Wissenschaftler der Universität Regensburg auf den Spuren von IT-Angriffen

Digitale Forensik in Unternehmen

Stefan Meier, wissenschaftlicher Mitarbeiter am Lehrstuhl für Wirtschaftsinformatik I an der Universität Regensburg, hat die Problematik digitaler Angriffe auf Unternehmen erforscht. Der Regensburger Wirtschaftsinformatiker erstellt eine Bestandsaufnahme der digitalen Forensik als junger Wissenschaft und stellt zugleich die Methodik IT-forensischer Untersuchungen in Unternehmen vor. Die Ergebnisse seiner Arbeit sind ein wichtiger Beitrag zur Grundlagenforschung in der Wirtschaftsinformatik und bieten Einblicke und Anwendungsbeispiele in die aktuell vieldiskutierte Thematik digitaler Angriffe. Zugleich schließen sie eine Lücke in der bisherigen Forschung.

Hintergrund: IT-Systeme von Unternehmen sind heute oft Ziel von digitalen Angriffen. Die Angriffe beschränken sich nicht nur auf Attacken externer Angreifer, sondern es gibt auch eine zunehmende Zahl von gezielten Angriffen durch die eigenen Mitarbeiter eines Unternehmens oder durch Mitarbeiter von Dritten, wie zum Beispiel Dienstleistern und Partnerunternehmen.

Unter diesen Angriffen sind „klassische" Angriffe wie Datendiebstahl oder Sabotage von Anlagen, aber auch immer wieder Handlungen aus dem Bereich der Wirtschaftskriminalität. Bei solchen digitalen Angriffen auf Unternehmen werden die Kontroll- und Schutzmechanismen in den IT-Systemen oft gezielt umgangen oder sogar geschickt genutzt. Ziel des Angriffes ist in den meisten Fällen, Geld auf eigene Konten zu transferieren.

Solche Betrugshandlungen kommen selten ans Licht, vielfach werden diese nur durch Zufall oder bei der Prüfung der Buchhaltung entdeckt. Sobald eine Betrugshandlung oder ein digitaler Angriff jedoch offenkundig ist, werden Methoden aus der digitalen Forensik angewandt, um die Tatbestände detailliert zu untersuchen. Ein typisches Beispiel für die Nutzung der Methoden und Softwarewerkzeuge aus der digitalen Forensik ist die Analyse von Festplatten aus Computern, anhand derer geprüft werden kann, ob mit dem Computer eine bestimmte Tathandlung wie der Download einer illegalen Datei oder die Weitergabe interner Dokumente eines Unternehmens ausgeführt wurde.

IT-Systeme von Firmen sind oft Ziel von digitalen Angriffen. FOTO DPA

Stefan Meier hat in seiner Bestandsaufnahme von digitaler Forensik in Unternehmen herausgefunden, dass sich viele Unternehmen bislang kaum mit der systematischen Untersuchung von digitalen Angriffen auf ihr Unternehmen befassen. Wie seine Untersuchung ergab, ist einer der Gründe dafür, dass es zu wenige etablierte Best Practices auf dem Gebiet der digitalen Forensik gibt.

Grundlage für künftige Software-Werkzeuge

Ein weiterer Grund liegt darin, dass die soziotechnische Natur der Systeme – die Tatsache, dass es Menschen sind, die mit den Computern interagieren – in der bisherigen Praxis digitaler Forensik zu wenig Beachtung fand. Um die bestehende Forschungslücke zu schließen, hat Meier eine Methodik entwickelt, mit der digitale Spuren aus den IT-Systemen von Unternehmen unter Berücksichtigung ihrer soziotechnischen Natur digital-forensisch verarbeitet werden können.

Ein zentrales Element spielen dabei die Prozesse der Unternehmen, die sowohl die reguläre Entstehung von Daten definieren als auch das Zusammenspiel und die Beziehungen zwischen Menschen und den Computersystemen festlegen. In zwei Fallstudien hat Dr. Meier die neue Methodik auf ihre Praxistauglichkeit hin überprüft: In beiden untersuchten Fällen konnten die den Betrugshandlungen zugrunde liegenden Prozesse digital nachverfolgt und somit die Ausführung bewiesen werden.

Die Evaluation der Methode offenbarte jedoch auch, dass aktuell ein großer Bedarf an weiterer Forschungs- und Entwicklungstätigkeit auf dem Feld der digitalen Forensik besteht: „Die IT-Systeme von Unternehmen sind oft sehr komplex. Beispielsweise werden Bestellungen aus Onlineshops direkt in Produktionssysteme übertragen und nach der Produktion vollständig automatisiert versendet. Die dabei entstehenden digitalen Spuren lassen sich nur über geeignete Softwarewerkzeuge sichern und verwerten. Solche Softwarewerkzeuge gibt es aber bislang nicht", erläutert Meier den Stand der Forschung. Die Ergebnisse der Forschungsarbeit liefern wichtige Grundlagen zur Entwicklung zukünftiger Software-Werkzeuge, mit deren Hilfe die hochkomplexen heutigen IT-Systeme von Unternehmen untersucht werden können. > CLAUDIA KULKE

Wel
eine
beei

Wer
tion ein
will, so
möglic
Augen
legte W
Fähigk
identifi
bereits
baren S
schen,
nen rei
rückgre
als and
scheidu

Nein
Bayreu
schaftle
fördern
Fähigk
prozess
Handlu
tieren.
sind hi
dann, v
den, ihr
relevan
und ur
nehmer
die Qu
tracht g
gern ur
treffen,
langen
müssen

Die S
mit mit
den an
ner
School
aufgefo
schaftli
der En
Origina
möglicl
len. In e

Deutsches Rechtssystem soll in Ukraine bekannt werden

Augsburger Juristen helfen bei Fakultätsaufbau an Uni Kiew

Wie Diabetes kleine Herz-Blutgefäße schädigt und so das Infarkt-Risiko erhöht

Verschwindende Äderchen