IT-Forensiker seziert Festplatten

Veröffentlicht am 20.02.2013 | Lesedauer: 4 Minuten

Berlin - Er vergleicht seine Arbeit mit der eines Pathologen an einer Leiche. Doch hat es der IT-Forensiker Karsten Zimmer mit Festplatten und anderen Datenträgern zu tun. Diese verbergen oft viele Informationen.

Handtaschenraub und Körperverletzung sind Karsten Zimmer fremd - wenn der IT-Forensiker ans Werk geht, sind die Verbrechen in Festplatten von Computern versteckt. «Es rufen mich Unternehmen an, die Sicherheitslücken aufdecken wollen, genauso wie Unternehmen, die den Verdacht äußern, dass sie Opfer eines Hackerangriffs geworden sind oder dass Daten von ihnen nach außen gelangen», sagt Zimmer.

Ist ein Vorfall verdächtig, versucht Zimmer, die Spuren auf den entsprechenden Datenträgern nachzuverfolgen. Daten und Hergänge werden rekonstruiert. Die Ergebnisse sollen auch vor Gericht Bestand haben. Dafür arbeitet der 48-Jährige häufig verdeckt in einem Unternehmen. Er probiert die Technik aus und recherchiert, wie das Unternehmen mit Daten umgeht. «Ich muss psychologisch tätig werden, ich muss mich in die Lage des Täters und des Mitarbeiters versetzen.» So bekam er bei einem Fall heraus, wer in einer Firma Kundendaten an einen Wettbewerber weitergab.

Wie ein Ermittler am Tatort gehe er vor, sagt der Informatiker, der zugleich auch Mitglied im Bund Deutscher Kriminalbeamter ist. Doch er arbeitet auch an «toten Objekten». Das ist der Fall, wenn ihn zum Beispiel die Staatsanwaltschaft um eine Auswertung bittet. Dann untersucht Zimmer sichergestellte Festplatten, Handys, Kameras oder Navigationsgeräte.

Die Aufklärung eines Falls kann laut Zimmer Wochen oder sogar Monate dauern. «Jeder Fall ist anders. Wenn ich nach Schema F gehen würde, dann würde ich sehr, sehr schnell Fehler machen», sagt er. Das liege auch an seinem Kundenstamm, der nicht nur Unternehmen umfasse: «Es ruft mich aber auch eine ganze normale Mutter an, wenn ihr Kind Opfer von Facebook-Mobbing-Attacken geworden ist.» Ein ganz anderes Feld war es, als Zimmer herausfand, dass bei einem Trojaner, der Bankdaten ausspähen sollte, Verwaltungen in mehren Ländern betroffen waren.

Untersucht Zimmer Daten zum Beispiel auf einem Laptop, baut er zunächst die Festplatte aus und schließt sie an einen Sicherungsrechner an. Er macht eine Kopie der Festplatte und sucht mit einem speziellen Programm nach Schlüsselworten. «Ich muss konkrete Hinweise haben, sonst ist das

Suchgebiet zu groß», erläutert er. Dabei überprüft der IT-Forensiker unter anderem alte Mails, die Speicherinformationen der Web-Browser oder ermittelt, wer den Laptop wann benutzt hat. Meistens sei seine Arbeit von Erfolg gekrönt: «In der Regel ist es so, dass ich zum Großteil nachweisen kann, wo Daten hingegangen und woher sie gekommen sind.»

Die Computerkriminalität hat nach Einschätzung des Bundes Deutscher Kriminalbeamter eindeutig zugenommen. Die Straftaten würden aber in der polizeilichen Kriminalstatistik nicht erfasst, sobald die dafür genutzten Server in anderen Ländern stünden, kritisiert der stellvertretende Vorsitzende Bernd Carstensen. Zudem sei die Polizei zu wenig mit Experten ausgestattet. «Die Leute, die müssen nicht nur Kriminalisten sein, sondern die brauchen auch für diese Bereiche natürlich das technische Know-How.»

Daneben steigt die Zahl der Angriffe. Der Virenspezialist Kaspersky Lab zählte 2012 über 1,5 Milliarden abgewehrte Attacken über den Webbrowser - ein Plus von fast 60 Prozent. Die Deutsche Telekom (https://www.welt.de/themen/telekom/) analysiert Angriffe aus dem Internet mit einem Frühwarnsystem. Dieses simuliert über digitale Köder Schwachstellen und soll Attacken anziehen. «An einigen Tagen haben wir bis zu 400 000 Angriffe gesehen», sagt Telekom-Vorstandsmitglied Thomas Kremer. «Unsere Experten schätzen, dass etwa 100 000 neue oder modifizierte Schadprogramme pro Tag auftauchen.»

Digitale Forensik (http://dpaq.de/9b3b5)kann man inzwischen als Masterstudiengang studieren. Die Experten werden später genügend zu tun haben, denn das Bewusstsein für Datensicherheit ist laut Zimmer nicht besonders groß. «Die Unternehmen sind zum größten Teil selber daran Schuld, weil die Sicherheitsmechanismen einmal nicht greifen, einmal zu wenig angesetzt sind.» Einer Illusion sollte man sich dennoch nicht hingeben. Zimmer: «Es gibt keine 100-prozentige Sicherheit.»

Infos zum Studiengang Digitale Forensik (http://dpaq.de/9b3b5)

Leitfaden IT-Forensik (http://dpaq.de/3XXKR)

dpa-info.com GmbH