

## Interviewfragen

### **1 Mit welchen Formen von Computerkriminalität haben Sie in der Praxis besonders häufig zu tun?**

Das Feld der Computerkriminalität ist ein weites. Computerbetrug und Datenspionage rangieren ganz oben in den Statistiken. Computerbetrug umfasst jede Erringung von Vermögensvorteilen durch die Nutzung eines PCs – der PC wird zum Tatwerkzeug. Dazu gehört zum Beispiel die Fälschung von Ertragsberichten bei Finanzfonds. Datenspionage kommt auch sehr häufig vor – die gewünschten Informationen sind ja nur einen Mausklick entfernt. Viele Mitarbeiter auf allen Ebenen nehmen Kundendaten oder ganze Projekte mit, wenn sie das Unternehmen verlassen. Elektronisch gespeicherte Daten sind handliches Diebesgut. Nicht zu unterschätzen ist auch die böswillige Sabotage von Rechnern. Der Fantasie ist dabei keine Grenze gesetzt. Wenn ein Jérôme Kerviel bei seinem Derivat Handel für die Société Générale zum Beispiel Dokumente und E-Mails zu vorgeschriebenen Sicherungsgeschäften fingierte, um interne Controlling-Prozesse zu umgehen und so größere Spekulationsgeschäfte tätigen zu dürfen, ist dies auch eine Verfehlung, die nachweisbar wäre.

### **2 Das Zusenden eines Computervirus erfüllt regelmäßig die Tatbestände der versuchten Computersabotage, der Datenmanipulation und/oder des Ausspärens von Daten. Viele Unternehmen und Privatpersonen haben aber täglich dutzende solcher Schädlinge im Posteingang. Lohnt sich eine Anzeige überhaupt?**

Das ist eine echte Herausforderung, zumal solche Anzeigen nur sehr geringe Erfolgsaussichten haben und vor allen Dingen sehr aufwändig sind, insbesondere wenn die Attacken aus dem Ausland kommen. Dazu müsste mit Hilfe des Providers die Herkunft des Angriffes belegt werden können – was oft kaum möglich ist und wofür viele Behörden auch gar keine Zeit haben. Viele Viren wollen außerdem auch nicht unbedingt einen Schaden im Sinne von Spionage anrichten, sondern eher Rechenkraft für Botnetze kapern oder checken, welches passende Spamangebot man dem Anwender zusendet. Viel gefährlicher und zugleich ungemein schwieriger zu ermitteln sind heutige gezielte Angriffsmethoden mit Malware aus monetären Motiven, die man schon zu organisierter Kriminalität zählen kann.

### **3 Angenommen, ein Datendiebstahl kann auf frischer Tat beobachtet werden. Wie kann das Opfer gleichzeitig die Beweise sichern und einen weiteren Abfluss vertraulicher Daten – etwa**

## **über einen von außen gehackten PC – verhindern?**

Eigentlich haben hier die Schadensbegrenzung und die Beweissicherung Vorrang. Schon ein simples Ausschalten eines Rechners kann Beweise – in Form von Log-Einträgen – vernichten. Anleitungen, die kursieren, zum Beispiel das RAM-Modul tiefzukühlen und Log-Einträge sozusagen einzufrieren, haben eher James-Bond-Charakter als Praxisbezug. Es sei denn, es wird zufällig ein akuter Angriff erkannt, dann heißt es erstens Netzwerkverbindung kappen – also Schaden begrenzen - und zweitens LogFiles, RAM und Cash Daten sichern - also Spuren sichern.

**4 Technisch lässt sich ein Datendiebstahl ja eigentlich nur bis zu dem Rechner zurückverfolgen, an dem er begangen wurde. Gibt es einen rechtssicheren Weg, ihn auch auf eine konkrete Person zurückzuführen? Der Mitarbeiter könnte sich ja sonst darauf zurückziehen, ein anderer habe in seiner Abwesenheit seinen PC manipuliert.**

Welcher Mensch vor der Tastatur war, lässt sich allein mit technischen Mitteln nicht nachweisen. Die gewonnenen Beweise müssen substantiiert werden, d.h. es muss nachgewiesen werden, dass es plausibel ist, dass der Verdächtige XY an diesem Rechner saß und eine Aktion durchgeführt hat oder dass er es gar nicht hat sein können. Ein klassisches Beispiel: Ein Zugriff auf passwortgeschützte Daten erfolgte, als der Inhaber im Urlaub war oder nicht mehr im Betrieb war. Im Grunde sucht man hier nach digitalen Alibis. Anderes Beispiel: Eine E-Mail mit vertraulichen Informationen wurde in falschem Namen von einem anderen Rechner verschickt. So etwas lässt sich dank IP- und MAC-Adressen nachweisen.

**5 Es gibt inzwischen etliche Tools, die ein „sicheres Löschen“ durch mehrfaches Überschreiben der Daten mit Zufallswerten ermöglichen. Haben Sie eine Chance, auch derart vernichtete Beweise zu rekonstruieren, und wenn ja, wie bewerten Gerichte die Glaubwürdigkeit der so gewonnenen Beweise?**

Hier kommt es sehr auf die Überschreibungsmethoden und verwendeten Algorithmen an. Bei entsprechender Sorgfalt lässt sich dann nichts mehr machen, denn Überschreiben mit digitalen Einsen und Nullen heißt zwangsläufig Änderung der magnetischen Informationen. Das ist wie wenn in der realen Kriminalität der Täter seine Fingerabdrücke verwischt. Nur wenn der Täter nachlässig war, bleibt hier etwas übrig. Daten die nicht überschrieben und nur gelöscht wurden und daher zu retten waren, lassen sich glaubwürdig und einwandfrei nachweisen. Generell steigt die Akzeptanz

digitaler Beweismittel in Deutschland immer mehr.

**6 Wenn ein Unternehmer Sie beauftragt, Beweise auf einem möglicherweise kompromittierten Computer zu sichern, ist es immerhin denkbar, dass Sie auch gegen ihn selbst belastendes Material finden (zum Beispiel Geldtransfers an den Steuerbehörden vorbei), und in jedem Fall kommen Sie mit vertraulichen Interna des Unternehmens in Berührung. Welchen Grad von Vertraulichkeit können Sie Ihren Auftraggebern zusichern?**

Absolute Vertraulichkeit – so wissen wir zu jedem Zeitpunkt, wer welche Daten besitzt und bearbeitet und für die Integrität der Daten verantwortlich ist – selbst jede interne Übergabe wird entsprechend protokolliert. Um andererseits nicht zum Auftragstäter zu mutieren, weisen wir zum Beispiel jeden Kunden auf die Beachtung geltender Datenschutzrichtlinien hin, empfehlen den Einbezug von Betriebsrat oder Datenschutzbeauftragten. Des Weiteren muss jeder Auftraggeber bestätigen, dass er rechtlicher Eigentümer der Daten ist und die Ermittlungsergebnisse nur zu rechtlich zugelassenen Zwecken verwendet. Als Computer Forensik- Spezialisten ist es nicht unsere Aufgabe und wir maßen es uns auch nicht an, eventuell entdeckte Geld-Transaktionen zu bewerten. Wir sind keine Finanzexperten, die eine Unterscheidung zwischen legalen und illegalen Überweisungen durchführen sollten. Wir konzentrieren uns in unserer Arbeit absolut neutral auf nachvollziehbare Fakten. Wenn sich Hinweise auf Straftaten wie Kinderpornographie oder konkrete Kapitalverbrechen finden würden, würden wir das oberste Management des Auftraggebers vorab informieren und gegebenenfalls aus ethischen Gründen die Staatsanwaltschaft informieren. Verpflichtet dazu sind wir nicht.

**Reinhold Kern, Director Computer Forensics Kroll Ontrack GmbH Böblingen**