Die Täter haben sich gewandelt. Oftmals sitzen sie heute vor dem Computer, erpressen einzelne Personen und Unternehmen oder greifen sogar die Infrastruktur eines Landes an. Foto: shutterstock

Hackern einen Schritt voraus

Daniel Hammer lehrt an der Hochschule Offenburg IT-Sicherheit – wie Unternehmen sich vor Angriffen schützen können und über die Spurensuche im Netz

Von Antonia Höft

Tatort im Netz: Im 21. Jahrhundert führen nicht nur Blutspuren zum Täter. Die Täter hinterlassen in manchen Fällen einen digitalen Abdruck. Daniel Hammer, Professor für IT-Sicherheit, bietet an der Hochschule Offenburg Vorlesungen und Seminare an, in denen Studenten die Beweissicherung in der digitalen Welt lernen. Im Interview mit der Mittelbadischen Presse hat er über Spurensicherung im Netz, neue Tätergruppen und die Leichttsinnigkeit der Bürger gesprochen.

■ ***Herr Hammer, Sie bilden an der Hochschule Offenburg also Hacker aus?***

Daniel Hammer: Ja.

■ ***... das heißt konkret?***

Hammer: Bei uns an der Hochschule Offenburg bekommen die Studenten im Studienfach Unternehmens- und IT-Sicherheit (UNITS) eine Grundausbildung, was Informatik, Programmieren und Bertriebssysteme betrifft. Aber auch betriebswirtschaftliche Aufgaben müssen sie beherrschen. Sie wissen dann wie ein Unternehmen funktioniert. Zu diesem Bild gehört natürlich auch, dass man weiß wie man sich verteidigt, wenn man im Netz angegriffen wird.

■ ***Sie geben eine Vorlesung in diesem Studiengang, die sich »Digitale Forensik« nennt. Das bedeutet, dass IT-Kenntnisse mit der klassischen Forensik kombiniert werden. Wie kann man sich das genau vorstellen?***

Hammer: Bei der digitalen Forensik befindet sich der Tatort im Netz. Wie auch bei einem Krimi versucht man, den Tathergang zu rekonstruieren. Wenn beispielsweise bei einem Unternehmen in ein Webserver eingebrochen wurde, wertet man in der digitalen Forensik die Spuren aus und stellt sich die Fragen: Wie tragisch ist der Einbruch? Hat der Täter internes Wissen der Firma gestohlen? Denn aktuelle Studien belegen, dass 90 Prozent der Daten im Unternehmen digital vorliegen. Wenn sich jemand also einhackt, steht ihm viel zur Verfügung, so auch Kundendaten. Der bekannte Forensiker Edmond Locard sagte, wenn zwei Personen Kontakt haben, gibt es immer Spuren. Und das kann man auch auf die digitale Welt übertragen.

■ ***Bei einer Tat in der realen Welt bekommt irgendwer ja mit, wenn eine Person vermisst wird. Wie gehen Signale in der digitalen Welt ein? Bemerken Unternehmen oder Personen nicht meist zu spät, wenn Datenklau stattgefunden hat?***

Hammer: Das stimmt natürlich, wenn der Nutzer nicht achtsam umgeht, wird er nicht bemerken, wenn sein Computer gehackt wurde. Hier gilt dann das sicherheitstechnische Umfeld in einem Unternehmen zu gestalten, was die Studenten bei uns lernen. Das bedeutet, dass sie Angreiferwarnsystem auf dem Netzwerk installieren. Und da müssen die Studenten natürlich wissen, wie ein Hacker vorgeht. Ich habe mal eine Diplomarbeit vergeben mit dem Titel: die Hochschule aus Hackersicht. Wie würde ein Angreifer die Hochschule Offenburg hacken. Es war sehr erstaunlich, wo Dokumente lagen mit Beschreibungen zu bestimmten Hochschulsystemen.

■ ***Und die Arbeit liegt öffentlich einsehbar?***

Hammer: Die war eine gewisse Zeit gesperrt, bis man die Probleme gelöst hatte. Aber mittlerweile kann man sie in der Bibliothek sichten.

■ ***Digitale Forensik befasst sich also mit ausgespähten Daten, Konten-Klau und im Grunde auch Identitätsdiebstahl. Was versteht man unter Live-Forensik?***

Hammer: Der normale Fall ist, dass ein System bereits gehackt wurde. Der IT-Forensiker untersucht also nach dem Vorfall den Computer. Die Untersuchung nennt sich Postmortem-Analyse und findet nach dem Herunterfahren des Systems statt. Anders ist es bei der Live-Forensik, da beginnt die Untersuchung bereits während des Vorfalls, während der Angreifer auch im System ist.

■ ***Wie wird gewährleistet, dass bei solch einer Analyse des digitalen Fingerabdrucks keine Unschuldigen überwacht werden?***

Hammer: Ein digitaler Forensiker will grundsätzlich alle Daten sichern, da diese wichtig für die Analyse sein könnten. Natürlich kann es aber sein, dass das System auch privat benutzt wurde und so persönliche Daten wie Fotos oder Gesprächsverläufe vorliegen, die nichts mit der Tat zu tun haben. Das ist eine Zone, wo Anwälte immer wieder tätig werden, und fordern, dass diese Zusatzinformation nach dem Fall gelöscht werden. Das stellt den Bereich »Digitale Forensik« vor Herausforderungen.

■ ***Seit wann hat die Polizei den Bereich »Digitale Forensik« ausgebaut?***

Hammer: Die Polizei hinkt dem noch hinterher, denn in der allgemeinen Ausbildung kann dieser Bereich nicht abgedeckt werden. Dazu benötigt es viel mehr Spezialisten, denn das Täterbild hat sich über die Jahre gewandelt. Ein Straftäter im Bereich Cyber Crime zu werden ist heute relativ einfach: Wer einen Link zu einer faschistischen Webseite setzt, macht sich schon strafbar. Zudem werden die Täter immer professioneller.

■ ***Wie sieht Ihre Prognose für die nächsten 15 Jahre aus?***

Hammer: Heute haben schon so trivial erscheinende Dinge wie Glühbirnen oder Uhren SIM-Karten, und damit Potenzial für Angreifer. Computer sind in unserer Gesellschaft omnipräsent. Früher war der Computer ausschließlich zum Arbeiten da, heute muss er netzfähig sein. Das bietet Tätern eine große Angriffsfläche und die wird in den nächsten Jahren steigen. Firmen und Menschen werden erpresst, Infrastrukturen eines Landes können angriffen werden, und das macht es spannend für Tätergruppen, die sich bislang mit Kalaschnikows bekämpften. Das Ergebnis ist kein Blut oder Tote.

■ ***Wo liegen die Fehler bei den Opfern?***

Hammer: Das lässt sich in einem Wort zusammenfassen: Ignoranz. Der Hack eines Computersystems fängt mit dem Hack des Menschen an. Wenn Personen denken, keiner könnte etwas bei ihnen holen, ist das ein Irrglaube. Barack Obama hat vor nicht allzu langer Zeit auf Frau Merkels Handy gegriffen und hat eine gigantische Überwachung durch die NSA organisiert.

■ ***Wie können sich Bürger besser schützen?***

Hammer: Leute vertrauen ihrem Computer Informationen an, ohne sich Gedanken zu machen und sind leichtsinnig in den sozialen Netzwerken: Sie posten so viel. In einer modernen Welt kann man sich nicht gegen einen technischen Fortschritt wehren, aber man sollte auch die Verantwortung erkennen. Wir wehren uns nicht, dass wir immer mehr Daten abgeben. Die Politik wirbt zwar mit Sicherheit, aber es bedeutet auch mehr Kontrolle.

■ ***Der Bundestag hat ja nun sogar das Überwachen von Chats erlaubt. Was sagen Sie zu dem Gesetz?***

Hammer: Na klar, wenn es nach unseren Herrschenden ginge, dürfte es bei Twitter & Co. nur noch Katzenbilder, Kuchenrezepte, Lobhudelei und verbales Hacken-Zusammenknallen geben. Ein dicker Skandal! Und wir wählen diese Politiker auch noch, statt ihnen richtig Feuer zu machen. Da muss ich an Bob Dylans Text »Steal a little and they throw you in jail; steal a lot and they make you king« (zu Deutsch: Stiehlst du ein bisschen, werfen sie dich ins Gefängnis, stiehlst du viel, machen sie dich zum König) denken.

ZUR PERSON

Ich bin ein »Geek«

Daniel Hammer, Professor für IT-Sicherheit an der Hochschule Offenburg, lebt seit 2004 in der Ortenau. Der 52-jährige Informatiker kommt aus Berlin und hat seine Leidenschaft zum Beruf gemacht. »Ich bin, was viele als Geek (Computernarr) bezeichnen. Ich möchte mit IT-Sicherheit Studierende für die Herausforderungen in der digitalen Welt sensibilisieren.

Foto:Privat

HINTERGRUND

Zum Studiengang: Unternehmens- und IT-Sicherheit

Die Hochschule Offenburg bietet den Bachelor-Studiengang »Unternehmens- und IT-Sicherheit« (UNITS) seit 2010 an. 35 Anwärter werden jedes Wintersemester angenommen. Es ist ein siebensemestriges Vollzeitstudium mit drei Semestern Grundstudium und vier Semestern Hauptstudium.

In diesem Studiengang müssen die Studenten auch das Fach »Digitale Forensik« belegen. Zu den Schwerpunkten des Studiengangs gehören unter anderem Computer- und Netzwerksicherheit, Zugriffskontrolle und Identity Management, Risikoanalyse, Kryptographie, Sicherheit von Webapplikationen und elektronischem Geldverkehr, Unternehmensorganisation und Personalführung, rechtliche und ethische Grundlagen der IT-Sicherheit, Datenschutz und Überwachung sowie IT-Incident Management für Unternehmen und deren kritische IT-abhängige Strukturen. In Laboren und Projekten geht es darum, dem Hacker nicht nur auf der Spur, sondern einen Schritt voraus zu sein.

Die Studierenden an der Hochschule Offenburg lernen dabei den Computer als Tatwerkzeug in angewandten IT-Einbruchsszenarien kennen und erlernen Methoden und Tools der Computer-Forensik, der Schwachstellenanalys und der Entwicklung von Software für sichere IT-Systeme. Die Studenten können mit dem Abschluss und dem Wissen in der IT-Sicherheitsberatung, in leitender Position für Sicherheit und Management in Unternehmen arbeiten oder auch der Polizei als externe Berater zur Verfügung stehen.

Quelle: Hochschule Offenburg

www.hs-offenburg.de

Kontakt

Antonia Höft
(Mittelbadische Presse)
antonia.hoeft@reiff.de

Christina Dosse
(Hochschule)
0 78 51 / 205 262
christine.dosse@hs-offenburg.de