IT- & DATENSICHERHEIT

Digitalen Angreifern auf der Spur

Immer mehr Unternehmen werden Opfer von Hackerangriffen. Das ruft neue Kriminaltechniken wie die digitale Forensik auf den Plan.

Von Rico Schubert

Forensische Methoden kommen inzwischen auch in der digitalen Welt zum Einsatz.

Foto: WavebreakMediaMicro - stock.adobe.com

REGENSBURG. IT-Systeme von Unternehmen sind heute häufig das Ziel von Angriffen. Meldungen über Tausende Kunden- oder Millionen von Kreditkartendaten, die gestohlen wurden, sind keine Seltenheit. Dabei droht die Gefahr nicht nur von außen. Immer häufiger werden Unternehmen auch durch eigene Mitarbeiter gezielt angegriffen. Dazu zählen der Diebstahl von Daten oder die Sabotage von Anlagen. Bei solchen digitalen Angriffen werden die Kontroll- und Schutzmechanismen in den IT-Systemen gezielt umgangen oder sogar geschickt genutzt.

Täter hinterlassen Spuren

Dr. Stefan Meier, wissenschaftlicher Mitarbeiter an der Universität Regensburg und Inhaber der Meier Computersysteme GmbH, hat sich in seiner Dissertation mit der Methodik forensischer Untersuchungen in Unternehmen beschäftigt. „Die digitale Forensik sichtet und analysiert digitale Spuren in IT-Systemen mit dem Ziel, Tatbestände und etwaige Täter festzustellen und digitale Beweismittel und Analyseschritte gerichtsfest aufzubereiten, das heißt, sie so darzustellen, dass sie den strengen Anforderungen von Gerichten an Beweismittel genügen", erklärt Meier. So können etwa mithilfe der Methoden und Softwarewerkzeuge aus der digitalen Forensik Festplatten analysiert werden, um etwa herauszufinden, ob ein bestimmter Computer eine bestimmte Tathandlung wie den Download einer illegalen Datei oder die Weitergabe interner Dokumente eines Unternehmens ausgeführt hat. „Das ist Aufgabe der Forensik: Ich weiß, wie Dinge funktionieren und kann die Aktionen nachvollziehen – die Anmeldung am Rechner, die Browservorgänge, das Umkopieren von Daten et cetera. Wenn es zum Beispiel in Unternehmen einen unberechtigten Datenabfluss gibt, schaut man sich an, welche USB-Sticks angeschlossen waren, auf welche Netzlaufwerke der Nutzer Zugriff hatte, welche Dateien von A nach B kopiert wurden. Das kann man alles nachvollziehen. So lassen sich viele Aktionen rekonstruieren", sagt Meier. „Vor Gericht geht es beispielsweise darum, zu belegen, dass Logdaten nicht im Nachhinein verändert worden sind", erklärt Prof. Dr. Günther Pernul, der Inhaber des Lehrstuhls für Informatik an der Universität Regensburg. Dazu werden diese Daten mit einem Zeitstempel versehen und versiegelt – damit sind sie „gerichtsfest".

KMU sind beliebte Ziele

Das Thema ist auch für kleine und mittlere Unternehmen (KMU) in der Region bedeutsam. Sie verfügen über hohe Spezialkenntnisse und -fähigkeiten, die durch aufwendige Entwicklungsarbeit erworben wurden. Daneben sind sie häufig als Zulieferer fest in die Lieferketten von Großkonzernen integriert und können somit als Einfallstor dienen, um an deren Geschäftsgeheimnisse zu gelangen.

Trotz der bekannten Gefahren befassen sich viele Unternehmen bislang kaum mit der systematischen Untersuchung digitaler Angriffe auf ihre IT-Systeme – dies hat Meier in seiner Bestandsaufnahme dargelegt. Dabei gibt es mittlerweile dazu einen eigenen Forschungsbereich in der digitalen Forensik, der genau diese Frage untersucht. So kann zum Beispiel mithilfe forensischer Methoden nachgewiesen werden, dass statt der vermuteten 20 000 tatsächlich nur 1000 Datensätze abhandengekommen sind. „Das ist schon ein großer Unterschied, wie viele Kreditkarten die Firma ersetzen muss. Und sicher auch ein finanzieller Anreiz, in die digitale Forensik zu investieren, um im Ernstfall herauszufinden, wie groß der Schaden tatsächlich ist", erläutert Meier.

Ein weiteres Ergebnis seiner Beschäftigung mit dem Thema ist die Erkenntnis, dass die soziotechnische Natur der Systeme in der bisherigen Praxis digitaler Forensik zu wenig beachtet wurde – schließlich sind es Menschen, die mit Computern interagieren. Außerdem hat Meier an Fallbeispielen dargelegt, dass die Prozesse eine zentrale Rolle spielen, mit denen Unternehmen sowohl die reguläre Entstehung von Daten als auch das Zusammenspiel und die Beziehungen zwischen Menschen und den Computersystemen definieren.

Notwendigkeit steigt

Die genannten Fallbeispiele konnten „gelöst" werden. Doch wie sieht es in der realen Welt aus? Die Strafverfolgungsbehörden sind mittlerweile sehr gut ausgestattet, es gibt Spezialeinheiten in den Polizeidirektionen, auch die Landeskriminalämter und das Bundeskriminalamt haben entsprechende Abteilungen. „Wenn man heute mit dem Handy zur Polizei geht, können Spezialisten vieles herausfinden", sagt Meier.

Doch in Zeiten von Industrie 4.0 oder Cloud-Computing werden digitale Spuren sowie Methoden und Werkzeuge zu ihrer Auswertung immer wichtiger. Seit etwa zehn Jahren steigt die Zahl der Veröffentlichungen auf diesem Gebiet, sagt Meier. Auch an der Universität Regensburg gibt es das Forschungsprojekt „Dingfest" unter Leitung von Günther Pernul, das sich mit der „Detektion, Visualisierung und forensischen Aufbereitung von Sicherheitsvorfällen" beschäftigt.

INTERVIEW

Gespräch mit Dr. Stefan Meier, wissenschaftlicher Mitarbeiter am Lehrstuhl für Wirtschaftsinformatik I an der Universität Regensburg

Die Unternehmen brauchen eine digitale Polizei

Cyberkriminalität und digitale Forensik sind zwei aktuelle Schlagworte in der IT. Was ist darunter zu verstehen?

Dr. Stefan Meier: Cyberkriminalität bezeichnet grundsätzlich das Tun eines Menschen, der mit Computersystemen arbeitet und dabei etwas Kriminelles macht. Das betrifft nicht nur Mitarbeiter im Unternehmen, denn Malwarekampagnen können auch Privatanwender treffen. Unter dem Schlagwort Cyberkriminalität wird untersucht, wie man sich gegen solche Angriffe verteidigen kann. Es geht eher um präventive Maßnahmen und nicht um das Aufarbeiten eines Verbrechens, wenn es bereits geschehen ist. Das ist der entscheidende Unterschied zur digitalen Forensik. In der Forensik geht es ausschließlich um die Aufklärung von Verbrechen.

Also digitale Polizeiarbeit?

Genau. In der digitalen Forensik muss erst ein Verbrechen passiert sein, ehe der Forensiker mit wissenschaftlich fundierten Methoden aufklären kann. Das kann man sich wie in der Ballistik oder bei einer DNA-Analyse vorstellen. Man versucht, in der digitalen Forensik heute das methodische Vorgehen, wie es aus den klassischen forensischen Wissenschaften bekannt ist, ins Digitale zu tragen.

Dr. Stefan Meier
Lehrstuhl für Wirtschaftsinformatik, Universität Regensburg

Wie geht man dann vor? Kann man aus der Festplatte auch nachträglich noch etwas herauslesen oder geht es um digitale Dokumente oder falsche Identitäten?

Der Forensiker ist glücklich, wenn er auf Logdateien zurückgreifen kann. Auf die physische Welt übertragen sind die Logs wie Videoaufzeichnungen. Hat man eine, hat man einen besseren Ausgangspunkt, um Verbrechen aufzuklären. Aber man kann auch auf einer Festplatte anhand charakteristischer Spuren herausfinden, welcher USB-Stick wann zum Beispiel am Computer war. Bei allen Vorgängen, die auf einem modernen Computersystem ablaufen, werden Daten erzeugt. Man weiß, wie der Browser funktioniert, um die Historie zu speichern. Diese Historie kann man auslesen, um herauszufinden, auf welchen Webseiten sich ein Computernutzer bewegt hat. Manche Dokumente führen intern selbst Buch, was mit ihnen passiert ist. Natürlich ist das alles sehr programm- und plattformabhängig. Aber generell ist es möglich, vieles im Nachhinein herauszufinden: Welche Dokumente wurden erstellt und wann, wer hat ein Dokument wann bearbeitet, auf welchen Speicherorten wurde es wann gesichert? Das ist Aufgabe der Forensik: Ein Forensiker weiß, wie Dinge funktionieren und welche Daten wann erzeugt werden und kann darauf aufbauend die Aktionen nachvollziehen.

Nutzt man spezielle Software dafür?

Ja. Aber das ist immer fallspezifisch. Derzeit gibt es drei, vier relevante Hersteller von Standardsoftware für die klassische Computerforensik. Deren Programme können gut darstellen, was der Benutzer wann gemacht hat. In anderen Bereichen muss man die Tools selbst herstellen. Denn aufgrund der Tatsache, dass es so viele unterschiedliche Systeme gibt, gibt es natürlich keine Standardsoftware für jedes System.

Wie ist das bei Unternehmen?

Fast noch wichtiger als die eingesetzte Software sind in Unternehmen die organisatorischen Prozesse. Hier kann man viel falsch machen, gerade wenn es ums Meldewesen geht. Stellen Sie sich vor, der Mitarbeiter stellt fest, dass irgendetwas im Gange ist. Wen informiert er? Den Chef, die IT oder doch gleich die Polizei? Für den Mitarbeiter ist wichtig, zu wissen, wie er sich richtig verhält. Ein Beispiel aus den USA: Ein Mitarbeiter hat dort auf Firmenservern Kinderpornografie gefunden und wurde später aufgrund dieser Anzeige sofort entlassen. Er musste beweisen, dass er nicht für die Daten verantwortlich ist – eine sehr unglückliche Situation für den Administrator. Daher muss das im Vorfeld geklärt werden, was der Mitarbeiter in einem solchen Fall tun soll.

Wie wird sich diese neue Wissenschaft weiterentwickeln?

Die Firmen und die Strafverfolgungsbehörden merken, dass bei Verbrechen immer häufiger das Tatwerkzeug Computer im Spiel ist – etwa beim klassischen Betrugsfall oder beim Kreditkartenbetrug. Aber auch bei Verbrechen wie Mord und Totschlag gibt es digitale Spuren. Mittlerweile hat fast jeder ein Smartphone, eine Smartwatch oder ein Navigationssystem im Auto, das automatisch Daten aufzeichnet. Diese digitalen Spuren können dann kriminalistisch verwertet werden. Ich denke daher, dass die digitale Forensik grundsätzlich immer wichtiger werden wird. Es werden mehr Leute in dem Bereich arbeiten, da immer mehr Daten anfallen, die ausgewertet werden müssen. Auch für Firmen wird es immer wichtiger, da die digitalen Spuren zunehmen. Schon heute bauen größere Firmen eigene Response-Teams auf, sozusagen als erste Eingreiftruppe, wenn etwas passiert. In diesen Teams arbeiten Experten, die dann die Spuren sichern können. Daneben gibt es spezielle Dienstleister. Insgesamt ist das ein Zukunftsthema.

Interview: Rico Schubert
Foto: Louisa Knobloch/Archiv