Breites Spektrum

Das Expertenforum „IT-Defense 2009“ in Potsdam bot Denkanstöße für Sozialwissenschaftler, IT-Sicherheitsexperten und Computerfreaks.

Was die Angriffe auf die Sicherheit von IT-Systemen betrifft, ist zwischen 1998 und 2001 der Vandalismus, das Verfremden und Zerstören von Websites im Vordergrund gestanden. 2001 bis 2004 war die Zeit der Angriffe mit Hilfe von Würmern. Ab 2004 sind „Botnetze“ entstanden und seit 2006 erfolgt zunehmend die kriminelle Nutzung von Angriffen, berichtete Andrew Cushman, Leiter des *Microsoft Security Response Centers (MSRC)*.

Nach dem *Microsoft Security Report* weist Afghanistan die höchste Infektionsrate von Rechnern mit Schadsoftware auf (76,4 von 1.000, somit 7,64 %), Japan mit 1,8 die niedrigste. Deutschland und Österreich liegen mit 5,3 bzw. 5,2 im ersten Halbjahr 2008 nur wenig darüber, allerdings mit Steigerungsraten von 19,7 Prozent (Deutschland) bzw. 25,7 % (Österreich) gegenüber dem 2. Halbjahr 2007.

Die in Deutschland ermittelte Schadsoftware betraf zu 30,3 Prozent (504.000 infizierte Computer) Trojaner, Downloader und Dropper, zu weiteren 19,2 Prozent (320.000 Computer) andere Trojaner und zu 19,7 Prozent (327.000 Computer) Adware. Würmer (2,8 %) und Viren (1,5 %) sind demgegenüber nur mehr gering vertreten.

Website und Recht. Worauf man bei der Gestaltung einer Website achten muss, um nicht in teure Haftungsfallen zu tappen, berichtete Rechtsanwalt Jörg Heidrich, Justitiar des Heise Zeitschriften-Verlags *(www.heise.de)*. In Betracht kommen vornehmlich Verletzungen des Wettbewerbs-, Marken-, Urheber-, Datenschutz- und des Strafrechts. Bei Blogs können presserechtliche Probleme auftreten, bei Podcasting (Anbieten von Audio- oder Videodateien über Internet) Probleme insbesondere mit dem Urheberrecht und dem Recht am eigenen Bild sowie mit Pornografie und Jugendschutz.

Heimanwender sind häufig Ziel von Datendieben aus dem Internet. Mittels harmlos wirkender Downloads werden Schadprogramme in den Rechner eingeschleust, die geheime Daten ausspionieren können.

Allgemein gilt, dass Diensteanbieter im Internet (Provider) nicht für Inhalte haften, die sie für andere speichern oder übermitteln. Insofern sind sie privilegiert, wobei Bestrebungen im Gang sind, die Provider in den Kampf gegen Urheberrechtsverletzungen einzubinden.

Provider haften für fremde Inhalte, wenn sie von deren Rechtswidrigkeit Kenntnis erlangt haben und die Information nicht unverzüglich entfernt oder gelöscht haben. Für die eigenen Inhalte einer Website haftet man ohnehin voll.

Die Haftung trifft den Betreiber laut Impressum, den Eigentümer nach *Whois,* den Provider ab Kenntnis und kann – dies ist noch strittig – auch den Admin-C (der für die administrativen Kontakte zuständig ist), den Tech-C (den technischen Ansprechpartner) oder den Zone-C (den Ansprechpartner der Name-Server) treffen. Links auf andere Websites, auch Deep-Links, sind, als zum Wesen des Internet gehörend, gestattet, sofern nicht auf rechtswidrige Inhalte verwiesen wird oder vom Betreiber der Website eine Linksetzung auf diese untersagt wurde. Eine Verpflichtung zu regelmäßiger Kontrolle der verlinkten Seiten wird nicht anzunehmen sein. Jedenfalls aber haftet der Linksetzer, wenn er nachträglich Kenntnis von der Rechtswidrigkeit der verlinkten Inhalte erhält. Die Haftung kann sich straf- und/oder zivilrechtlich ergeben. Aus eigenem erklärte Haftungsausschlüsse (Disclaimer) bieten keinen Schutz.

Bei einem Internet-Forum, in das andere Beiträge einbringen können (User Generated Content), ergibt sich das Problem, ob auch der Betreiber des Forums für diese Inhalte haftet. Nach dem zu einer Markenrechtsverletzung ergangenen „Rolex“-Urteil des BGH vom 11.3.2004, Az. I ZR 304/01, mittlerweile bestätigt durch ein inhaltsgleiches Urteil vom 19.4.2007,

IT-DEFENSE

IT-Experten-Forum

An der IT-Defense vom 11. bis 13. Februar 2009 in Potsdam nahmen IT-Sicherheitsexperten aus Staat und Wirtschaft teil. Die Zielsetzung der Veranstaltung ist laut Stefan Strobel, Geschäftsführer des Veranstalters *Cirosec,* eine „Mischung aus hoch spezialisierten technischen Vorträgen, strategischen Konzeptionen und fachspezifischer Unterhaltung mit Tiefgang“ zu bieten. Wegen des großen Andrangs ist die Anzahl der Teilnehmer seit fünf Jahren mit 200 begrenzt.

Die IT-Defense 2010 wird vom 3. bis 5. Februar 2010 in Brühl bei Köln stattfinden.

www.it-defense.de

FOTO: SYMANTEC

Az. I ZR 35/04, betrifft das Haftungsprivileg nicht den Unterlassungsanspruch. Zwar ist dem Forenbetreiber nicht zuzumuten, jedes in einem automatisierten Verfahren unmittelbar ins Internet gestellte Angebot darauf zu überprüfen, ob Schutzrechte Dritter verletzt werden, doch muss er, wenn ihm Rechtsverletzungen bekannt werden, nicht nur das konkrete Angebot bzw. den Eintrag unverzüglich sperren, sondern auch technisch mögliche und zumutbare Maßnahmen ergreifen, um Wiederholungen zu verhindern. Insbesondere, wenn Pseudonyme zugelassen werden, muss eine erhöhte Sorgfalt bei der Überprüfung des Inhalts aufgewendet werden. Für den Forenbetreiber empfiehlt sich, Nutzungsbedingungen festzulegen.

Andrew Cushman: „IT-Systeme werden zunehmend für kriminelle Angriffe genutzt.“

Cold Boot Attack. Der flüchtige Speicher (RAM) eines PCs ist nicht so flüchtig, wie angenommen wird, dass also beim Ausschalten des Geräts alle im Arbeitsspeicher befindlichen Daten gelöscht sind. Wie Bill Paul und Jacob Appelbaum berichteten, sind die Daten sogar bei Zimmertemperatur durch etwa eine Minute noch so weit vorhanden, dass sie bei nur minimalem Verlust ausgelesen werden können. Diese Zeit verlängert sich, wenn die Chips gekühlt werden, wozu Druckluft ausreicht.

Diese Erkenntnisse eröffnen neue Angriffsszenarien, aber auch Chancen für die Forensik. Im RAM sind die Daten unverschlüsselt abgelegt. Schutzmechanismen des Betriebssystems, die nach einem Hochfahren des Computers den Einstieg in die Programme von der Eingabe des richtigen Passworts abhängig machen, können so umgangen werden. Ein typischer Fall wäre, einen auf die Eingabe des Passworts wartenden Laptop zu „crashen“ und dann die Daten aus dem Arbeitsspeicher auszulesen oder die (gekühlten) Chips zu entnehmen und zum Zweck des Auslesens in einen anderen Rechner einzusetzen. Auf jeden Fall empfiehlt sich, einen Laptop, der zeitweise unbeaufsichtigt gelassen wird, abzuschalten und nicht bloß im Ruhemodus weiterlaufen zu lassen.

Jörg Heidrich: „Provider haften nicht für Inhalte, die sie für andere speichern.“

RFID. In Transpondern verwendete Kryptochips können entschlüsselt werden, wenn man sich die Mühe macht, mechanisch bis auf die Ebene der einzelnen logischen Schaltelemente hinabzusteigen. Dazu wird, wie Jan Krissler und Karsten Nohl berichteten, der Chip in feinster Schleifarbeit Schicht für Schicht abgetragen. In einem Mikroskop mit 500-facher Vergrößerung werden die Schaltkreise in ihren Strukturen erkennbar und mit Algorithmen analysiert, die aus der Gesichtserkennung stammen. Mit Computerprogrammen werden sie dann zu einem sinnvollen Aufbau verknüpft, aus dem sich als eine Art des Reverse Engineering die auswertbare Gesamtfunktion ergibt.

Kurt Hickisch

Fotos: Kurt Hickisch