






Wie sich die Web-Nutzung verändert hat

Autor(en): Christiane Pütter

08.03.2011

Drucken | Versand | PDF | Vorlesen |     

Social Networks verdrängten 2010 die E-Mail und die Nutzer suchen lieber nachrichtliche Inhalte als Pornografisches, wie eine Studie des Sicherheits-Anbieters Blue Coat ergab.



User kommunizieren lieber über Blogs, Chats und Instant Messaging, als eine E-Mail zu schreiben.
Foto: ErickN - Fotolia.com

Die Krise wirkt sich auch auf die Web-Nutzung aus. Das erklären jedenfalls die Autoren des Blue Coat Web **Security** Report 2011. Der Report basiert auf der Analyse von wöchentlich rund drei Milliarden Anfragen nach Webinhalten. Für 2010 ist den Analysten zweierlei aufgefallen: Die Nutzer **tauschen sich lieber über Blogs, Chats und Instant Messaging aus, als zu mailen**. Außerdem suchten sie im vergangenen Jahr häufiger Nachrichtliches als Porno-Seiten.

Blue Coat glaubt, dass insbesondere Letzteres mit der weltweit hohen Arbeitslosigkeit und "ihren finanziellen Herausforderungen" zusammenhängt. Die "Befriedigung persönlicher Lüste" habe "mehr

geschäftorientierten Inhalten" weichen müssen. Inwieweit sich das mit einer wirtschaftlichen Erholung wieder ändert, lassen die Analysten offen.

Die Studienautoren leiten aus den gesammelten Daten **Thesen für die IT-Sicherheit** im neuen Jahr ab. Ihrer Meinung nach zeichnet sich bereits ab, dass Cyber-Kriminelle auf die Veränderungen reagieren.

Das heißt konkret: Cyber-Kriminelle machen sich die steigende Beliebtheit von **Social Media** zu Nutze. Sie missbrauchen die vertrauensvollen Beziehungen innerhalb sozialer Netze, um beispielsweise Daten für den Zugriff auf Banking-Anwendungen und Online-Konten zu bekommen.

Die Sicherheitsexperten gehen davon aus, dass Kriminelle auch in diesem Jahr versuchen werden, User auf diesem Weg zu infizieren. Soziale Netze entwickeln sich zunehmend zum Angriffsvektor für **Malware**.

Um die Bedeutung von **Social Media** zu verdeutlichen, haben die Studienautoren die **Zahl der Facebook-Nutzer** zusammengerechnet. Ergebnis: "Wäre **Facebook** ein Land, läge es auf dem dritten Platz hinter China und Indien."

Auch auf die Hinwendung zu seriöseren Web-Inhalten reagieren **Hacker**, so der Report weiter. Die Migration der Angriffsinfrastrukturen von kostenlosen Domains auf bekannte Sites mit vertrauenswürdiger Reputation sei "eine der auffallendsten Veränderungen der Bedrohungslandschaft".

Malware wandert auf seriöse Sites

Folge davon: Seriöse Websites zählen in den meisten Unternehmen **nicht zu denen, die wegen Sicherheitsbedenken gesperrt werden**. Malware kann sich über solche Sites also schneller verbreiten. Blue Coat rät IT-Entscheidern daher, sich weniger auf Reputationsbewertungen zu verlassen.

Darüber hinaus gibt der Sicherheitsanbieter CIOs für 2011 Folgendes mit auf den Weg:

- Dynamische Abwehr: Über dynamische Links bauen Cyberkriminelle Angriffsinfrastrukturen auf, bei denen sie lediglich den Speicherort ihrer Malware verändern. Um die Auslieferung von Malware sowie Betrugsmaschen und Phishing zu blockieren, ist eine Abwehr nötig, die dynamisch reagiert, neue und unbekannte Inhalte bewertet und dynamische Links analysiert.

- Echtzeit-Bewertungen: Wenn Abwehrmechanismen Webanfragen nicht in Echtzeit analysieren und sofort Einstufungen zurückliefern, setzen sie ihre Nutzer Angriffen aus, die oft nur wenige Stunden dauern können, so Blue Coat.

Schutz für mobile Nutzer

- Schutz für mobile Nutzer: Weil mittlerweile viele Menschen **von unterwegs aus arbeiten**, muss der Webzugang rund um die Uhr und an jedem Ort geschützt werden.
