Jens Nedon, Sandra Frings, Oliver Göbel (Hrsg.)

IT-Incident Management & IT-Forensics

Erste Tagung der Fachgruppe SIDAR der Gesellschaft für Informatik

24. – 25. November 2003 in Stuttgart, Deutschland

Gesellschaft für Informatik 2003

Lecture Notes in Informatics (LNI) - Proceedings
Series of the Gesellschaft für Informatik (GI)

Volume P-39

ISBN 3-88579-368-7
ISSN 1617-5468

Volume Editors
Jens Nedon
ConSecur GmbH
Schulze-Delitzsch-Strasse 2, D-49716 Meppen
Nedon@consecur.de
Sandra Frings
Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO
Nobelstraße 12, D-70569 Stuttgart
Sandra.Frings@iao.fhg.de
Oliver Göbel
RUS-CERT (Universität Stuttgart)
Breitscheidstr. 2, D-70174 Stuttgart
Goebel@CERT.Uni-Stuttgart.DE

printed by Köllen Druck+Verlag GmbH, Bonn

Elektronische Beweise!

Reinhold Kern

Kroll Ontrack GmbH
Hanns-Klemm-Straße 5
D-71034 Böblingen
rkern@ontrack.de

Abstract: Wenn 10 Aktenordner aus einem Regal fehlen, fällt das sofort auf. Was ist aber, wenn Computerdaten kopiert, gestohlen oder manipuliert wurden? „Nur 1,6% aller Wirtschaftsdelikte sind Computerdelikte, die“, so Bundesinnenminister Otto Schily, „aber 60% des gesamten Wirtschaftsschadens ausmachen“.

Ob in der Chefetage, im Büro oder in der Lagerhalle: Veruntreuungsschäden gibt es in allen Ebenen. Steigende Anonymität und die verbreitete Angst vor Jobverlust lassen zudem die Hemmschwelle bei kriminellen Aktivitäten sinken. Die Bandbreite der Mitarbeiterkriminalität ist weit gefächert: Datendiebstahl und –missbrauch, Insider-Geschäfte, Spionage, Korruption, Erpressung, u.v.m.. Auch die neueste BKA Statistik 2001/2002 (www.BKA.de) bestätigt einen Anstieg von über 50% bei betrügerischen Delikten mittels Computer.

Kalkulationen, Business-Pläne, Verträge und Vereinbarungen werden heutzutage am PC erstellt, elektronisch versandt und gespeichert. Email ist heute zum Kommunikationsmedium Nummer 1 in allen Unternehmen avanciert. Mehr als 90 Prozent aller Dokumente werden am PC erstellt, aber über 70 Prozent hiervon wurden niemals ausgedruckt.

Firmencomputer nehmen daher eine Schlüsselstellung in der Wirtschaftkriminalität ein. Die Computer Forensik bietet die Chance, einem Anfangsverdacht nachzugehen und Ermittlungen zielgerichtet zu führen. Auch wenn zunächst der Schutz des Unternehmens und nicht die Strafverfolgung im Vordergrund steht, müssen Indizien und Verdachtsmomente so erhoben werden, dass Sie eine strafgerichtliche Verfolgung nicht behindern oder gar ausschließen. Dieser Wunsch macht die Computer Forensik nicht nur zu einer sensiblen Schnittstelle zwischen Unternehmen und Justiz, sondern auch zu einem Thema für Spezialisten der Datenwiederherstellung und Ermittlung.

Jährlich investieren wir ca. 10 Millionen US $ in die kontinuierliche Weiterbildung unserer weltweit über 400 Mitarbeiter und in die Weiterentwicklung unserer Technologien, damit Ihre Mandanten den Herausforderungen moderner krimineller Aktivitäten entgegentreten können.

Mit dem Vortrag möchten wir sowohl auf die technischen Möglichkeiten als auch auf die Bedeutung elektronischer Beweise hinweisen.

Vortragsinhalte

- Voraussetzungen (Forensik Readiness)
  - Bewusstsein für Risiken und Haftung
  - Unternehmenspolicies, Datenschutzgesetze
  - Empfehlungen der EU Kommission - CTOSE
- Fallbeispiele
- Computer Forensik Prozess
  - Wie sind Daten gespeichert
    - Was bedeutet Daten Löschen oder Formatieren
    - Was sind Log–Files – elektronische Spuren
    - Wo sind die elektronischen Fingerabdrücke
  - Erfassung aller relevanten Daten
    - Images der Festplatten
    - Kopien von Backup Bändern
    - Handheld PCs, Wechselspeichermedien, USB Sticks
    - Mobile Telefone
  - Wiederherstellung gelöschter Dateien
  - Filterung, Sortierung und Analyse der gesamten Daten
    - Schlagwörter, Zeitraum, Personen
    - Analyse der Aktivitäten
  - Berichterstellung und Dokumentation
  - Expertenzeuge vor Gericht