

**Echte Insider-Informationen von
Security-Experten!**

Hacking Intern

Düsseldorf November 2002. Laut Studie des britischen IT-Security-Unternehmens mi2g - <http://www.mi2g.com/> - verdoppelte sich dieses Jahr die Zahl der Hacker-Angriffe auf kleine und mittlere Unternehmen. Hacker

konzentrieren sich demnach zunehmend auf wenig gesicherte Ziele, zu denen – nicht zuletzt durch die zunehmende Verbreitung von Flatrates und Highspeed-Internetzugängen - auch privat genutzte Rechner zählen. DATA BECKERs neues Standard-Werk zum Thema IT-Sicherheit, **Hacking Intern**, klärt seriös und fundiert über die Strategien und Werkzeuge der Hacker auf und zeigt effektive Schutzmaßnahmen.

Die Autoren versorgen den Leser mit tief greifendem Expertenwissen, das einen fundierten Einblick in die Angriffstechniken und Werkzeuge der Hackerszene gibt und ihn so in die Lage versetzt, Angriffe rechtzeitig zu erkennen und zu vereiteln. Versteckte Sicherheitslücken in Windows-Systemen werden offen gelegt und Strategien zur Absicherung des Rechners gegeben.

Und da auch drahtlose Netzwerke und Clientdienste zunehmend ins Visier der Web-Gangster geraten, vermitteln die Autoren auch für diese Bereiche erprobte Strategien.

Hacking Intern macht Hackern, Skript-Kids und Datenspionen das Leben schwer.[dg]

Titel

Hacking Intern
Lieferbar: 04.11.02
Inhalt: 880 Seiten

Preis

39,95 Euro

ISBN

3-8158-2284-X

Bezugsadresse

DATA BECKER GmbH & Co. KG
Merowingerstr. 30
40223 Düsseldorf

Pressesprecher

David Grosvenor (Fachpresse)
Tel.: +49 (0)211/9331-509
Fax: +49 (0)211/9331-444
dgrosvenor@databecker.de

Jörg Wieters (Tagespresse)
Fon +49 (0)211/9331 - 430
Fax +49 (0)211/9331-444
jwieters@databecker.de

Hacking Intern: Die Autoren



Wolfram Gieseke machte seine ersten Erfahrungen mit Hackern, als er während des Studiums der Künstlichen Intelligenz und Computerlinguistik Netzwerke an der Universität betreute. Später entsagte er dem geruh-samen Akademikerleben und stürzte sich stattdessen in die faszinierende Welt der Internetstartups, wo er unter anderem an der Entwicklung sicherer eCommerce-Systeme beteiligt war. Seit einigen Jahren berät er mittelständische Unternehmen bei Internet- und Intranetaktivitäten sowie den damit verbundenen Sicherheitslösungen und führt Mitarbeiterschulungen durch. Außerdem schreibt er Fachbücher und Artikel für Fachzeitschriften. Er hat bereits mehrere erfolgreiche Anwenderbücher zum Thema Internet und Sicherheit veröffentlicht.



Marko Rogge ist mit seinen 29 Jahren ein freischaffender Sicherheits- und Firmenberater/-Consultant, Autor und mehr. Er hat mehrere Projekte initiiert, teilweise nichtkommerziell, mit dem Anspruch, Anwender, aber auch Professionelle auf wichtigen Gebieten der Informations- und Computersicherheit zu informieren und weiterzubilden, und er orientiert sich stark daran, Wissen und Ideen einem großen Publikum verständlich zu vermitteln. Durch seine Arbeiten und Publikationen versucht Marko Rogge, Usern und Firmen im IT-Sicherheitsbereich die Augen zu öffnen, und wird dabei von vielen Freunden unterstützt. Sozialkritisch betrachtet Marko Rogge viele Bereiche der Informationstechnologie und wertet diese in zahlreichen Berichten aus, um anderen Menschen die Möglichkeit zu geben, ebenfalls mehr darüber zu erfahren. Marko Rogge wurde geprägt und hat sich als Autor weiterentwickelt durch viele Bekanntschaften und Freundschaften zu Programmierern der Antiviren- und Anti-Trojaner-Programme sowie WhiteHat-Hackern der Sicherheitsindustrie.



Marc Ruef konnte sich schon immer für Computer begeistern. Im Alter von neun Jahren entwickelte sich diese Leidenschaft immer mehr Richtung Programmierung und so wurde im Zusammenhang mit künstlicher Intelligenz zunehmend die Funktionsweise von Computerviren ein Thema. Der Einstieg in die Computersicherheit war absehbar. Einmal für das Genre interessiert, publizierte er viele Fachartikel (Zeitschriften und Internet), in denen altbewährte Methoden und neue Techniken vorgestellt werden. Beruflich ursprünglich für die Installation und Administration von Firewall- und Intrusion Detection-Systemen spezialisiert, wurde mehr und mehr der Schritt Richtung Security Tests gegangen. Heute arbeitet er als Spezialist für Security Audits und Penetration Tests, betreut vorwiegend Banken und Versicherungen auf diesem Gebiet. Zusätzlich referiert er regelmäßig als Gastdozent und führt Schulungen im Bereich der Computersicherheit durch.



Uwe Velten beschäftigte sich in seiner Diplomarbeit und auch bei der Deutschen Telekom AG/PZ Telesec mit dem Thema Datenverschlüsselung und Signatur. Dabei standen auch die unterschiedlichen Angriffsszenarien auf Chipkarten und Programmmodulen im Vordergrund. In all den Jahren hat er den Spaß an der Programmierung nicht verloren und entwickelt inzwischen seine eigene Sicherheitssoftware.

Hacking Intern

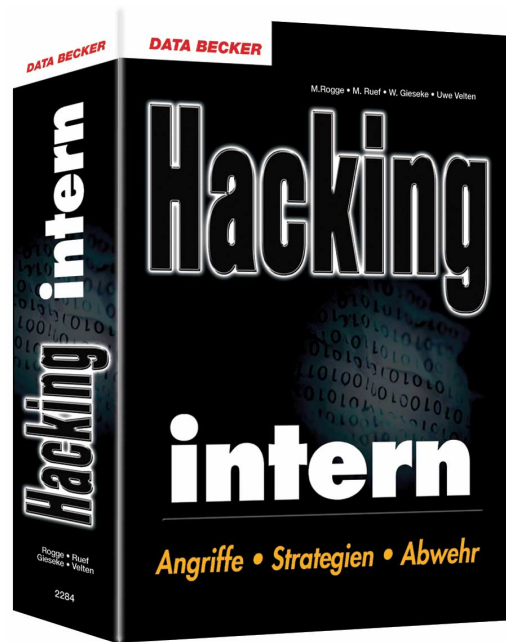
€39,95

Bestell-Nr: 442284

ISBN 381582284X

Lieferbar: 05.11.02

Inhalt: 880 Seiten



aus dem Inhalt

Anatomie einer Attacke: Das Vorgehen der Web-Verbrecher

- Fallbeispiele: Scheinbar „geniale“ Angriffe aus dem Internet
- Systeme und Sicherheitslücken über das Internet gezielt aufspüren
- Typische Angriffsszenarien auf Windows- oder Linuxrechner

Virtuelle Hacker: Viren, Würmer und Trojanische Pferde

- Die unterschiedlichen Angriffsmechanismen im Vergleich
- Computerviren, Trojanische Pferde und Würmer en detail
- Schädliche Skripttypen und –sprachen im kritischen Selbsttest

Unter Beschuss: Client- und Serverdienste

- Heimliche Codeinstallationen beim Internet Explorer
- IRC, Messenger, Outlook & Co. im Viren-Visier
- Übergriffe auf das System via SQL und TS

Risikofaktor Windows: Sicherheitslücken aufgedeckt

- Unsichere Windowskomponenten analysieren und sicher machen
- Usermanagement und Rechtevergabe
- Gefahrenquellen und Schnittstellen auf dem Prüfstand

Projekt Sicherheit: Angriffe vereiteln

- Firewalls, Intrusion Detection und Security Auditing
- Kryptografie und sichere Passwörter
- Biometrie auf dem Prüfstand
- Gefahrenpotenzial im Wireless LAN

... u.a.v.m.