Computerforensik – ein Minenfeld

Computerkriminalität hat viele Gesichter. Die digitale Spurensuche ist ein möglicher Weg zur Wahrheitsfindung. Anhand von Fallbeispielen aus der Praxis erklären zwei Computerforensiker, wo dabei die Stolpersteine liegen.

→ VON CHRISTOPH BAUMGARTNER & JAN ALSENZ

Grundsätzlich hinterlassen alle Aktivitäten am Computer digitale Spuren – sei es in Form von Einträgen in Logfiles, als Signale, als Dateien oder als Dateifragmente in flüchtigen oder permanenten Datenspeichern. Die Krux liegt darin, wer welche Spuren lesen und auswerten darf, ob die Spuren sich noch lesen lassen und ob es sich lohnt, sein Recht einzufordern.

Kein Opfer von Computerkriminalität legt Wert auf Publicity, weil dies das (Firmen-) Image nachhaltig schädigen kann. Es gibt dabei kaum etwas zu gewinnen, aber viel zu verlieren. Aus diesem Grund enden derartige Fälle selten vor Gericht. Die aufsehenerregenden Ereignisse betreffend Informationsdiebstahl und offiziellem Ankauf des digitalen Diebesguts durch einen Rechtsstaat führten zu hitzigen Diskussionen. Das je nach Quelle Ovid oder Machiavelli zugesprochene Zitat «Der Zweck heiligt die Mittel», gilt aber in der Schweiz zumindest aus juristischer Sicht nicht.

Jegliche Auseinandersetzungen im Umfeld eines vermeintlichen Informationsdiebstahls finden im Spannungsfeld «Informationsschutz versus Datenschutz» statt. Vereinfacht ausgedrückt gelten folgende Definitionen: Der Informationsschutz vertritt das Interesse des Arbeitgebers am Schutz der eigenen Geschäftsgeheimnisse, beispielsweise Verfahrenstechniken, Forschungsergebnisse und Kundenbeziehungen. Als Datenschutz wird das Recht des Individuums auf Anerkennung seiner Privatsphäre bezeichnet. Was das dann im konkreten Fall für den Arbeitgeber bedeuten kann, zeigen folgende Beispiele aus unserer Praxis.

FALL 1: DER DATENKLAU

Der CIO eines Industrieunternehmens hegte den Verdacht, dass einer seiner Mitarbeiter seine Position als Systemadministrator ausnutzt, um sein Gehalt mittels Verkauf von Daten an die Konkurrenz aufzubessern. Der CIO beauftragte einen anderen Administrator damit, gezielt nach digitalen Beweisen zu suchen und seinen Kollegen zu überwachen. Ab diesem Zeitpunkt wurde der gesamte Netzwerkverkehr (Datenzugriffe, Mailverkehr und Surfverhalten) des Verdächtigten überwacht. Dabei erhärtete sich der Verdacht des CIO, und der illoyale Administrator wurde fristlos entlassen. Doch wer glaubt, damit habe sich der Fall erledigt, irrt: Der Entlassene zog vor das Arbeitsgericht, dieses entschied auf unlautere Kündigung. Das besagte Unternehmen musste dem Entlassenen mehrere Monatslöhne als Genugtuung nachzahlen und sollte ihn umgehend wieder einstellen. Aufgrund des zerrütteten Arbeitsverhältnisses verzichteten beide Parteien jedoch auf die Wiedereinstellung. Doch, wie kam es zu dieser Entwicklung, obwohl der Beschuldigte seinen Arbeitgeber nachweislich geschädigt hatte?

«Vorschneller Aktivismus spielt sehr oft dem Täter in die Hände»

Christoph Baumgartner

Die Beweise wurden vom Gericht nicht anerkannt, weil diese unerlaubterweise gesammelt wurden. Das Unternehmen hatte es unterlassen, den Verdächtigten im Voraus über seine ab dem Zeitpunkt der Information bevorstehende Überwachung zu informieren. Dieses Vorgehen hat den Nachteil, dass wohl niemand so dumm sein wird, nach dieser offiziellen Information weiterhin fragwürdigen Aktivitäten nachzugehen. Ausserdem dürfen in diesem Fall keine elektronischen Daten verwertet werden, die vor dem Zeitpunkt der Information anfielen.

Eine bessere Lösung ist, die Einführung eines sogenannten Überwachungsreglements, in dem klar beschrieben steht, in welchen Fällen das Unternehmen, auf welcher Stufe, durch wen, für welche Zwecke, welche Daten sammeln und auswerten darf. Die entsprechenden Passagen können auch im IT-Nutzungsreglement festgehalten werden. In jedem Fall müssen die Mitarbeiter das Dokument unterschreiben – zwecks Bestätigung der Zurkenntnisnahme. Besonders erwähnenswert ist auch, dass aus Sicht des Datenschutzes die IT-Anwender vor sich selbst geschützt werden müssen. Es sollen also in erster Linie geeignete technische Massnahmen wie Zugriffskontrollen nach dem Need-to-Know-Prinzip, Virenschutz, Webfilter etc. implementiert werden, welche die geneigten User davon abhalten, vom Arbeitgeber nicht erwünschten Tätigkeiten nachzugehen.

FALL 2: DER GEHACKTE SERVER

Der Inhalt der Website eines Medienunternehmens wurde von Hackern modifiziert. Nachdem das Unternehmen die Manipulation erkannt hatte, spielte der Administrator das Backup der Originalwebsite ein, mit dem Resultat, dass der Inhalt wenige Minuten später erneut verändert wurde. Dieses sogenannte Website Defacement mündete in ein Katz-und-Maus-Spiel. Nach einigen Durchläufen entschied der IT Leiter, den Webserver bis auf Weiteres abzuschalten. Nachdem der Webserver von Malware desinfiziert und gehärtet wurde, konnte er nach knapp vier Stunden wieder ans Netz gehen.

Wie ist in so einer Situation vorzugehen? Als Erstes sollte im laufenden Betrieb das Netzwerkkabel des Webservers ausgesteckt werden. So kann Schadensbegrenzung betrieben werden, um Peinlichkeiten zu vermeiden. Lieber temporär keinen Internetauftritt haben, als den Websiteinhalt nicht kontrollieren zu können und sich im harmlosesten Fall dem Spott Dritter auszusetzen. Falls möglich, kann über ein anderes System auch eine Wartungsmeldung anstelle der Website angezeigt werden. Die Websitebesucher müssen ja nicht zwingend über den wahren Grund der Störung informiert sein. Nun bleibt genug Zeit, die weiteren Schritte zu planen. Gilt es nur, den Normalbetrieb möglichst rasch wiederherzustellen oder soll auch nach dem Urheber gesucht werden? Im zweiten Fall gilt es, möglichst viele Beweise zu sichern. Hierzu sollten ein Speicherabbild erstellt und die Logs von umliegenden Systemen gesichert werden. Zumindest muss jedoch eine Kopie der Festplatte erzeugt werden.

FAZIT: BEWEISE SICHERN

In den meisten Fällen von Computerkriminalität ist es nach guter Beweissicherung möglich, das «Was» und «Wie» zu ermitteln. Das «Wer» erweist sich meistens als deutlich schwieriger. Viele Attacken erfolgen durch Malware, die den infizierten Home-PC eines ahnungslosen Users als Sprungbrett benutzt. Selbst wenn sich dieser im Land befindet, sitzt der wirkliche Angreifer meist im Ausland und missbraucht für seinen Angriff beispielsweise Privat-PCs oder auch die IT-Infrastruktur einer Universität als Brückenkopf. Deren IP-Adressen sind somit wertlos, entsprechend schwer ist es, über den ISP an die Adresse des vermeintlichen Übeltäters zu kommen. Ein guter Hacker versucht zusätzlich, entweder (fast) keine oder falsche Spuren zu hinterlassen, indem er beispielsweise mittels Rootkits oder unter falscher digitaler Identität arbeitet, die Logging-Funktionalität des angegriffenen Systems deaktiviert oder die Logfiles nach vollbrachter Tat löscht. Falls rechtliche Schritte erwogen werden, ist also übertriebener Optimismus fehl am Platz.

Im Bereich Computerforensik drängt sich schnell die Frage der Verhältnismässigkeit auf. Wenn keine zwingenden Gründe für die Strafverfolgung vorliegen, sollte zumindest hinterfragt werden, ob sich der Aufwand lohnt, die eigene Rechtsabteilung oder den Anwalt zu bemühen, um via langwieriger Rechtshilfegesuche zu versuchen, des Täters habhaft zu werden. Derartige Aktivitäten können auch zum Bumerang werden, wenn sich herausstellt, dass das Delikt nur erfolgreich war, weil der Webserver nicht zeitnah gepacht wurde oder die internen Kontrollsysteme versagt haben. Erschwerend kommt hinzu, dass in manchen Ländern zwar die gesetzliche Grundlage für die Strafverfolgung von Computerdelikten besteht, die lokalen Behörden dies aber als Kavaliersdelikte abtun oder bei der Strafverfolgung andere Prioritäten setzen. Manchmal ist es ratsam, die bittere Pille zu schlucken und daraus zu lernen. ←

«Ein guter Hacker hinterlässt entweder fast keine oder falsche Spuren»

Jan Alsenz

Christoph Baumgartner ist CEO und Inhaber der auf IT Strategie und IT Security Consulting spezialisierten OneConsult GmbH. **Jan Alsenz** ist Team Leader Security Audits im selben Unternehmen. Seine Spezialgebiete sind anspruchsvolle Security Audits, Systemanalysen und Reverse Engineering

BILD: FOTOLIA