

Kunst der Täuschung

Auf der IT-Defense 2007 in Leipzig referierten international anerkannte Experten über Möglichkeiten im Bereich der IT-Sicherheit.

Zum fünften Mal wurde in Deutschland die „IT-Defense“ abgehalten, diesmal in Leipzig. Die 200 Plätze für die Veranstaltung vom 7. bis 9. Februar 2007 waren bereits im Dezember 2006 ausverkauft. Jeder zehnte Teilnehmer kam aus Österreich. Vorangegangen war ein zweitägiges Training („Hacking Extreme“), eine Intensivausbildung, um Angriffsmethoden zu erkennen und abzuwehren.

Cirosec-Geschäftsführer Stefan Strobel stellte die Zielsetzung des Kongresses dar: Mit erstklassigen Profis an zwei Tagen vor Fachleuten wie Sicherheitsbeauftragten, EDV-Leitern, Administratoren, Datenschutzbeauftragten, Entwicklern, aktuelle Fragen der IT-Sicherheit auszubreiten und zu diskutieren, mit der Möglichkeit, am dritten Tag in Form von Round-Tables in kleinen Gruppen im Gespräch mit den Referenten noch tiefer in deren Spezialgebiet einzudringen. Geboten werden sollen anstelle akademischer Konferenzen, „Themen und Referenten, die uns auch selbst Spaß machen.“ Dementsprechend breit gefächert war das Vortragsprogramm.

IT-Sicherheit. Ein etwas düsteres Bild der Entwicklung der IT-Sicherheit zeichnete Felix „FX“ Lindner. Die Fehlerhäufigkeit von Programmen liege seit 20 Jahren konstant zwischen 0,5 und 2,0 pro 1.000 Programmzeilen, wogegen sich der Umfang kommerzieller Software im Durchschnitt alle 18 Monate verdopple. Die Zahl der Sicherheitsfachleute könne nicht im



Kevin Mitnick: „Der Angreifer muss Vertrauen aufbauen, um Daten zu erlangen.“

gleichen Ausmaß vergrößert werden. Allein die Entwicklung eines neuen Betriebssystems, das kürzlich auf den Markt gekommen ist, habe mehr gute Sicherheitsfachleute erfordert, als der Markt hergegeben habe. Auch in offenen Programmen, deren Quellcode frei zugänglich ist und die durch die „Community“ weiterentwickelt werden, sieht Lindner keine Besserung: „Warum sollten erfahrene Leute



Felix Lindner: „Mehr Sicherheitsexperten nötig, da immer mehr Software.“

umsonst arbeiten, wenn sie eine Menge Geld verdienen könnten?“ Durch die Abschottung der Systeme mit Firewalls werde immer mehr der Anwender zum Angriffspunkt; die in Hackerkreisen bekannt gewordenen Verwundbarkeiten nicht serverbasierter Anwendungen ist in den letzten Jahren im Steigen begriffen.

Bot-Netze. Ein Angreifer kann dazu übergehen, Rech-

ner so in seine Gewalt zu bringen, dass sie wie Roboter einem einheitlichen Befehl folgen und beispielsweise über einen als Angriffsobjekt ausgewählten Rechner gleichzeitig so herfallen, dass dieser lahmgelegt wird („distributed Denial of Service-Attacks“) – was auch für Erpressungen ausgenutzt werden kann. Der zentrale Rechner sucht im Internet automatisch nach Rechnern, die er mit einem Schadcode infizieren kann, und diese suchen wiederum andere. Die Malware verbreitet sich selbstständig.

Eine Gegenmaßnahme besteht darin, Fallen zu stellen, in denen dem suchenden Angreifer vorgespielt wird, es liege ein über eine Schwachstelle für ihn infizierbares System vor. Über die bekannten „Honigtöpfe“ („Honey Pots“) hinaus soll der Angreifer veranlasst werden, interaktiv mehr über sich preiszugeben, sodass man zum Schadcode kommt, diesen analysieren und damit mehr über diese Gefahrenquelle erfahren kann.

Über Bemühungen, automatisiert Malware zu sammeln, berichtete der Informatiker Thorsten Holz. Das „Nepenthes“ (<http://nepenthes.mwcollect.org>) genannte Suchprogramm (in der Botanik werden unter Nepenthes Pflanzen verstanden, die mit Enzymen gefüllte Kannen ausbilden, die hineinfallende Insekten verdauen) hat in vier Monaten 50 Millionen Files überprüft und an die 1.000 verschiedene Botnets entdeckt. Die größten Netze umfassten an die 30.000 Rechner. Die Aufbereitung und Analyse der gefundenen

SICHERHEITSMESSE

Die „IT-Defense“ wird von der *Cirosec GmbH*, D-74076 Heilbronn, seit 2003 jährlich in verschiedenen Städten abgehalten. Die 2002 gegründete *Cirosec* bietet herstellernerneutrale IT-Sicherheitsberatung und Implementation und hat die Schwerpunkte der Unternehmenstätigkeit auf dem Gebiet der Netzwerksicherung und der von Web-Applikationen und Datenbanken, mobiler und Wireless-Security, Verwundbarkeits- und Risiko-

Management, Incident Handling und Forensik. Zu dem 20-köpfigen Team gehören Experten, die als Buchautoren, Dozenten oder Referenten internationaler Kongresse bekannt sind.

Ferner führt das Unternehmen Trainings und Seminare auf dem Gebiet der Forensik sowie des Hackings durch, um zum Zweck geeigneter Abwehr mit Angriffsmethoden der Hacker vertraut zu machen. www.cirosec.de



Teilnehmer der IT-Sicherheitstagung im Rahmen der „IT-Defense 2007“ in Leipzig.

Programme erfolgt, ebenfalls automatisiert, in einer abgeschotteten „Sandbox“ (www.cwsandbox.org).

Social Engineering. Täuschungshandlungen gegenüber Menschen, um zu Informationen zu gelangen, werden „Social Engineering“ genannt. Es geht darum, das Vertrauen eines anderen zu gewinnen, um diesen zu veranlassen, vertrauliche Informationen preiszugeben.

Ein Meister der Informationsgewinnung auf diese Weise war Kevin Mitnick. Der verurteilte Hacker stellt heute seine Erkenntnisse und Erfahrungen zur Bekämpfung dieser Art von Angriffen auf IT-Systeme zur Verfügung – als anerkannter Fachmann, Keynote-Speaker auf Kongressen und Buchautor („The Art of Deception“, 2002; „The Art of Intrusion“, 2005). Bei der IT-Defense berichtete er

über seine Erfahrungen und stellte sich für einen Round Table zur Verfügung. Als „Social Engineer“ müsse man ein überzeugendes äußeres Auftreten und ein gewinnendes Wesen am Telefon mitbringen, die Fähigkeit, sich als „Good Guy“ darzustellen, dem man Vertrauen schenkt und dem man einen überzeugend vorgebrachten Wunsch nicht abschlagen kann. Die Schwachstelle Mensch wird ausgenutzt, dem Hilfsbereitschaft anezogen und im Berufsleben zur Pflicht gemacht wird, der anderen vertraut und keinen Grund sieht, an deren Glaubwürdigkeit zu zweifeln – der auch nicht ahnt, welche Folgen zu große Vertrauensseligkeit haben kann und glaubt, es treffe immer nur die anderen.

Passwort für ein Schokoladenei. Die Werkzeuge des Angreifers sind Telefon und

E-Mail. Er braucht sich nicht um unterschiedliche Betriebssysteme zu kümmern, die Suche nach offenen Ports und Firewalls; er braucht auf keine verräterischen Logfiles Rücksicht zu nehmen – und das bei minimalem Risiko, geringen Kosten und einer fast hundertprozentigen Erfolgsquote.

Der Angreifer kann zunächst versuchen, zu einem Passwort zu gelangen – was offenbar nicht einmal schwer ist. Bei einem unter Mitarbeitern der Waterloo Station in London durchgeführten Test waren 70 Prozent bereit, ihr Passwort für ein Schokoladen-Osterei herzugeben. Im Jahr zuvor waren es 90 Prozent, denen als Gegenleistung ein Kugelschreiber genügt hatte.

Am anfälligsten sind Help-Desks, die ja darauf trainiert sind, jemandem zu helfen. Wer glaubwürdig behauptet, sein Passwort ver-

gessen zu haben, kann mit entsprechender Hilfe rechnen, muss allerdings auf unerwartete Fragen gefasst sein, für die sich ein vorbereitetes Ausstiegsszenario empfiehlt. Man kann einen gerade einlangenden dringenden Anruf vortäuschen, der zu einem Abbruch des Gesprächs zwingt, verbunden mit der Ankündigung einer neuerlichen Kontaktaufnahme – wenigstens weiß man jetzt, welche Fragen gestellt werden und worauf man sich für den nächsten Anruf vorzubereiten hat.

Auch Phishing-Mails können nützlich sein, sich einen Zugang zu verschaffen, etwa mit der getürkten Mitteilung, der Empfänger habe einen Geldbetrag erhalten und müsse zur Bestätigung nur noch seinen Zugangscode in ein Adressfeld einsetzen. Der Angreifer muss Vertrauen aufbauen, wozu ein gewisses Insi-

Ihr Partner für

**KUNDENKARTEN
POS-TERMINALS
BONUS-SYSTEME** Cards & Systems

- Kreditkarten
- Bankkarten
- Kundenkarten

G Cards & Systems EDV-Dienstleistungs GmbH
Landstraßer Hauptstraße 5, 1030 Wien
Tel.: 01 / 790 33-0, Fax: 01 / 790 33-900
service@cardsys.at, www.cardsys.at

Dr. med. Eva-Maria Liebhart
Fachärztin für Gynäkologie und Geburtshilfe
Kinderwunsch
A-1200 Wien, Engerthstraße 56, Tel. 0664/635 26 48
Di. 18.00 - 20.00 Uhr, Mi 15.30 - 18.00 Uhr
Termin nach tel. Vereinbarung, keine Kassen

BeautyLINE Cosmeticvertrieb, Haider & Mag. Schumann GmbH
Wellness & Bodystyling

FON +43(0)1/368 84 66
FAX +43(0)1/368 84 66 - 4
E-MAIL: office@beautyline.co.at
BÜRO: PAPPENHEIMGASSE 35/3, A-1200 WIEN

DR. MED. RONALD RINGL
FACHARZT FÜR ZAHN-, MUND- UND KIEFERHEILKUNDE

A-1030 WIEN
LÖRBERGASSE 15
TEL: 713 44 30
www.meinzahnarzt.cc

der-Wissen gehört. Es geht um Namen, Titel, Positionen, Tätigkeitsbereiche und Sachbearbeiter, Organisationsstrukturen, Telefonnummern, persönliche Vorlieben, Biografien. Manche dieser Informationen sind offen zugänglich wie Darstellungen des Unternehmens im Internet, Geschäftsberichte, Werbeausendungen. Man kann sich aber beispielsweise auch als Stellensuchender ausgeben und mit dem Ziel der Informationsgewinnung durchfragen.

Eine Methode dazu stellt auch das „Dumpster Diving“ dar, umgangssprachlich „Mistkübel stieren“. Im Abfall finden sich Korrespondenzen, Namen, Pläne, Adressen- und Telefonverzeichnisse, Handbücher, Kalender, Datenträger, Ausdrucke. „One man’s trash is another man’s treasure“ (Der Abfall des einen ist der Schatz des anderen). Mit Hilfe derartiger Unterlagen lassen sich glaubhafte Geschichten aufbauen, warum man dieses oder jenes haben will, und es lässt sich Vertrauen aufbauen.

„Hören Sie auf Ihr inneres Unbehagen“, rät Mitnick, damit derartige Angriffe nicht zum Erfolg führen. „Achten Sie darauf, wenn Ihr Gegenüber bei Fragen nach seiner Erreichbarkeit unbestimmt bleibt, sich Nachfragen entzieht, ungewöhnliche Verlangen gestellt werden, man sich Ihnen anzubiedern versucht oder Autoritäten ins Spiel gebracht werden.“ Man kann nicht alle Anzeichen versuchten Ausspähens erkennen, meint Mitnick, und die Mitarbeiter müssten auch nicht wie Lügendetektoren arbeiten.

Der Schlüssel liege darin, sie dazu zu bringen, sich an die Sicherheitsrichtlinien zu halten, die einfach und klar abgefasst sein müssten. Rol-

lenspiele könnten zu solchen Verhaltensweisen beitragen, und das Management müsse in ein derartiges Training eingebunden werden. Was die Umgangsformen betrifft, muss ein „Nein“ als Antwort akzeptiert werden. Das Bewusstsein für die Wichtigkeit von Information muss verstärkt werden, ständige Wachsamkeit ist geboten.

Penetrationstests sollten nicht nur mit technischen Mitteln, sondern auch mit solchen des Social Engineering durchgeführt werden, unter Einbeziehung des „Dumpster Divings“. Über Social Engineering geführte Angriffe sollten gleich gewertet werden wie technische Angriffe, und entsprechende Reaktionen auslösen.

RFID-Chips können trotz ihres derzeit noch geringen Speicherplatzes durchaus der Gefahr von Viren und Würmern ausgesetzt sein. Voice over IP (VoIP), Telefonieren über Internet, kann zu Spät (Spam over IP) führen, sodass dann beispielsweise über „BotNets“ akustisch für *Viagra* geworben wird.

Cirosec-Mitarbeiter Tobias Klein stellte die Arbeitsweise eines Programms für *Linux/Unix* zur Aufdeckung von Rootkits vor, das bei laufendem Betrieb eingesetzt werden kann, wodurch einer etwaigen Verschlüsselung der Daten beim Abschalten des Computers zuvorgekommen wird (Rootkits sind Programme, die sich im Innersten eines Rechners verstecken können und dadurch normalerweise unangreifbar bleiben).

Die nächste IT-Defensive (www.it-defense.de) ist für Ende Jänner 2008 in Hamburg geplant.

Kurt Hickisch