duktivität. Zwei Scareware-Familien, FakeXPA und FakeSecScan, waren in der ersten Jahreshälfte noch nicht unter den Top 25, wurden aber im zweiten Halbjahr auf mehr als 1,5 Millionen Computern entdeckt und gehören damit zu den zehn häufigsten Sicherheitsgefahren. Zudem wurde der Trojan-Downloader Win32/Renos auf 4,4 Millionen PCs registriert, ein Anstieg von 66,6 Prozent innerhalb eines halben Jahres.

Der Security Intelligence Report zeigt auch, dass sich Angreifer durch die steigende Sicherheit der Betriebssysteme verstärkt auf die Anwendungsebene konzentrieren. Über 90 Prozent der Schwachstellen in der zweiten Jahreshälfte 2008 wurden in Applikationen und Browsern entdeckt. Außerdem bestätigt der Report, dass es merkliche Fortschritte im Bereich Sicherheit bei neuen Versionen von Microsoft-Programmen gibt. Bei Browser-basierten Angriffen auf Windows XP-PCs waren Microsoft-bedingte Schwachstellen zu 40,9 Prozent verantwortlich, im Vergleich zu 42 Prozent im letzten Report. Bei Windows Vista-Computern sank der entsprechende Anteil von 6 auf 5,5 Prozent.

Schließlich weist der Report nach, dass gestohlene und verloren gegangene Computer-Ausstattung mit 50 Prozent weiterhin der häufigste Grund für Sicherheitsprobleme sind. Um diese Gefahr zu mildern, müssen Hardware und Betriebssysteme entsprechend vorbereitet sein. Dies bedeutet für Hersteller, dass sie weiterhin an der Verwirklichung einer End-to-End Security arbeiten müssen. Dazu gehören auch Trusted Plattform Modules und die BitLocker Laufwerksverschlüsselung von Microsoft. Technische Vorkehrungen sind in Unternehmen aber von strengen Sicherheitsrichtlinien zu ergänzen.

Aufgrund der Ergebnisse des Security Intelligence Reports ruft Microsoft alle Beteiligten auf, weiterhin an der Entwicklung von Innovationen zum Schutz der Nutzer vor Online-Kriminellen zusammenzuarbeiten. Unternehmen und Privatnutzer sollten anhand der Richtlinien im Report ihre Sicherheitsvorkehrungen prüfen und verbessern. Dazu gehören die Nutzung von Microsoft Update, automatische Aktualisierungen von Anwendungen und Sicherheitsprogrammen bekannter Anbieter aus vertrauenswürdigen Quellen, Nichtöffnen von Anhängen in Mails oder Instant Messages von unbekannten Absendern, strenge Sicherheitsvorkehrungen bei mobilen Datenträgern sowie für Unternehmen die Nutzung des Microsoft Security Assessment Tools (MSAT) und die Regulierung von Remote Management Software.

Weitere Informationen gibt es unter *www.microsoft.de/sicherheit*.

## Buchbesprechungen

**Haio Röckle**

**Schmeh, Klaus: Versteckte Botschaften (TELEPOLIS): Die faszinierende Geschichte der Steganografie, 246 Seiten, dpunkt Verlag, 2008, ISBN: 3936931542**

Bücher über Informationssicherheit wenden sich normalerweise an Spezialisten und stoßen außerhalb der Fachwelt kaum auf Interesse. Einer der wenigen Autoren, der mit dieser Regel bricht und in seinen Büchern schon seit Jahren auch ein Laienpublikum anspricht, ist der Informatiker Klaus Schmeh. Dieser ist im Hauptberuf für die Gelsenkirchener Firma cryptovision aktiv. Schon Schmehs 2007 erschienenes Buch "Codeknacker gegen Codemacher" war populärwissenschaftlich orientiert und beschrieb die Geschichte der Verschlüsselung in einer Form, die zwar kein wesentliches Fachwissen vermittelt, dafür jedoch als spannende Bettlektüre sehr geeignet ist.

Von der Geschichte der Kryptografie ist es nur ein kleiner Schritt zur Geschichte der Steganografie (unter Steganografie versteht man das Verstecken von Daten). Während es jedoch zu ersterem Thema bereits mehrere Buchveröffentlichungen gibt, hat sich bisher kein Buchautor an der Geschichte der Steganografie versucht. Mit seinem neuen Buch "Versteckte Botschaften", das Ende 2008 im dpunkt-Verlag erschienen ist, will Klaus Schmeh diese Lücke nun schließen. Über einen Mangel an Themen für sein Buch kann sich Schmeh zweifellos nicht beklagen. Versteckte Botschaften gab es bereits im antiken Griechenland, wo der Herrscher Histiaios einem Sklaven eine geheime Nachricht auf den Kopf tätowierte, um diesen später mit
nachgewachsenen Haaren als Boten loszuschicken. Spätere Generationen von Datenschmugglern verwendeten Zigarren-Bestellungen, Musiknoten, mikroskopisch verkleinerte Buchstaben und vieles mehr zur getarnten Nachrichtenübermittlung. Poeten schrieben Gedichte, deren Anfangsbuchstaben sich zu einer Nachricht zusammensetzen, Künstler schmuggelten unbemerkt skandalöse Aussagen in ihre Bilder.

Klaus Schmeh nutzt die große Bandbreite, die das Thema bietet, und zündet in seinem Buch ein wahres Feuerwerk an steganografischen Anekdoten und Methoden. Das Spektrum reicht von steganografischen Zauertricks (die offensichtlich auch das berühmte "Medium" Uri Geller nutzt) bis zu computerbasierten Methoden. Im letzten Teil des Buchs geht Schmeh zudem auf steganografische Nachrichten ein, die seiner Meinung nach gar keine sind, aber von sensationslüsternen Zeitgenossen dazu gemacht werden. Hierzu zählt Schmeh unter anderem den berühmt-berüchtigten Bibel-Code und den kaum weniger bekannten Da-Vinci-Code.

Angesichts dieser Inhalte dürfte klar sein, dass "Versteckte Botschaften" nicht nur ein Fachbuch ist. Ebenso handelt es sich um eine unterhaltsame Lektüre, die immer wieder zum Staunen, Schmunzeln und Nachdenken anregt. Für IT-Sicherheitsfachleute hat das Buch sicherlich wenig konkreten Nutzen, wenn man von ein paar netten Anregungen für den Smalltalk absieht. Sehr gut geeignet ist das Buch dagegen für Personen, die Spaß an technischen Spielereien haben. Die diversen Episoden in "Versteckte Botschaften" sind auch und gerade für Laien problemlos zu verstehen und obendrein äußerst kurzweilig.Im Gegensatz zum Kryptografie-Geschichtsbuch "Codeknacker gegen Codemacher" vom gleichen Autor erfordert "Versteckte Botschaften" praktisch überhaupt kein technisches Verständnis. Kein Wunder, dass inzwischen auch populäre Medien – beispielsweise die Radiosender Deutschlandfunk und WDR 5 – über dieses Buch berichtet haben. Welches andere Buch zu einem Informationssicherheitsthema kann so etwas für sich behaupten?

Der Deutschlandfunk rezensiert das Buch zusätzlich auf seiner Web-Seite. Dort heißt es: "Wer das Buch liest, darf sich nicht nur gut unterhalten fühlen, sondern erwirbt mit Sicherheit gute Voraussetzungen, um in einem Fernsehquiz ganz abseitige Fragen beantworten zu können." Dem ist nichts hinzuzufügen.