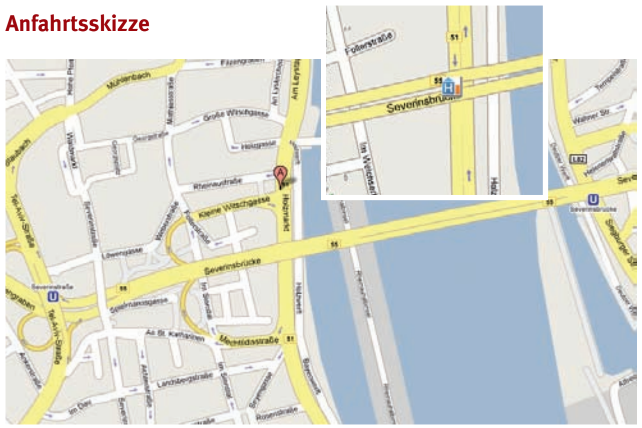
13. Mai 2009 | Köln
17.00 bis 21.00 Uhr
Organisation und Durchführung: Network Computing

Programm

16.30h		Check-In
17.00h		Vortrag: Spionage hat Konjunktur – Lagebericht 2009 KoSiB eG, Vorstand, Boris Bärmichl
17.30h		Kaffeepause
18.00h		3 Stunden Live-Hacking mit Sebastian Schreiber, White-Hat-Hacker und Geschäftsführer SySS GmbH
ca. 21.00h		Get-together mit Fingerfood und Bier

Veranstaltungsort: **NH Köln-City**
Holzmarkt 47
50676 Köln

Anfahrtsskizze



Anmeldecoupon

Hacking-Night Köln
Teilnahmegebühr: Euro 149,00 netto

Anmeldung bis zum 11. Mai 2009 unter

Fax: +49 (0)81 21-95 15 98

Vollständige Firmenbezeichnung

Abteilung

Ansprechpartner

Straße

PLZ, Ort

Telefon, Fax

E-Mail (Ich bin damit einverstanden, von Ihnen per E-Mail Informationen zu erhalten.)

Homepage

Abweichende Rechnungsanschrift

Ort / Datum / Stempel / rechtsverbindliche Unterschrift

Organisation:

13. Mai 2009 | Köln
17.00 bis 21.00 Uhr

Organisation und Durchführung:
Network Computing

Veranstaltungsort:

NH Köln-City
Holzmarkt 47
50676 Köln

13. Mai 2009 | Köln
17.00 bis 21.00 Uhr
Organisation und Durchführung: Network Computing

network Computing
Tests • Trends • Technik für CIOs • CTOs • CSOs

»10 Jahre Live Hacking«

– eine Maßnahme zur Erzeugung von Security Awareness

Im Gegensatz zu anderen Gefahren des geschäftlichen sowie privaten Alltags werden Missbrauchsfälle im Bereich der IT-Security den Opfern in aller Regel nicht bekannt: vertrauliche Daten, die z.B. durch Hackerattacken gestohlen werden, sind trotz des Datendiebstahls noch auf der Festplatte und der Diebstahl bleibt völlig unentdeckt. Wird Computerspionage in einem Unternehmen aufgedeckt, erfolgt die Behandlung des Vorfalls normalerweise streng vertraulich und wird auch nicht bekannt gemacht. Daher wird so ein Fall auch nicht zum Präzedenzfall, der anderen im Umgang mit eigenen Sicherheitsvorfällen dienen kann.

Menschen bewerten Gefahren intuitiv – aufgrund der mangelnden Erkenntnis über Schadensfälle wird daher IT-Security völlig unterbewertet. Um Menschen davon zu überzeugen, dass IT-Risiken keinesfalls hypothetisch, sondern sehr konkret sind, führt der Autor seit nun mehr 10 Jahren Live Hackings im In- und Ausland vor, bisher war er schon in über 20 Ländern.

Demonstriert werden Attacken, die zum einen schnell durchzuführen und zum anderen einfach zu vermitteln sind. Unter keinen Umständen darf während eines Live Hackings gegen geltendes Recht verstoßen werden; dies ist insbesondere im Ausland relevant, sofern ein besonders scharfes bzw. ein unklares Hackerstrafrecht herrscht.

Der Autor demonstriert besonders gerne folgende Attacken:

1. Angriff auf trojanisiertes Nokia-Handy
Während »alte« Handys in erster Linie Telefone waren, sind heutige Mobiltelefone vollwertige Computer; sie verfügen über Betriebssystem, Webbrowser und Mailprogramm – und lassen sich ähnlich wie andere Computer trojanisieren. In der Demo wird gezeigt, wie sich ein trojanisiertes Handy als Wanze missbrauchen lässt.

2. Einfache Angriffe auf Webshops
Für einen Kriminellen sind Web-Shops attraktive Angriffsziele; sie beherbergen vertrauliche Kundendaten und bilden Geschäftsprozesse ab, über die viel Geld umgesetzt wird. Mittels drei völlig unterschiedlicher Angriffe wird gezeigt, wie sich Web-Shops überlisten lassen.

3. Google-Hacking
Streng vertrauliche Daten gelangen immer wieder durch menschliche Fehler und Nachlässigkeit ins Internet. Hier wird gezeigt, wie unter Anwendung der Suchmaschine Google Listen mit Login-IDs und Passwörtern angezeigt und vertrauliche Überwachungskameras ausgespäht werden können.

4. XSS-Attacke
XSS ist eine komplexe Attacke, durch die sich fremde Identitäten auslesen und übernehmen lassen (»Identity Theft«). Die Attacke an sich ist sehr komplex, lässt sich aber anhand eines Beispiels plastisch darstellen.

5. SSL-Attacke gegen Internet-Banking (PINs/TANs)
SSL gewährt die sichere Übermittlung von Passwörtern, Kreditkartennummern sowie PINs und TANs. Es wird gezeigt, wie sich die verschlüsselte Kommunikation unter Anwendung eines Man-in-The-Middle-Angriffs aufbrechen und manipulieren lässt.

6. Hardwarespion
Auch wenn die PCs seitens ihrer Betriebssysteme durch eine Personal Firewall und sonstigen Virenschutz ausreichend gesichert sind, lassen sich mit Spionage-Hardware effektive und unerkannte Spionage-Attacken durchführen.

7. Angriff auf drahtlose Überwachungskameras
Im Handel verfügbare drahtlose Überwachungskameras sichern die Kommunikation zwischen Kamera und Überwachungsmonitor äußerst mangelhaft, nämlich überhaupt nicht. Der Angriff ist mit günstiger Hardware durchführbar – und zeigt, dass sich die Hersteller mehr für die Absatzchancen ihrer Produkte interessieren als für deren Sicherheit.

8. »Mogeln bei Moorhuhn« – der andere Weg zum Highscore
Ähnlich wie professionelle Anwendungen sind auch Computerspiele im Internet Client-Server-Applikationen; wird auf die Sicherheit des Clients vertraut, so lassen sich spektakuläre Attacken leicht demonstrieren.

9. Sniffing trotz Switch
Unter Anwendung von ARP-Cache-Poisoning und ARP-Relaying wird gezeigt, wie sich unverschlüsselte Kommunikation wie Printing, VoIP, etc. ausspähen lässt.

10. Angriff per USB-Sticks
Microsoft hat für USB-Massenspeicher das Feature »Autorun« deaktiviert, d.h. ausführbare Dateien auf USB-Sticks werden »eigentlich« nicht beim Anschließen an den PC gestartet. Manipuliert man den USB-Stick allerdings, so lässt sich dieser Schutz leicht umgehen.

11. Kreditkartenzahlung im Internet
Zahlungssysteme von kleinen sowie großen Webshops werden in der Regel über Payment-Provider abgewickelt. Die im Einsatz befindlichen Geschäftsprozesse lassen sich oft ohne großen Aufwand überlisten. Die Angriffe sind von unglaublicher Schlichtheit und verblüffen die Zuschauer immer wiede.

12. Bluetooth-Angriff auf Nokia-Handy
Bluetooth ist ein Kurzstreckenfunk-Protokoll, das sich unter Umständen leicht überlisten lässt.

13. Karma-Attacke auf WLAN-Laptops
Mit Hilfe der Karma-Attacke lassen sich sogar über LAN angebundene Notebooks in ein durch den Täter betriebenes WLAN locken: das Notebook lässt sich so vorbei an der Firmenfirewall angreifen; die Kommunikation des Notebooks wird problemlos ausgespäht.

Diese Demonstrationen lösen bei den Zuschauern oft Erstaunen und Unfassbarkeit aus. »Dass es so einfach geht, hätte ich nie gedacht« ist eine häufige Reaktion auf Live Hackings; bei vielen verändert sich danach der Blickwinkel hinsichtlich Computersicherheit und ihres eigenen Umgangs mit ihrem PC. Dennoch beginnt bei der Mehrheit der Computernutzer das Umdenken erst dann, wenn tatsächlich ein Schaden vorgefallen ist.
Dem Autor dieses Artikels ist es daher wichtig, sowohl in der Geschäftswelt als auch bei Privatpersonen ein Bewusstsein für die Wichtigkeit von Computersicherheit zu schaffen. Denn Angriffe auf Computersysteme, Datenausspähung und Datenklau sind an der Tagesordnung und schon durch wenige Sicherheitsvorkehrungen lässt sich oft viel Schaden und damit verbundener Ärger verhindern und auch oftmals viel Geld sparen.

unterstützt von SySS, KoSiB eG Kompetenzzentrum für Sicherheit

Ihr Ansprechpartner

Simone Strohmeier
Projektleiterin Events
Telefon +49 8121 95-1590
E-Mail simone.strohmeier@cmp-weka.de