

## Firmen-E-Mail-Adressen begehrtes Ziel von Hackern

Firmenmitarbeiter in Deutschland gehen immer noch zu unachtsam mit der Herausgabe der eigenen Geschäfts-E-Mail-Adresse um. Fast jedes vierte Unternehmen klagt über Missbrauch von Firmenadressen zu Spamzwecken oder um sich Zugang zu Firmennetzen zu verschaffen. Damit ist diese Methode des Angriffs auf Firmen-IT die zweithäufigste nach Viren und Trojanern. Die IT-Abteilungen investieren inzwischen massiv in Sicherheitsvorkehrungen und interne Aufklärungskampagnen. Erste Erfolge sind zu erkennen: Die Zahl der Sicherheitsverstöße aufgrund zweckentfremdeter E-Mail-Adressen ist seit 2005 rückläufig. Vor zwei Jahren lag die Zahl bei 33,7 Prozent, 2006 beklagten sich 27,2 Prozent der Unternehmen über den Missbrauch der elektronischen Postadresse. Zu diesen Ergebnissen kommt die Studie „IT-Security 2007“ der InformationWeek, die zusammen mit Steria Mummert Consulting ausgewertet wurde.

Eine wahre Fundgrube für Firmen-E-Mail-Adressen sind die in Mode gekommenen Business-Netzwerke. Immer mehr Geschäftsleute nutzen diese Plattformen zur Pflege und zum Aufbau von Geschäftskontakten. Dabei geben sie ihre Kontaktdaten samt E-Mail-Adresse häufig uneingeschränkt einer breiten Öffentlichkeit preis. Hacker können sich mit Hilfe dieser öffentlich zugänglichen Angaben eine fremde Identität verschaffen und so weitere relevante Informationen für das Eindringen in ein Firmennetz zusammentragen.

Der Missbrauch der E-Mail-Adressen von Mitarbeitern kann zudem so weit gehen, dass Hacker unter Nutzung des bekannten und seriösen Namens E-Mails versenden können, die beispielsweise schädliche Dateianhänge, Viren oder Trojaner enthalten. Möglich ist das mit so genannten Ghost-Mailern, einer Software, die die Kopfzeile einer E-Mail vollständig manipulieren kann. Die Folge sind erhebliche Imageschäden für die Unternehmen, deren Firmenadresse missbraucht wird. Zwar kam es in diesem Jahr nur bei 6,9 Prozent der befragten Unternehmen zu dieser Form von Identitätsdiebstahl. Der Trend zeigt allerdings nach oben. 2006 lag die Zahl bei 4,9 Prozent und 2005 sogar nur bei 1,1 Prozent.

Als Schutz vor derartigen Sicherheitsverstößen eignen sich in der Regel nur präventive Maßnahmen, da der wahre Absender bössartiger Nachrichten zumeist nicht oder nur sehr unzureichend identifiziert werden kann. Ein komplettes Verbot, sich über Social-Networking-Portale beruflich auszutauschen, wäre allerdings zu drastisch. Mit konkreten Handlungsanweisungen in den IT-Sicherheitsrichtlinien lässt sich jedoch der Zugang zu Firmendaten deutlich erschweren, so dass ein Großteil der Hacker das Interesse verliert. Einfachstes Mittel ist, Firmeninformationen beispielsweise auf den Business-Netzwerkseiten und anderen Portalen nicht für jedermann sichtbar zu machen. Hierzu gehören unter anderem E-Mail-Adressen, genaue Positionsbeschreibungen der Mitarbeiter oder Angaben zu Betriebssystemen, Datenbanken, Netzwerkgeräten und Applikationen. Noch wichtiger sind die Einführung und Umsetzung eines für alle Mitarbeiter verbindlichen IT-Sicherheitskonzepts. Jeder fünfte Betrieb versäumt es derzeit noch, die eigenen Mitarbeiter mit den IT-Sicherheitsbestimmungen ausreichend vertraut zu machen. Zudem eignen sich regelmäßige Schulungen aller Mitarbeiter, um ein

Bewusstsein für die Vorgehensweisen von Hackern zu schaffen. Dazu gehört auch die Weiterbildung der IT-Administratoren, damit sie möglichst denselben Wissensstand haben wie potenzielle IT-Störenfriede.