„Inside Man" - Digitale Beweissicherung

Weltweit wird mehr Geld mit im Verbrechen im digitalen Bereich verdient, als mit Drogenhandel. Die Gründe hierfür sind vielfältig: einerseits laden EDV-Systeme durch ihre mangelnde Absicherung zum digitalen Einbruch ein, andererseits muss man sich „die Finger nicht dreckig machen" und kann von Ferne unbemerkt auf diese System zugreifen. Nicht zuletzt ist die Hemmschwelle für „Gelegenheitskriminelle" geringer, denn alles spielt sich in einer virtuellen Welt ab, nichts ist real, alles nur Daten, Bits und Bytes, Nullen und Einsen, entgegengesetzte magnetische Polarisationen,...

Was ist ein Beweis?

In der Logik wird nach induktiven und deduktiven Beweisen unterschieden, wobei der induktive Beweis, auch empirischer Beweis genannt, aus Beobachtungen und Erfahrungen gewonnen wird während im deduktiven Beweis aus bereits anerkannten Sätzen (Prämissen) durch logische Schlussfolgerungen der zu beweisende Satz gewonnen wird.

„Ein Beweis ist in der Mathematik die als fehlerfrei anerkannte Herleitung der Richtigkeit oder auch Unrichtigkeit einer Aussage" (Wikipedia). Das ist dem ITler am liebsten, wahr und falsch, schwarz und weiß, null und eins…. Doch leider wird es nicht so einfach werden.

Um nicht irgendein Phantom zu jagen, das sich später als Hardwaredefekt oder Schusseligkeit eines schlecht ausgebildeten Mitarbeiters entpuppt, sollten die elementaren Fragen geklärt werden:

Was, wo, wann, wie, wer und warum? Fragen, die die Grundlage einer jeden Beweissicherung bilden.

Was ist geschehen?

Sucht man nach digitalen Beweisen, muss es auch einen handfesten Grund dafür geben. Dies können Auffälligkeiten bei Mitarbeitern, Servern oder PCs sein, aber auch fehlerhafte Buchungen, Konstruktionszeichnungen beim Mitanbieter oder der eigene Prototyp auf dem Messestand nebenan. Formulieren Sie das Vorgefallene sehr genau, denn je genauer die Tat beschrieben wird, desto glaubwürdiger ist sie bei den Strafverfolgungsbehörden.

Dies wird an einem simplen Beispiel deutlich: Rufen Sie bei der Polizei an und teilen dem diensthabenden Beamten mit, dass in ihrer Wohnung der Tresor gewaltsam geöffnet wurde und das Geld fehlt, so ist jedem klar, dass eingebrochen wurde und Vermögenswerte entwendet wurden.

Anders beim digitalen Verbrechen. Auch hier ein Beispiel, das verrückt klingt, jedoch dem Betroffenen einen nicht unerheblichen finanziellen Schaden zugefügt hat: Ein PC-Benutzer spielt oft das Internet-Spiel „Second Life" und hat sich dort viele virtueller Werte erworben, die auch in reale Währung transferiert werden können. Diesem Spieler wird nun seine virtuelle Identität gestohlen und seine virtuellen Werte werden gewinnbringend bei z.B. Ebay versteigert, also in die reale Welt transferiert. Dem Spieler ist faktisch ein Schaden entstanden.... Aber wie erklärt man das schlüssig einem Laien?

Digitale Verbrechen folgen anderen Mustern und sind nicht leicht auszumachen. Relativ leicht zu finden ist die Datenspeicherung von Bildern oder Filmen, die unter das Jugendschutzgesetzt oder Volksverhetzung fallen. In diesen Fällen ist ein Mehr an Daten auf den PCs und Servern zu finden, wenn auch oft gut versteckt. Schwierig ist in diesen Fällen nur das Klassifizieren des Materials. Schwie-

riger wird es, wenn Daten manipuliert wurden. Die Entdeckung erfolg oft mittels „Kommissar Zufall" oder durch gezielte Überwachung von geheimen Daten. Der dritte und schwerste Fall tritt ein, wenn Daten kopiert wurden. Dann liegen die genauen Beweise meist nicht mehr im eigenen Hause.

Wo geschah der Vorfall?
Im eigenen Interesse sollte man sich im Klaren sein, wo der Vorfall im Unternehmen stattfand, bevor ein IT-begeisterter Staatsanwalt erst mal die gesamte IT-Infrastruktur sicherstellt. Je nach Größe des Vorfalls und des Unternehmens empfiehlt es sich, alle involvierten Systeme zweimal zu duplizieren und die Originalfestplatten im Tresor zu verwahren (Grundsatz: NIE das Original anfassen!) oder dem Staatsanwalt zu überlassen, eine Kopie wieder in die Server einbauen und die zweite (und jede weitere) Kopie zur Recherche verwenden. Problematisch bei der Frage nach dem Wo ist, dass es im Unternehmen unzählige Stellen geben kann, um Daten zu verändern, zu kopieren oder zu löschen.
Bei Veränderung oder Löschung ist der Ort des Geschehens relativ leicht zu bestimmen, doch die Beweise, die zum Täter und zur Aufklärung des Vorfalls führen, liegen nicht immer am selben Ort. Zuerst müssen die Beweise gesichert werden, die den Vorgang transparent machen, also aktuelle Festplatte und alte Sicherungen als Beweis für die Manipulation. Danach muss der Weg der Manipulation sichergestellt werden. Dazu benötigt man neben den Zugriffsrechten auf diese Daten auch die Nachweise, wer zugegriffen hat und wann der Zugriff erfolgte. Diese Nachweise können in diversen Protokolldateien, die in dem Netzwerk verteilt sind oder auf NAC-Systemen (Network Access Control) zu finden sein. Auch Firewall-Logs können zur Aufklärung des Sachverhalts nötig sein. Vergessen Sie nicht die (kleinen) externen Speichermedien. Oft werden Daten auf Speichermedien „versteckt", die als erstes garnicht danach aussehen: witzige USB-Sticks, SD-Karten in Fotokameras, mobile Telefonen, PDAs… aber auch CDs und, weil keiner mehr daran denkt, Disketten. Und vergessen Sie die Festplatten in den Druckern nicht!

Das Wie und Warum erfahren Sie in der nächsten Ausgabe und was Sie dagegen tun können.