

„Ein Unternehmer sollte wissen, welche aktuellen Gefahren auch seinem Unternehmen im Alltag drohen“



Marko Rogge, IT-Sicherheitsberater

Mit „Hacker“ von Regisseur Alexander Biedermann kam Ende vergangenen Jahres ein Film in die deutschen Kinos, in dem Hacker unterschiedlicher Generationen porträtiert werden. Von den legendären „Btx-Hackern“ Steffen Wernéry und Wau Holland, die am Abend des 19. November 1984 eine Lücke im Btx-System fanden, durch die sie 135.000 DM von der Hamburger Sparkasse auf das Konto ihres Hackervereins transferierten, bis zu Hackern von heute zeigt Biedermann Menschen, die eines verbindet – die geistige Herausforderung, die das Knacken gesicherter IT-Systeme darstellt. Einer der heutigen Hacker ist Marko Rogge. Der Enddreißiger hat sich auf die Sicherheitsberatung von Unternehmen spezialisiert. Chefredakteur Peter Pagel sprach mit ihm über Hacker und IT-Sicherheit und darüber, ob Unternehmer Hackerversteher werden müssen.

Interview Peter Pagel ■ Foto Andre Zahedi

WuM: Was unterscheidet die verschiedenen Generationen der Hacker voneinander?

Marko Rogge: Ich habe beobachtet, dass sich die Definition dessen, was einen Hacker ausmacht, deutlich verschoben hat. War es zu den Anfangszeiten doch mehr spielerisch, so ist heute eine richtige Branche daraus geworden, die immer kommerzieller wird. In den Anfangszeiten war so etwas kaum denkbar und widersprach auch der „Hacker-Ethik“.

Was führt dazu, dass man sich für das Thema IT-Sicherheit begeistert?

Ich kann nur für mich sprechen. IT-Sicherheit ist ein sehr komplexes Thema, das niemals stehenbleibt. Man muss deshalb ständig am Ball bleiben. Aus dem Grund, eben noch mehr herausfin-

den zu wollen, habe ich mich immer intensiver der IT-Sicherheit gewidmet. Aber auch die IT-Sicherheit stellt ja nur eine Schnittmenge der Informationssicherheit dar. Ich denke, dass die meisten Hacker in sich den Forschungsdrang haben, hinter die Kulissen zu blicken und herauszufinden, wie sich Systeme austricksen lassen, und so die IT-Sicherheit auszuhebeln. Daraus gewonnene Kenntnisse können dann zur Erhöhung der Sicherheit beitragen, weil man viele Schwachstellen bereits kennt.

Sind Hacker die Guten, die Bösen oder weder noch?

Grundlegend sollte man klar differenzieren, dass Hacker an sich positiv denkende und handelnde Menschen sind. Sie decken in der Regel Schwachstellen auf und informieren darüber. Das, was man landläufig als böse ansieht, bezeichnet man manchmal auch

als Cracker. In der Regel arbeiten diese mit kriminellern Hintergrund, um sich materiell oder finanziell zu bereichern. Außerdem gibt es die Bezeichnung „Black Hat Hacker“, der eher als Cracker gilt, und die „White Hat Hacker“, die eben die Guten darstellen. Sicherlich dazwischen auch die „Grey Hat Hacker“, die sich, wie der Name schon sagt, in einer Grauzone teilweise am Rande der Gesetze bewegen.

Wäre es für Unternehmen wichtig, die Hackerszene besser zu verstehen?
Unternehmer müssen die Hackerszene nicht zwangsläufig besser kennen oder verstehen. Viel wichtiger ist es, dass Unternehmer für sich die Notwendigkeit sehen, sich vor kriminellen Elementen zu schützen. Ein Unternehmer sollte wissen, welche aktuellen Gefahren auch seinem Unternehmen im Geschäftsalltag drohen können. Dazu zählt ganz weit vorne immer noch der Bereich der professionell betriebenen Wirtschaftsspionage, die häufig auf der Ebene der EDV durchgeführt wird – unter anderem auch deshalb, weil viele Firmen in dieser Hinsicht relativ arglos sind.

Was macht einen guten Hacker aus? Oder: Warum ist jemand, der bloß ein paar Tools zum Einsatz bringt, noch lange kein Hacker?

Die Kreativität, die ein Mensch aufgrund seiner Intelligenz entwickeln kann, wenn es um das Aufdecken von Schwachstellen geht, kann durch kein Tool ersetzt werden. Deswegen ist es insbesondere bei Auditierungen und Sicherheitstests von entscheidender Bedeutung, dass man eine manuelle Überprüfung von Schwachstellen durchführt, indem man beispielsweise die bestehende Sicherheitsstruktur angreift und überwindet. Die daraus resultierenden Sicherheitsverbesserungen haben eine ganz andere Qualität als reines Testen mit gängigen Programmen. In der Praxis muss ein Hacker also wissen, wo die Standards ausreichen und wo er kreativ werden, unvorhergesehene Wege gehen oder Tools effektiv kombinieren muss.

Wie viel IT-Sicherheit ist möglich?

Ein Kollege von mir brachte dazu einmal in seinem Buch ein schönes Zitat, das ich gerne als Antwort nutzen möchte: „Sicherheit der Informationsverarbeitung ist dann gegeben, wenn die Höhe der einzelnen Risiken die Risikohöhe nicht überschreitet, die gerade noch akzeptiert werden kann.“

Dabei muss ein Unternehmer für sich und seine Daten eine entsprechende Analyse durchführen, um die einzelnen Risiken und das Ausmaß des Risikos für sich zu kennen.

Herr Rogge, wir bedanken uns für das Gespräch.

Informationen zum Film „Hacker“ unter: www.hacker-film.de
Mehr über Marko Rogge unter: www.marko-rogge.de

Der Wert der IT – Neue Perspektiven für den Einsatz von IT



WWW.GABLER.DE



Dirk Buchta /
Marcus Eul /
Helmut Schulte-Croonenberg

Strategisches IT-Management

Wert steigern, Leistung steuern,
Kosten senken.

**3., überarb. u. erw. Aufl.
2009. 239 S. Geb. EUR 52,95
ISBN 978-3-8349-1206-0**

Strategisch und umfassend für Top-Entscheider wird der Themenkomplex der IT im Unternehmen ergebnisorientiert und klar verständlich aufbereitet. Mit vielen nützlichen Checklisten.

Einfach bestellen:
buch@gabler.de
Telefon +49(0)611. 7878-626

**KOMPETENZ IN
SACHEN WIRTSCHAFT**

