„E-Mails immer verschlüsseln“

IT-Sicherheitsexperte Sebastian Schreiber führt seit Jahren Penetrationstests über Auftrag von Unternehmen durch und ortet Schwachstellen in IT-Systemen.

Herr Schreiber, bei den Penetrationstests versuchen Sie, wie ein Hacker in die Rechner Ihrer Auftraggeber einzudringen. Was sind die häufigsten Schwachstellen, auf die Sie dabei stoßen?

Schreiber: Aus der laufenden Beobachtung der Hackerszene, aber auch durch eigene Entwicklungen, kennen wir etwa 20 Angriffsarten. In etwa 80 Prozent der Fälle führen bereits die Methoden des Cross Site Scripting (XSS) oder der SQL-Injection zum Ziel. Bei XSS werden Codes im Kontext eines anderen ausgeführt; bei der anderen Methode wird einer Eingabe des Benutzers ein zusätzlicher Befehlsinhalt untergeschoben. Derartige Angriffe gelingen bei Webservern, die keine ausreichende Filterung aufweisen, indem Benutzerbezeichnungen nicht auf Plausibilität überprüft werden oder Eingaben nicht auf Sonderzeichen, hinter denen sich schädliche Befehle verbergen. Betroffen von diesen Angriffsarten sind alle Webanwendungen wie die von Banken und Kreditkartenunternehmen, aber auch Chatrooms und Foren – vereinfacht gesagt, alle mit dem Web in Verbindung stehenden Systeme, bei denen etwas über die Tastatur eingegeben werden muss. Hier sind die Webprogrammierer gefordert.

Wenn Sie auf Schwachstellen von Systemen stoßen, wie gehen Sie da vor?

Schreiber: Die Vorgangsweise und die Eindringtiefe in Systeme werden vorher mit dem Auftraggeber abgesprochen. Wir gehen nach Checklisten vor. Die einzelnen Schritte werden dokumentiert; es herrscht das Vier-Augen-Prinzip. Ein Hacker führt natürlich keine solche Qualitätssicherung durch, er arbeitet vielleicht sogar darauf hin, dass das System abstürzt, in das er eindringt. Wir dagegen müssen entsprechende Vorkehrungen treffen. Zum Zehn-Jahres-Jubiläum unseres Unternehmens werden wir eine Pen-Test-Ethik herausbringen, von der wir hoffen, dass sich auch andere Anbieter von Penetrationstests diesem Regelwerk anschließen werden. Wir sehen uns als Vorreiter insofern, als wir das einzige Unternehmen in Deutschland sind, das sich ausschließlich auf Penetrationstests spezialisiert hat.

Sebastian Schreiber: „Wer sich der Gefahr nicht bewusst ist, wird auch keine Gegenmaßnahmen ergreifen.“

Wie groß ist das Interesse daran, seine Rechner abzusichern?

Schreiber: Das Problem liegt darin, dass Diebstahl von Geld sehr schnell erkannt wird, der von Informationen dagegen nicht. Wenn jemand glaubt, es werde nicht regnen, wird er auch keinen Regenschirm mitnehmen, wenn er außer Haus geht. Umgelegt auf die IT-Welt: Wer sich der Gefahr nicht bewusst ist, wird auch keine Gegenmaßnahmen ergreifen, zumal ihr Nutzen in der Kalkulation keinen Niederschlag findet. Bewusstseinbildung ist nach wie vor erforderlich. Ein Täter handelt aus der Anonymität eines Internet-Cafés heraus. Er kann auf die große Zahl setzen – wer könnte schon gleichzeitig Zehntausende Banken überfallen. Im Web kann man das, beispielsweise durch Phishing-Attacken. Ob der Täter für sich handelt oder im Auftrag, ob er die Informationen verkauft oder nicht, bleibt offen. Jedenfalls besteht hier ein Ansatzpunkt auch für die organisierte Kriminalität.

Wo sehen Sie derzeit die größten Gefahren für die IT-Sicherheit?

Schreiber: Am vorsichtigsten sollten die Leute heutzutage bei WLANs und damit zusammenhängend bei Voice over IP, dem Telefonieren über Internet

IT-SICHERHEIT

Penetrationstests

Unter einem Penetrationstest versteht man die Überprüfung eines Informationstechniksystems durch Spezialisten („Tiger Team“), die versuchen, in das System einzudringen und Schwachstellen zu orten, um die Sicherheit zu verbessern.

Die von Dipl.-Informatiker Sebastian Schreiber – damals noch als Student – 1998 gegründete *Syss GmbH* führt über Auftrag von Unternehmen und Institutionen Penetrationstests durch und verhält sich dabei wie ein Hacker, der in ein Rechnersystem eindringen will. Erkannte Schwachstellen werden dem Auftraggeber mitgeteilt und ihm Maßnahmen zum Schließen der Sicherheitslücken empfohlen. Das in Tübingen etablierte Unternehmen beschäftigt 13 Personen. Schreiber ist durch seine Live-Hacking-Auftritte auf Sicherheitsmessen und durch Fernsehauftritte und Fachartikel zu Fragen der IKT-Sicherheit bekannt geworden.

www.syss.de

FOTO: KURT HICKISCH

DATENSICHERUNG

Verdacht auf Kinderpornografie: Immer mehr sichergestellte Datenträger.

Starke Zunahme

Die Zahl der Hausdurchsuchungen gegen Verdächtige wegen Kinderpornografie hat sich 2007 verdoppelt. Immer größere Datenmengen auf den Computern machen den Beamten zu schaffen.

Die Beamten der Kinderpornobekämpfungsstelle im Wiener Landespolizeikommando hatten bereits bis November 2007 doppelt so viele Hausdurchsuchungen gegen Verdächtige (160) wie im gesamten Jahr 2006 (80). Die Datenmenge ist dabei nicht nur durch die Zahl der sichergestellten Datenträger explodiert; 2006 waren es allein 279 PCs, 2007 werden es über 400 sein; hinzu kommen CD-Roms und DVDs.

Die Aufarbeitung der Datenträger wird immer aufwändiger durch die immer größer werdenden Datenmengen pro Datenträger. „Noch vor wenigen Jahren waren ein, zwei Gigabyte auf einer Festplatte eine Sensation“, erläutert Peter Brozek, Leiter der Gruppe zur Bekämpfung der Kinderpornografie im LPK Wien. Heute gebe es Festplatten im Terabyte-Bereich, also tausend Gigabyte. Bei einer Hausdurchsuchung im Sommer zum Beispiel stellten die Beamten einen Computer und mehrere CD-Roms sicher. Auf den Datenträgern fanden sich neben Tausenden erlaubten Pornodarstellungen insgesamt eine halbe Million Kinderporno-Bilder und Kinderporno-Filme.

Immer häufiger entdeckt wird laut Peter Brozek harte Kinderpornografie. Die Opfer werden in den Filmen gefesselt, geschlagen, sie weinen und sind oft unter sechs Monate alt. Ebenso im Steigen ist die Zahl sichergestellter harmlos scheinenden „Posing-Bilder“, Fotos von Kindern in Reizwäsche und Stöckelschuhen. Für die Beamten ist es mühsam, aus einem Fotosatz von mehreren Hundert Bildern diejenigen herauszufinden, die nach dem Strafrecht strafbar sind. Das trifft bei „Posing-Bildern“ nämlich nur dann zu, wenn Großaufnahmen von der Schamgegend zu sehen sind oder die Kinder auf den Fotos „reißerisch verzerrt“ sind.

Zuletzt wurde die Wiener Gruppe zur Bekämpfung der Kinderpornokriminalität im Herbst 2006 um zwei Beamte aufgestockt. Derzeit sind in der Gruppe acht Polizisten beschäftigt. Ihre Arbeit besteht hauptsächlich daraus, Verdächtige aufzugreifen, zu vernehmen und Datenmaterial sicherzustellen und zu sichten, das Kinderpornografie enthalten könnte. Hinweise kommen in drei von vier Fällen in Form von Großaktionen, meist von ausländischen Dienststellen inszeniert. Der Rest sind Hinweise aus eigenen Recherchen und Hinweise aus der Wiener Bevölkerung.

sein. WLANs bieten innerhalb einer Firma den Vorteil, dass keine Drahtverbindungen bestehen oder hergestellt werden müssen und der Anwender mobil ist, haben aber den großen Nachteil, dass der sich über Funk abspielende Datenverkehr mitgehört werden kann. Ähnlich ist es bei Voice over IP: Die digitalisierten Sprachsignale können aufgefangen und aufgezeichnet werden. Prinzipiell sollte WLAN-Verkehr immer verschlüsselt erfolgen. Die technisch hiefür verfügbaren Möglichkeiten sollten auch genutzt werden.

Welche Vorsichtsmaßnahmen sollten im E-Mail-Verkehr und bei Handys angewendet werden?

Schreiber: E-Mails sollten, auch wenn sie drahtgebunden versendet werden, immer verschlüsselt werden. Ein kostenloses Programm dafür ist das aus PGP abgeleitete GPG. Verschlüsseln sollten Sie, so viel Sie können. Wenn man bei einem Handy die Bluetooth-Verbindung nicht braucht, weil kein Freisprechen erforderlich ist, sollte man diese Verbindung entweder ab- oder zumindest unsichtbar schalten. Mit Bluetooth betriebene Geräte suchen sich nämlich immer einen Ansprechpartner in der näheren Umgebung; das könnte für Angriffe ausgenützt werden.

Welche allgemeinen Verhaltensregeln empfehlen Sie?

Schreiber: Umsicht und Vorsicht sind geboten und eine kritische Einstellung gegenüber dem Internet. Man muss sich mit der Technologie auseinandersetzen, um zu verstehen, wie etwas funktioniert, und Dinge hinterfragen. Es empfiehlt sich, den Rat von Experten einzuholen.

Interview: Kurt Hickisch

FOTO: EGON WEISSHEIMER