Computer Forensics

Die Informationstechnologien haben heute auf praktisch alle Bereiche unserer Gesellschaft Einfluss. Mittels der zum Teil komplexen Systeme und durch ihre Vernetzung untereinander ergeben sich viele Möglichkeiten, Manipulationen der gespeicherten oder transportierten Daten durchzuführen. Diese Datenzugriffe erfolgen dann nicht immer autorisiert und mit einer guten Absicht.

VON ROGER AUINGER

Gerade in Zeiten, in denen Mitarbeiter Lohnkürzungen, Entlassungen und andere Verluste in Kauf nehmen müssen, ist das Risiko relativ gross, dass sich jemand auf unberechtigte Art und Weise bereichert. Mitarbeiterdelinquenz findet auf allen Hierarchiestufen einer Unternehmung statt. Die Möglichkeiten einen Schaden zu verursachen sind sehr viel zahlreicher, je höher sich eine Person in der Hierarchie befindet. Grundsätzlich müssen aber folgende drei Bedingungen erfüllt sein, dass eine Person überhaupt zum Delinquenten wird. In erster Linie muss die entsprechende Person unter dem nötigen Druck stehen, welche sie zu einer Tat veranlassen würde. In einem zweiten Schritt muss die Person sich selber gegenüber zur Überzeugung gelangen, dass ihr delinquentes Verhalten aus irgendwelchen Gründen für sie gerechtfertigt ist und es dabei eigentlich nur darum geht, sich seinen zustehenden Anteil zu sichern. Als Drittes ist es für das typische Wirtschaftsdelikt notwendig, dass die fehlbare Person sich in gewissem Masse sicher fühlt, nach der strafbaren Handlung nicht überführt zu werden.

Jede Organisation, unabhängig ihrer Zugehörigkeit zur jeweiligen Wirtschaftsklasse, wird sich früher oder später mit der Verhinderung oder der Aufklärung eines Wirtschaftsdeliktes auseinander setzen müssen. Vielerorts fehlt das Bewusstsein, dass jede wirtschaftende Einheit zum Opfer werden könnte. Es ist für jede Institution oder Organisation wichtig, entsprechend ihren individuellen Risiken, angemessene Kontrollen zu implementieren. Mittels Bewusstseinssteigerung und interner Kontrollen kann bereits ein grosser Teil des Gefahrenpotenzials minimiert werden. Das Fehlen dieser beiden Schutzvorkehrungen führt oftmals zu einem immensen finanziellen Verlust, der vielerorts nicht einmal entdeckt wird.

Prävention und rechtliche Aspekte

Für jedes Unternehmen ist es somit sicherlich ratsam, präventiv einmal eine Art Gefährdungsanalyse in den eigenen vier Wänden durchzuführen. Es gibt eine ganze Reihe von Indikatoren, welche Anhaltspunkte für wirtschaftskriminelle Vorfälle sein könnten. So ist es zum Beispiel verdächtig, wenn in der Buchhaltung eine überaus grosse Anzahl von Korrekturbuchungen gemacht werden. Wichtig dabei ist natürlich die Berücksichtigung von unternehmens- und branchenüblichen Vergleichszahlen. Oftmals sind es auch Schlüsselpersonen oder solche Mitarbeiter, die nie in die Ferien gehen, welche vielleicht mit dem nötigen Feingefühl analysiert werden sollten.

Um die Rentabilität eines Unternehmens gleichbleibend zu halten oder zu steigern, ist es daher unter anderem wichtig, präventive Massnahmen zu etablieren, welche das Auftreten von wirtschaftskriminellen Vorfällen verhindern. In einem nächsten Schritt ist es insbesondere bei einem begründeten sowie auch bei einem unbegründeten Verdacht auf eine wirtschaftskriminelle Handlung wichtig, professionell und richtig an die Sache heranzugehen. Oft werden dabei zum Beispiel übergeordnete Rechte, welche der Verdächtige geltend machen könnte, einfach nicht beachtet. In vielen Fällen möchte das Opfer keine Strafanzeige gegen den Täter einreichen, da damit Prozesskosten, Imageverluste oder weitere negative Auswirkungen die Folge sein könnten. Es ist jedoch unerlässlich bei einem Ermittlungsverfahren, ob dies durch interne oder externe Ermittler durchgeführt wird, immer so vorzugehen, dass es jederzeit möglich wäre, bei der zuständigen Stelle eine Strafanzeige einreichen zu können.

Die rechtliche Situation ist nicht immer so, wie es am offensichtlichsten scheint. Aus diesem Grund ist es bei grösseren und komplexen Verdachtsmomenten notwendig, entsprechende juristische Unterstützung beizuziehen.

Ermittlung

Bei der effektiven Durchführung einer Ermittlung gibt es neben den rechtlichen Stolpersteinen auch eine Menge von Verfahrensfehlern, die begangen werden könnten. Vor allem sind die ersten Schritte nach einem so genannten Meldungseingang entscheidend, ob es zu einem späteren Zeitpunkt vielleicht möglich sein wird, einen Teil der abgeflossenen Vermögenswerte wieder rückführen zu können. Es ist darum hilfreich, wenn sich ein Unternehmen bereits einmal Gedanken gemacht hat, wer intern entsprechend involviert werden sollte oder mit wem eine externe Zusammenarbeit überhaupt in Frage kommen könnte. Je nach Tragweite des Falles ist vielleicht eine Information der Presse unabdingbar. Eine offene Kommunikation von begangenen Fehlern nimmt der Presse oftmals den Wind aus den Segeln. Es gibt nichts Rufschädigenderes als ein andauernder Skandal mit immer wieder neuen Schlagzeilen, welche die Gerüchteküche nur so brodeln lassen.

Verdachtsmomente lediglich mit unüberlegten Sofortmassnahmen gegenübertreten zu wollen, ist eine aussichtslose Angelegenheit, die so schnell endet wie sie begonnen hat. Es ist wichtig, sich alle verfügbaren Fakten, Hilfsmittel und Ressourcen zu Hilfe zu nehmen, um so die Chancen auf einen Ermittlungserfolg nicht von Beginn weg zu minimieren.

Beweismittelsicherung

Oftmals liegt einem Delikt als Tatwerkzeug eine Informationstechnologie zugrunde. Überall dort, wo dies der Fall ist, hinterlassen Daten verarbeitende Systeme Spuren, welche in Kombination einen wesentlichen Teil zur Aufdeckung eines Deliktes beitragen können. Insbesondere im computerkriminellen Umfeld ist es essenziell, auf technische Fachspezialisten zurückgreifen zu können, welche elektronische Beweise so sichern, dass sie beispielsweise gerichtlich verwertbar sind. Es besteht die latente Gefahr, dass die Beweismittel zu einem späteren Zeitpunkt nicht mehr korrekt gesichert werden können, da sie inzwischen verloren gegangen sind, als ein Beispiel dafür sind knappe Backup-Zyklen zu nennen.

Die Gewährung der Integrität sichergestellter Daten muss dabei, sofern möglich, bedingungslos eingehalten werden. Diese Integrität der Daten wird durch den Einsatz einer forensischen Software garantiert, welche von den sichergestellten Datenträgern mittels eines speziellen

Roger Auinger
ist Leiter der Arbeitsgruppe «Forensics» der Fachgruppe Security (FGSec) und Geschäftsführer der adverum ag in Zollikon ZH (roger.auinger@adverum.ch).

Verfahrens ein identisches Abbild (Image) erstellt, ohne dabei Originaldaten zu verändern. Bei der Sicherstellung elektronischer Informationen ist es von Vorteil, Experten und unternehmensinterne Personen als Zeugen für die korrekte Abwicklung der Beweissicherung beizuziehen.

Auch Spezialisten von Ermittlungsbehörden stehen immer wieder neuen Herausforderungen gegenüber. Ein Beispiel dafür ist: Ein PC soll in einem Büro beschlagnahmt werden. Der Türrahmen zum Raum, in welchem der entsprechende PC steht, wird mit einem starken Magnetfeld gespiesen. Falls der erwähnte PC durch dieses Magnetfeld zur Türe hinaus getragen wird, besteht die Gefahr, dass Daten auf der Festplatte dieses PCs unleserlich gemacht werden. Durch den Transport der Harddisk in einem Faradayschen Käfig könnte diese vor der Wirkung des Magnetfeldes geschützt werden.

Insbesondere neue Technologien setzen veränderte Vorgehensweisen bei der Beweismittelsicherung voraus. So haben heutzutage viele Laptop-Modelle bereits eine integrierte WLAN-Karte (Wireless LAN), die drahtlose Netzwerkverbindungen bis zu 150 Metern ermöglicht. Straftäter können also mit ihrem Laptop in den eigenen Räumlichkeiten arbeiten, aber ihre verbrecherischen Daten auf einem PC lagern, der beim Nachbarn auf der gegenüberliegenden Strassenseite im Keller steht. Prüfen die Ermittlungsbehörden bei der Beschlagnahmung vor Ort nicht das Vorhandensein eines drahtlosen Netzwerkes, werden sie nie auf die gewünschten Beweismittel stossen. Perfid wird die Situation, wenn ein Straftäter sich über den ungesicherten Wireless-Internetzugang seines Nachbarn strafrechtlich relevanten Inhalt aus dem Internet herunterlädt und diesen Inhalt auf der Festplatte des ungesicherten PCs des nichtsahnenden Nachbarn speichert.

Abschluss

Nach Beendigung der Ermittlungen ist ein Fall für ein Unternehmen noch nicht abgeschlossen. Was anschliessend an die Ermittlungsarbeiten, unabhängig des Ermittlungserfolges, notwendig ist, ist die entsprechenden Lehren zu ziehen. Das Ziel dieser Nachbearbeitung ist es, die Gründe für den Vorfall zu analysieren. Zu diesem Zweck soll erörtert werden, mit welchen effektiven Massnahmen der Vorfall hätte verhindert werden können. Hierbei ist es wichtig, die Wirksamkeit des allfällig vorhandenen internen Kontrollsystems zu verifizieren. Dabei wird in einem ersten Schritt analysiert, welche internen Kontrollen überhaupt existieren.

Anschliessend wird in einem zweiten Schritt geprüft, bei welchen Ausnahmen die internen Kontrollen nicht greifen. Aus diesen Erkenntnissen der Nachbearbeitung sollte ein Massnahmenkatalog entstehen, der unter anderem auch eine Neugestaltung einzelner Prozesse beinhalten kann. Schliesslich stellt sich für jedes Unternehmen aber die Frage: «Können die bestehenden Risiken, welche zu diesem Vorfall geführt haben, mit vertretbarem Aufwand eliminiert oder verringert werden oder sollen die bestehenden Risiken akzeptiert werden?»

Konklusion und Ausblick

Jedes Unternehmen, welches effektive Kontrollen gegen Computerkriminalität und somit auch gegen Wirtschaftskriminalität etabliert, steigert die eigene Rentabilität und trägt indirekt zu einem grösseren Wirtschaftswachstum bei. Werden diese Kontrollen intern sowie extern kommuniziert, erhöht dies die Hemmschwelle für angehende Delinquenten und trägt zu einem positiven Image bei, was in beiden Fällen eine positive finanzielle Entwicklung zur Folge haben kann. Solche und ähnliche Fragestellungen bearbeitet der Autor mit der adverum ag und seit zirka zwei Jahren mit einer interdisziplinären Arbeitsgruppe, der Fachgruppe Security (Schweizerische Informatikergesellschaft), mit dem Namen «Forensics», welche an der Orbit/Comdex ihren Leitfaden zum Thema «Computer Forensics» herausbringen wird. Während zwei «Tracks» werden dabei die erarbeiteten Resultate vorgestellt. An die Teilnehmer dieser beiden Sessionen wird die herausgebrachte Publikation abgegeben.

Sowohl für KMUs als auch für grosse Unternehmen ist dieser auf schweizerische Verhältnisse angepasste Leitfaden ein guter Einstieg, welcher die notwendigen Schritte bei computerforensischen Untersuchungen aufzeigt. ■