

Die neuen Gefahren aus dem Web

Jens Freitag, Senior Technology Consultant, Sophos GmbH

Kriminelle Malware-Autoren und Hacker suchen sich stets neue Wege, um IT-Systeme und PCs zu infizieren, Daten auszuspionieren oder unbemerkt Spam-Mails über fremde Rechner zu verschicken. Dabei haben E-Mail-Attachments als Verbreitungsmethode längst ausgedient. Heute nutzen Cyberkriminelle neue Web 2.0-Anwendungen für ihre Zwecke und hinterlegen Schadcodes vorzugsweise im Internet. Für den Schutz vor den vielfältigen Gefahren des Webs sind geeignete IT-Security-Technologien genauso wichtig wie die Durchsetzung rechtskonformer Sicherheitsrichtlinien.

Die Gefahr webbasierter Attacken wächst: Nach den Analysen der SophosLabs, der weltweiten Forschungszentren von Sophos, nimmt die Anzahl infizierter Websites kontinuierlich zu. Monat für Monat entdecken die Experten 5.000 neu infizierte Internet-Seiten. Lediglich rund jede fünfte Website, auf der Schadcodes hinterlegt ist, wurde dabei für kriminelle Zwecke eingerichtet – bei rund 80 Prozent handelt es sich um eigentlich harmlose Websites, die von Cyberkriminellen gehackt wurden. Ob Internet-Shops, Großkonzerne oder Regierungsbehörden – alle Firmen und Institutionen, die ihre Internet-Seiten nicht ausreichend schützen, können zur Zielscheibe solcher Attacken werden. In der Annahme, dass deren Websites sicher sind, rufen Internet-Anwender die Sites sorglos auf und holen sich so unbemerkt Viren und Würmer auf ihre Rechner.

Zugleich sinkt der Anteil infizierter Mails: Enthielt Anfang 2006 noch jede 77. E-Mail einen Virus, war im September 2007 nur noch eine von 833 Mails mit einem Schadprogramm infiziert. Es ist anzunehmen, dass sich dieser Trend auch in Zukunft fortsetzen wird und die Zahl infizierter E-Mails zugunsten webbasierter Angriffe weiter abnimmt. Nicht ohne Grund: Viele Anwender und Unternehmen schützen ihre E-Mail-Systeme heute mithilfe entsprechender Sicherheitslösungen am Gateway vor Schadcodes. Die Nutzung des Internets erfolgt hingegen oft ohne ausreichende Schutzvorkehrungen.

Die Tücken des Web 2.0

Parallel dazu werden Web 2.0-Anwendungen immer populärer und eröffnen sowohl Anwendern als auch kriminellen Hackern neue Betätigungsfelder. Internet-Nutzer greifen nicht mehr nur unkontrolliert auf Webseiten zu, sondern laden auch immer häufiger Programme, Audio- und Video-Daten aus dem Web herunter und kommunizieren per Instant Messenger mit Kollegen, Freunden und Geschäftspartnern. Cyberkriminelle nutzen dies gezielt für ihre kriminellen Machenschaften aus – mit Erfolg. Denn während sich inzwischen die meisten Nutzer der potenziellen Bedrohung durch E-Mail-Viren bewusst sind, rechnen die wenigsten damit, per Instant Messenger oder durch den Klick auf eine scheinbar harmlose Website ihre Rechner und Daten in Gefahr zu bringen.

Ein Beispiel für die neuen Angriffsmethoden ist der so genannte 'Skype-Wurm', der sich Mitte April 2007 über die Kanäle des bekannten VoIP-Programms verbreitete. Mithilfe einer an die Nutzer versendeten Nachricht mit eingebundenem Link lockten

Cyberkriminelle die ahnungslosen Anwender auf eine Website, auf der das Bild einer jungen Frau zu sehen war. Sobald die User die Site geöffnet hatten, machte sich im Hintergrund ein Trojaner daran, einen Wurm auf dem System des Anwenders zu installieren.

Mehr Sicherheit durch einheitliche Richtlinien

Angesichts der steigenden Risiken bei der Nutzung des Internets und neuer Kommunikationstechnologien ist es vor allem für Unternehmen wichtig, ihre Netzwerke, Rechner und Daten vor unberechtigten Zugriffen und Missbrauch zu schützen. Hierfür sind zum einen geeignete IT-Sicherheitstechnologien notwendig, die Schadprogramme, unerwünschte Applikationen und Hacking-Attacken zuverlässig blocken. Da es sich bei infizierten Websites oft um eigentlich harmlose Internet-Seiten handelt, sollten zudem Web-Security-Lösungen eingesetzt werden, die die Sites nicht nur nach vordefinierten Kategorien filtern, sondern alle Websites auf Schadcodes überprüfen.

Zum anderen ist die Einführung und Durchsetzung firmenweiter Sicherheitsrichtlinien unabdingbar. Firmen sollten zum Beispiel individuell festlegen können, welche Internet-Seiten aufgerufen und welche Web-Anwendungen im Unternehmen genutzt werden dürfen. Ohne entsprechende Schutz- und Kontrollmechanismen laufen Unternehmen Gefahr, rechtliche IT-Sicherheits- und Datenschutz-Vorgaben zu verletzen und vertrauliche Daten zu verlieren. Über die technischen Vorkehrungen sowie die Definition und Durchsetzung verbindlicher Sicherheitsrichtlinien hinaus sollten Unternehmen ihre Mitarbeiter im verantwortungsbewussten Umgang mit Anwendungen und Daten schulen. Nur so profitieren sie auf Dauer von den Vorteilen, die das neue Web zweifelsohne mit sich bringt.