

Unternehmen

Cisco Sicherheitsbericht des Jahres: Social Media ist neuer „Spielplatz“ für Cyber-Kriminelle

- *Jährlicher Sicherheitsbericht von Cisco zur globalen Lage der IT-Sicherheit veröffentlicht*
- *Social Media: Der Mensch als Risikofaktor*
- *Erstmals ROI Matrix der Cyber-Kriminellen*

Wien, 22. Dezember 2009. Cisco veröffentlichte seinen umfassenden Jahresbericht zur globalen Lage der IT-Sicherheit. Der „Cisco 2009 Annual Security Report“ zeigt erstmals, welche Auswirkungen die sozialen Medien, vor allem Social Networks, auf die Netzsicherheit haben und befasst sich insbesondere mit dem Faktor Mensch als Sicherheitsrisiko.

Social Media erfuhr 2009 ein explosionsartiges Wachstum. Alleine Facebook verdreifachte im Laufe des Jahres seine aktive Nutzerbasis auf 350 Millionen. Auch 2010 wird die Nutzung von Social Media mehr und mehr zunehmen, da immer mehr Unternehmen den Wert von sozialen Netzwerken erkennen. Soziale Netzwerke werden dadurch jedoch auch immer stärker zu einem Spielplatz für Cyber-Kriminelle. Nutzer dieser Netzwerke haben großes Vertrauen zu den Mitgliedern ihrer Communities und treffen oft keinerlei Vorsichtsmaßnahmen um die Ausbreitung von Malware und Viren zu verhindern. Der Sicherheitsbericht von Cisco enthält daher erstmals Informationen über die Kombination von schlechtem Nutzerverhalten, potenziellen Schwachstellen und veralteter Software. Diese Kombination kann sich verheerend auf die Netzwerksicherheit auswirken und das Risiko von Angriffen drastisch erhöhen.

Achim Kaspar, General Manager von Cisco Austria: „Die Gefahren von sozialen Netzwerken werden unterschätzt. Hier gilt es, wie im Internet generell, vorsichtig mit vertraulichen Daten umzugehen. Das regelmäßige Update von Sicherheitssoftware ist unumgänglich.“

Die wichtigsten Ergebnisse des Cisco Security Reports 2009

Die erfolgreichste kriminelle Organisation: Zeus – Dieser Trojaner ermöglicht durch gezielte Phishing- und Drive-by-Downloads das Ausspähen von Logins und Passwörtern zu zahlreichen Online-Banking-Anmeldeinformationen. Durch kostengünstige Toolkits war es den Cyber-Kriminellen möglich, Varianten von Zeus zu erstellen die nur schwer von Antiviren-Programmen erkannt werden konnten. Im Jahr 2009 infizierten die Zeus-Botnetze so fast vier Millionen Computer weltweit.

Die bemerkenswerteste kriminelle Innovation: Koobface – Dieser Wurm regenerierte sich selbst und erschien zunächst auf Facebook (2008) sowie in diesem Jahr auf Twitter. Koobface verleitet Nutzer zum Klicken eines Links zu einem YouTube-Video, wodurch der Wurm aktiviert wird. Mehr als drei Millionen Computer wurden von Varianten dieser Malware infiziert.

Cybercrime Return on Investment (CROI)

Neue Cybercrime Return on Investment (CROI) Matrix von Cisco: Erstmals enthält der Security Report eine Cybercrime Return on Investment (CROI) Matrix. Die CROI Matrix analysiert und prognostiziert, welche Formen der Internetkriminalität im nächsten Jahr die „Gewinner“ und „Verlierer“ sein werden.

Spam-Statistiken – Brasilien Nummer eins unter Spam-Versendern

Der Jahresbericht von Cisco erwartet 2010 einen Anstieg der Spam-Mails um 30 bis 40 Prozent im Vergleich zu den Zahlen aus 2009. Darüber hinaus zeigt der Report, dass in den USA und anderen Wirtschaftsnationen, beispielsweise in der Europäischen Union, die Anzahl der Spammer sinkt. Gleichzeitig verdeutlicht der Report, dass insbesondere jene Länder, bei denen gerade der Ausbau von Breitbandtechnologien beginnt, zu einer wachsenden Quelle von Spam werden. Die USA sind damit nicht mehr die Nummer eins unter den Spam-Versendern. Im Jahr 2009 ging dieser Platz an Brasilien.

„Mit den fließenden Grenzen von Social Media für die Nutzung im Business- und Privat-Bereich wird das Risiko von Störungen bei der Netzwerksicherheit enorm erhöht“, erklärt Patrick Peterson, Cisco Fellow und Chief Security Researcher bei Cisco. „Dabei ist oft der Mensch der größte Risiko-Faktor, nicht die Technologie. Bei fehlendem Erkennen von Sicherheitsbedrohungen werden wir durch unsere natürlichen Instinkte dazu verleitet, unseren ‚Freunden‘ in Social-Media-Netzwerken zu vertrauen und machen so unsere Heimcomputer und die Unternehmens-Netzwerke für Malware frei zugänglich. Der Nutzen von Social Media wird von immer mehr Unternehmen erkannt. Jedoch müssen diese Unternehmen auch verstärkt auf die Fortbildung ihrer Mitarbeiter achten um zu verhindern, dass vertrauliche Daten über diese Medien nach außen gelangen und um einen verantwortungsvollen Umgang sicher zu stellen.“

Ein neues Sicherheitsverständnis entwickelt sich derzeit auch durch das Thema Cloud Computing. Noch vor zehn Jahren war es für Unternehmen undenkbar, sensible Geschäftsdaten außerhalb der eigenen Firewall abzulegen. Viele Anwender sind derzeit gegenüber Cloud Computing so vertrauensvoll geworden, dass sie nicht darauf achten, wie sicher ihre sensiblen Daten gehostet und wie gut sie geschützt werden. Der Annual Security Report 2009 empfiehlt Unternehmen und Organisationen, die Sicherheitsmaßnahmen bei Anbietern für Cloud Computing gründlich zu klären.

Video: Patrick Peterson stellt die Highlights aus dem Cisco Annual Security Report 2009 vor
http://www.youtube.com/v/u9XBft_nCJ4=en_US=1

Security Intelligence Operations:

<http://tools.cisco.com/security/center/home.x>

Text- Download unter: http://www.cisco.com/web/AT/presse/aktuelles/ak_home.html

Aktuelle Informationen von Cisco Austria sind über die Kurznachrichten-Plattform „Twitter“ (www.twitter.com/Cisco_Austria) abrufbar.

Weitere Informationen:

Cisco Systems Austria GmbH, Millennium Tower, Handelskai 94-96, A-1200 Wien, www.cisco.at
Wolfgang Fasching-Kapfenberger, Tel. 01-240 30-6247, Fax 01-240 30-6300, wfaschin@cisco.com
The Skills Group, Christiane Fuchs-Robetin, Tel. 01-505 26 25-66, fuchs-robetin@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.