



Live-Hacking: Demonstration eines Angriffs auf einen Rechner, mit frei im Internet erhältlichen Programmen.

## Angriff über Babyphon

Auf der „Systems“ vom 23. bis 26. Oktober 2007 in München wurden verschiedene Angriffsarten auf Computersysteme vorgeführt.

Eine der fünf Ausstellungshallen der „Systems 2007“ war ausschließlich der Sicherheit in der Informations- und Telekommunikationstechnologie vorbehalten; überproportional war etwa ein Viertel der insgesamt 1.200 Aussteller in dieser Halle, der IT-Security Area, vertreten und hat die gesamte Bandbreite der Sicherungsmöglichkeiten gegen Angriffe auf Computer und Netze präsentiert.

In den Foren blau (Technik) und rot (Business) wurden im Viertelstundentakt insgesamt mehr als 200 Vorträge abgehalten, die auf Video aufgezeichnet wurden und samt den Handouts zu den Vorträgen im Internet unter [www.it-sa.de/programm](http://www.it-sa.de/programm) bis zur nächsten

„Systems“ aufgerufen werden können.

Traditionell wurde jeder der vier Messtage mit dem „Morning-Star“, dem Live-Hacking von Sebastian Schreiber der auf Penetrationstests spezialisierten Firma SYSS GmbH eingeleitet. Schreiber zeigte, wie leicht Angriffe auf Rechner durchgeführt werden können, er

griff dabei nicht einmal in die Trickkiste, sondern bediente sich im Internet frei erhältlicher Programmen. Mit Hilfe von Google werden Passwörter und Zugangsdaten in Erfahrung gebracht, oder es werden Preise von Online-Shops manipuliert. Ein Rechtsanwalt wachte darüber, dass die vom Gesetz gezogenen

Grenzen zu Delikten wie Ausspähen oder Abfangen von Daten, Datenveränderung oder Computerbetrug nicht überschritten werden. Zeigte der Anwalt die gelbe Karte, war eine Gefahrenstufe erreicht, die rote Karte bedeutete einen sofortigen Halt.

Vorgeführt wurde auch, wie man einen von einer drahtlosen Überwachungskamera überwachten Wertgegenstand verschwinden lassen kann, ohne dass dies am Monitor bemerkt wird. Die Kamera wird mit Hilfe eines Babyphons mit Bildwiedergabe aufgespürt. Kamera und Babyphon arbeiten auf der Frequenz 2,4 GHz, die Kamera als Sender, das Babyphon als Empfänger. Das vor der Weg-

### SYSTEMS

Die „Systems“ wurde im Jahr 2007 zum 26. Mal abgehalten und findet jährlich in den Hallen der Neuen Messe München statt. Die Messe ist als Fachmesse (B2B) ausgerichtet und hat 2007 über 40.000 Besucher verzeichnet sowie

rund 2.000 Kongressteilnehmer. Auf einer Ausstellungsfläche von rund 55.000 Quadratmetern haben 1.198 Unternehmen aus 28 Ländern ausgestellt.

Die nächste „Systems“ wird von 21. bis 24. Oktober 2008 stattfinden.



**Das Babyphon kann als Übermittler falscher Bilder an Überwachungskameras missbraucht werden.**

nahme des überwachten Gegenstands aufgenommene Bild wird aufgezeichnet und wieder eingespielt, so dass die Wegnahme nicht bemerkt wird. „Wir haben bei Rundgängen in Städten mit dem Babyphon alles Mögliche zu sehen bekommen, nur keine Babys“, berichtete Schreiber von derartigen Geräten, die um etwa 100 Euro im Handel erhältlich sind.

**Ein USB-Stick** besonderer Bauart kann so manipuliert werden, dass beim Anstecken an einen Rechner das System von ihm aus hochgefahren wird – ein Trojaner gleich mit. „Was glauben Sie, was passiert, wenn derartige USB-Sticks als Werbegeschenk verteilt werden?“, fragte Schreiber. „Es steckt ihn doch jeder gleich einmal an seinen Rechner an.“

Auch auf ein Handy kann ein Trojaner gebracht werden, der beispielsweise einlangende SMS unbemerkt weiterleitet. Das Handy kann zur Wanze werden, indem es so manipuliert wird, dass es ohne Zutun des Besitzers Gespräche abhört und dem Abhörenden weiterleitet. Für einen Lauscher kann nicht nur wichtig sein, was in den Vorstandssitzungen besprochen wird, sondern mitunter sehr viel mehr, was vorher von den Teilnehmern untereinander

beredet wird. Die Mitnahme von Handys in den Sitzungsraum zu verbieten, reicht unter solchen Umständen nicht aus. In kritischen Situationen ist es am sichersten, Handys nicht nur auszuschalten, sondern durch Entnahme des Akkus zu deaktivieren.

**Ungesicherte Funknetze**

haben es Schreiber besonders angetan. Immerhin haftet derjenige, der eine solche Anlage betreibt, für die Inhalte, die von dort aus ins Netz gehen, und zwar auch dann, wenn über ihn, weil er sein Netz unverschlüsselt betreibt, andere Inhalte eingespeist werden können.

Beim „Wardriving“, dem Aufspüren von WLANs vom Auto aus, können die Sender über GPS auf die Hausnummer genau lokalisiert werden. In Wien hat Schreiber festgestellt, dass 31 Prozent der untersuchten WLANs unverschlüsselt betrieben werden; am besten abgeschnitten hat Köln mit lediglich 19 Prozent. Von der Rechtsprechung wird allerdings die Standard-Verschlüsselung als ausreichend angesehen; ein besonderer Geheimhaltungsgrad wird nicht gefordert, liegt aber im eigenen Interesse.

**RFID-Tags** findet man schon häufig im Alltagsleben, im Einzelhandel, bei der Lagerhaltung, in Aus-

SKODA & MOSHAMMER

ÖFFENTLICHE NOTARE

DR. CLEMENS MOSHAMMER  
DR. WOLFGANG SKODA  
A-1100 WIEN • KEPLERPLATZ 14  
TEL. (+43 1 ) 602 41 09 • FAX DW -99  
NOTARE@SKODA-MOSHAMMER.AT  
U 1 KEPLERPLATZ – LIFT



**MEGATON Ges.m.b.H.**

Franz Schubertgasse 12A  
A-2372 Gießhübl

Tel.: 02236/43179 - Fax: 02236/43179-21

Beratung, Planung, Vertrieb und  
Errichtung von:

- ALARMANLAGEN
- VIDEOSYSTEME
- ZUTRIITTSKONTROLLEN
- BESCHALLUNGSANLAGEN



**WIRTSCHAFTS - DETEKTEI**

R. VESZTERGOMBI

Tel: 01 319 84 20

Homepage: [www.detektiv-agency.at](http://www.detektiv-agency.at)  
E-Mail: [wdv.detektiv@aon.at](mailto:wdv.detektiv@aon.at)

A - 1090 Wien Porzellang. 14-16

**Prim.Univ.Do.z.Dr. Michael MEDL**

Facharzt für Frauenheilkunde und Geburtshilfe  
Vorstand der gynäkologisch-geburtshilflichen Abteilung  
im Hanusch Krankenhaus

■ Ordination: Heinrich-Collinstr. 8-14/11/1, 1140 Wien  
Telefon: 911 34 40, Fax: 911 34 40 9



LÖSUNGEN FÜRS LEBEN.

Fit in jeder Lebenslage?

Aus der Oberbank Vorsorge-Kollektion:

Der Oberbank-Vorsorgeplan.  
Bereits **ab EUR 35,-/Monat**  
die finanzielle Zukunft sichern.

[www.oberbank.at](http://www.oberbank.at)

**Oberbank**  
3 Banken Gruppe

**SYSTEMS 2007**



„Systems 2007“: 40.000 Besucher, 2.000 Aussteller.

weisen und bei der berührungslosen Zutrittskontrolle oder in Sportschuhen, um den Start und Zieleingang eines Läufers zu registrieren, bei der Kennzeichnung von Tieren; sie können auch Menschen unter die Haut gepflanzt werden. Gegenüber dem Barcode sind sie berührungslos und ohne Sichtkontakt auslesbar.

*RFID-Tags* enthalten eine weltweit einzigartige Nummer (ein Barcode kennzeichnet hingegen lediglich eine Produktkategorie). Für den Kunden sind sie komfortabel, bringen aber einen Kontrollverlust insofern mit sich, als er nicht mehr erkennt, wann der Code ausgelesen wird.

**Mit Fragen des Kontrollverlustes** hat sich ein Referat der Firma *VisuKom* ([www.visukom.net](http://www.visukom.net)) beschäftigt. Es handelt sich dabei um ein Unternehmen, das IKT-Netzinfrastrukturen auf Sicherheitsrisiken prüft sowie Schwachstellen aufspürt und beseitigt.

In Kaufhäusern können *RFID-Tags* (im Jahr 2006 wurden über eine Milliarde davon verkauft) dazu verwendet werden, das Einkaufsverhalten von Kunden zu erfassen, etwa, welche Bereiche aufgesucht und welche eher gemieden werden, und letztlich kann auch der Weg des einzelnen Kunden verfolgt werden. Ent-

sprechende Abschirmmethoden wie Pass- und Kartenschutzhüllen wurden bereits entwickelt; ein RFID-Scannerdetektor-Armreif zeigt durch Aufleuchten einer Leuchtdiode an, wenn sich ein Scanner in der Nähe befindet. Auch vor Hacken und Manipulation von Inhalten oder einer Duplikation des Tags ist man nicht mehr sicher.

**Blickschutzfilter.** Um zu verhindern, dass beim Arbeiten am Laptop, etwa im Flugzeug oder in der Bahn, jemand von der Seite oder vom Rücksitz her mitliest, hat *3M* für Notebooks und Flachbildschirme ein Blickschutzfilter entwickelt. Die Folie engt durch eine Mikrolamellentechnologie den einsehbaren Bereich eines Flachbildschirms auf den unmittelbar davor Sitzenden ein. Mitlesen von der Seite her wird dadurch verhindert.

Die *Gesellschaft für technische Sonderlösungen – GTS* ([www.gtsl.de](http://www.gtsl.de)), Frankfurt, hat sich darauf spezialisiert, verbotene Inhalte von Webseiten, wie etwa Kinderpornografie, aufzuspüren, und Anbahnungsgespräche zu erkennen. Die automatisiert ablaufenden Verfahren sind in der Lage, Schriftzeichen und Schriften auch von außerhalb des europäischen Sprach- und Kulturraums in europäische Sprachen zu übersetzen. *Kurt Hickisch*

FOTO: KURT HICKISCH

**aquacity**  
St. Pölten

3100 St. Pölten  
Schießstattring 15

Tel.: 02742 / 352 661-0  
Fax: 02742 / 352 661-19

[www.aquacity.at](http://www.aquacity.at)