 22. Juli 2010 – Tiefgreifende Veränderungen in der Lebens- und Arbeitswelt verursachen einen nie dagewesenen Wandel in der IT-Sicherheitslandschaft. Der heute veröffentlichte Cisco MidYear Security Report 2010 veranschaulicht das dramatische Ausmaß dieser Veränderungen. Als Auslöser dieser Verschiebungen nennt der Cisco-Report vor allem die explosionsartige Ausbreitung von Web 2.0 und Netzwerkzugriffen über mobile Endgeräte sowie den anhaltenden Cloud- und Virtualisierungstrend.

### **Technologie verändert Lebensstil**

Gerade bei jungen Mitarbeitern verschwimmen immer mehr die Grenzen zwischen privater und beruflicher Gerätenutzung. Sie kommunizieren mit Partnern und Kunden genauso wie mit Angehörigen oder Freunden über Twitter, Facebook oder andere Social-Media-Plattformen – und dies mit jeder Art von Endgerät, überall, zu jeder Zeit. Technologische Innovationen verändern fundamental die Art und Weise, wie Menschen leben, arbeiten, spielen, Informationen austauschen und miteinander kommunizieren. Konsumenten adaptieren innovative Collaboration-Technologien typischerweise viel früher als die Wirtschaft. Unternehmen geraten daher leicht ins Hintertreffen bei der Anpassung der entsprechenden Sicherheitsrichtlinien. „Die starken Kräfte im Markt lösen die Grenzen zwischen Netzwerken mehr und mehr auf und das bewirkt neue Anforderungen an die IT-Sicherheit von Unternehmen. Besonders Österreichs KMU-lastige Wirtschaft muss sich stärker mit den Umwälzungen in der Internet-Sicherheit befassen“, so Achim Kaspar, General Manager von Cisco Austria. Unternehmen sollten laut den Studienautoren ihre IT umgehend transformieren und an die veränderte Situation anpassen. Nur so werden sie den neuartigen Sicherheitsanforderungen gerecht. Laut Cisco-Studie geht es hierbei nicht nur darum, Bedrohungen vom Unternehmensnetzwerk fernzuhalten, sondern auch um die Kontrolle der eigenen Firmenreputation in der wachsenden Web 2.0-Öffentlichkeit.

## MidYear Security Report – Kernaussagen im Überblick

- Als „tektonische Kräfte“ arbeitet die Studie insbesondere Social Networking, Collaboration, Virtualisierung, Cloud Computing sowie die extensive Nutzung mobiler Endgeräte als treibende Kräfte für drastische Veränderungen und Herausforderungen der IT-Sicherheit heraus. Als geeignete Maßnahmen empfiehlt der Report:
  - Durchsetzung von granularen, nutzerbezogenen Richtlinien für den Applikations- und Datenzugriff auf virtuellen Systemen
  - strikte Zugriffslimits für kritische Unternehmensdaten
  - dezidiertes Richtlinienwerk für den mobilen Informationszugriff
  - intensives Monitoring von Cloud-Aktivitäten
  - klare Verhaltensregeln für Mitarbeiter bei Social Media-Nutzung
- Ein Ergebnis der Cisco Security Intelligence Operations (SIO) besagt, dass weltweit 7 Prozent der Facebook-User durchschnittlich 68 Minuten pro Tag mit dem interaktiven Spiel FarmVille verbringen. Mit 52 Minuten täglicher Spielzeit und 5-prozentiger Nutzerzahl rangiert Mafia Wars auf Platz 2. Es folgt Café World mit 4 Prozent und 36 Minuten. Wenngleich der dadurch verursachte Zeit- und Produktivitätsverlust an sich noch nicht sicherheitsrelevant erscheinen mag, so stehen die genannten Online-Spiele doch im Verdacht, zur Einschleusung von Schadsoftware missbraucht zu werden.
- 15 Prozent der Anwender gestehen ein, das Verbot der Social-Medianutzung im Unternehmen mindestens einmal pro Woche nicht zu befolgen. 27 Prozent von ihnen verändern eigenmächtig Gerätekonfigurationen, um auf verbotene Web 2.0-Anwendungen zugreifen zu können.
- Die weltweite Spam-Flut wird im Vergleich zum Vorjahr voraussichtlich um 30 Prozent steigen. Spam-Quelle Nummer 1 sind die Vereinigten Staaten. Auf Platz 2 und 3 folgen Indien und Brasilien; auf Rang 4 und 5 Russland und Südkorea. In Brasilien ging das Spamaufkommen um 4,3 Prozent zurück – wahrscheinlich, weil dortige Internet Provider den Port-25-Zugriff limitiert haben. Cyberkriminelle haben weiterhin offizielle Web-Sites im Visier, gehen aber immer öfter strategisch vor und lancieren sogenannte Multi-Vektor-Attacken, die verschiedene Wege nutzen, um ins Netzwerk einzudringen. Hauptziel ist das Einschleusen von Phishing-Software und die Gewinnung weiterer Bots.

- Besonders alarmierend: Soziale Plattform sind nicht nur ein „Spielfeld“ für Cyberkriminelle, sondern werden zunehmend auch von terroristischen Organisationen als Kommunikationsplattform missbraucht.

Weiterführende Informationen zum Cisco MidYear Security Report 2010 finden Sie unter <http://www.cisco.com/go/securityreport>. Cisco Vice President John N. Stewart diskutiert zudem heute um 18 Uhr (MESZ) die Ergebnisse des Reports in einem TV-Broadcast mit Senior Security Research Mary Landesman. Zugang zum Broadcast bietet Ihnen folgender Link:

<http://tools.cisco.com/cmn/jsp/index.jsp?id=102551>

Text- und Bild-Downloads unter: [http://www.cisco.com/web/AT/presse/aktuelles/ak\\_home.html](http://www.cisco.com/web/AT/presse/aktuelles/ak_home.html)

Aktuelle Informationen von Cisco Austria sind über die Kurznachrichten-Plattform „Twitter“ ([http://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, <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), <http://www.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 International Ltd. 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.