

WAS IST IT-FORENSIK

Durch den Einsatz wissenschaftlicher Methoden zur gerichtsfesten Sicherung, Sammlung, Überprüfung, Identifikation, Analyse, Interpretation und Dokumentation von digitalen Spuren kann die IT-Forensik maßgeblich zur Wahrheitsfindung und zur Aufklärung von Straftaten beitragen.

Als digitale Spuren werden jegliche Formen von Daten bezeichnet, die mit Hilfe von Computersystemen gespeichert oder übertragen werden und ein belastendes oder entlastendes Indiz für die Durchführung einer Straftat darstellen. Sie können beispielsweise Informationen zu Besitz oder Weitergabe von Daten, finanziellen Transaktionen, Kommunikationspartnern, Nutzung von E-Mail- oder Chat-Programmen sowie sonstigen Auffälligkeiten liefern.

In der IT-Forensik kann die digitale Spurensuche auf jedem Gerät stattfinden, welches über einen integrierten elektronischen Speicher verfügt. Die Herausforderung für IT-Forensik-Labore besteht darin, mit unzähligen Varianten an mobilen Geräten, Speichermedien und Betriebssystemen umzugehen, die immer größer werdenden Datenmengen zu verarbeiten, darunter potenziell relevante, digitale Spuren zu finden und diese richtig zu interpretieren.

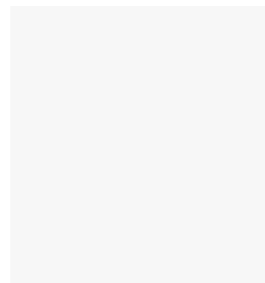
Die Erfassung und Dokumentation festgestellter Spuren findet in den gerichtsfesten Gutachten von Janotta & Partner unter Berücksichtigung geltender Gesetze statt.

Fundierte Systemkenntnisse unserer Mitarbeiter, der Einsatz von Spezialsoftware, moderne technische Ausrüstung sowie langjährig erprobte und optimierte Prozesse machen Janotta und Partner zum Experten auf dem Gebiet der IT Forensik.

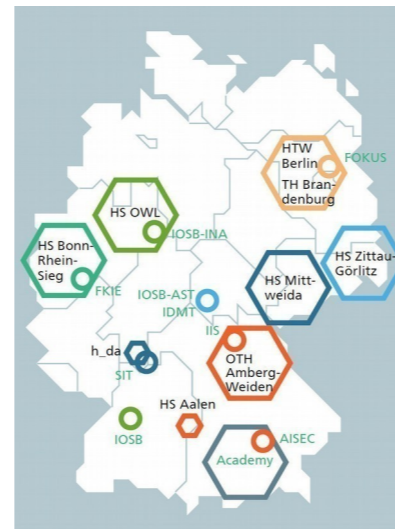
WIRTSCHAFTSKRIMINALITÄT

So gut wie keine Straftat aus dem Bereich Wirtschaftskriminalität kann ohne die Unterstützung von EDV-Systemen begangen werden. Dies bedeutet, dass bei der Aufklärung von Wirtschaftsstraftaten IT-Systeme fast immer wertvolle Informationen beinhalten. Relevante Informationsquellen können beispielsweise folgende IT-Systeme sein:

- CRM- und ERP-Systeme
- Buchhaltungssysteme
- Kommunikationssysteme, wie E-Mail, Chat etc.
- Dokumente in analoger oder digitaler Form



Kontakt:
Janotta & Partner
Adrian Janotta CEO
Breslaustrasse 28
97424 Schweinfurt bei Würzburg
Tel.: +49 (9721) 370 38 17
E-Mail: info@janotta-partner.de



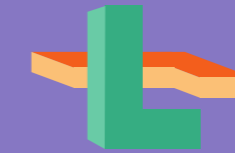
Janotta und Partner
Cybersecurity



Janotta & Partner
Cybersicherheit für Unternehmen

IT-FORENSIK CYBERSICHERHEIT

Ausgabe MAI 2017



IT-FORENSIK
WIRTSCHAFTSKRIMINALITÄT

SCHULUNGEN

Was ist mit IT-FORENSIK möglich?

Prinzipiell lassen sich alle Arten digitaler Speicher mit den Methoden der IT-Forensik auswerten.

- Der Arbeitsspeicher im laufenden Rechnerbetrieb
- In Rechnern eingebaute, sowie externe Festplatten einschließlich komplexer und proprietärer RAID Verbundsysteme
- Netzwerkkomponenten wie Router und Firewalls
- Mobiltelefone, Smartphones, Tablets und Navigationsgeräte
- Digitale Kameras und Videokameras
- Speicherkarten und USB-Sticks sowie optische Speichermedien wie CDs oder DVDs
- Magnetbänder mit Datensicherungen
- Rechnerbasierte Telefonanlage

Bei auszuwertenden Daten wird zwischen vom Nutzer verwalteten Daten und Spuren der Rechnernutzung unterschieden.

Vom Nutzer verwaltete Daten können bspw. Dokumente, Bild- und Videodateien oder gespeicherte Kommunikationsdaten wie E-Mails, Chat und SMS-Nachrichten sein. Im Unternehmensbereich zählen hierzu auch Datenbanken und Anwendungsdaten von z.B. ERP-Systemen oder Kassen- und Arzt-Abrechnungsanwendungen.

Bei der Auswertung von Rechnernutzungsspuren stehen z.B. die Analyse und Interpretation von Protokoll- bzw. Verlaufsdaten und Dateizeitstempeln sowie die Zuordnung vorhandener Dateien und Spuren zu einzelnen Nutzern im Vordergrund. Dabei werten unsere Experten Daten aller gängigen Betriebs- und Dateisysteme aus und beherrschen die Analyse von Programmen zur Internetkommunikation und den verwendeten Protokoll.

Cybercrime & Industriespionage

Cybercrime oder Computerkriminalität ist zu einem Massenphänomen geworden – insbesondere was den Teilbereich der Internetkriminalität angeht. Angriffe können sowohl einen hohen monetären Schaden als auch Reputationsschäden verursachen. Hierzu zählen neben Angriffen von Außen zum Beispiel zum Zweck der Industriespionage auch von Mitarbeitern verursachte Datenlecks sowie mittels Computern durchgeführte Betrugsdelikte. Bei der forensischen Aufbereitung eines Cybercrime-Vorfalles stehen folgende Ziele im Vordergrund:

- Sicherung aller relevanten Daten
- Schnelle Identifikation des Modus Operandi, um den oder die Täter zu identifizieren
- Identifikation der Täter und der Opfer.

Zu Cybercrime im engeren Sinn zählt das Cybercrime Bundeslagebild 2011 des deutschen Bundeskriminalamt:

- Ausspähen, Abfangen von Daten einschließlich Vorbereitungshandlungen
- Computerbetrug, Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten
- Computersabotage
- Datenveränderung
- Fälschung beweiserheblicher Daten
- Täuschung im Rechtsverkehr bei Datenverarbeitung

Ansprechpartner Adrian Janotta
Ort Bundesweit, Österreich und Schweiz
Telefon +49 (9721) 370 38 17
Zielgruppe Unternehmen aus Mittelstand und Konzern

Dauer der Tests Individuell
Kosten Tagespauschale je Tester 1442.62 EUR zuzügl. Mwst.

AUSWERTUNG MOBILER GERÄTE

Smartphones und Tablet-PCs ersetzen herkömmliche Computer zunehmend sowohl im Privat- als auch im Berufsleben. Sie werden immer mitgeführt, sind immer online, werden ständig zur Kommunikation und zum Fotografieren und Filmen genutzt und speichern häufig Geolokalisationsdaten. Entsprechend wichtig sind mobile Geräte insbesondere im Rahmen der Strafverfolgung.

Aufgrund der großen Relevanz mobiler Geräte verfügen wir über ein eigenes Team, das sich ausschließlich auf die Aufbereitung von auf mobilen Geräten gespeicherten Daten spezialisiert hat. Für die Datensicherung von neuen oder stark abgesicherten mobilen Geräten greifen wir zusätzlich auch auf spezielle Verfahren und selbst entwickelte Software zurück. Häufig ist für jedes neue Gerät und jede neue Betriebssystem-Version die Identifikation neuer Angriffsvektoren nötig, um eine Umgehung entsprechender Sperren zu ermöglichen.

Janotta und Partner bietet dem Auftraggeber zwei Möglichkeiten im Bereich der mobilen Auswertung:

1. Janotta und Partner extrahiert und interpretiert die Daten und stellt sie dem Auftraggeber für weitere Analysen zur Verfügung.

2. Die ausgelesenen Daten fließen in die weitere IT-forensische Analyse und die Gutachten-Erstellung durch Janotta und Partner mit ein.

Öffnungszeiten Montag bis Samstag von 9 Uhr bis 18 Uhr
Hauptsitz Sachweinfurt bei Würzburg
Mitarbeiter 8 Mitarbeiter und 2 Praktikanten
Durchgeführte Penetrationstests 254 Tests durchgeführt

Erfahrung 18 Jahre Erfahrung

Datendiebstahl aufdecken

Welche Daten werden entwendet?

Sowohl externe als auch interne Täter haben es vornehmlich auf folgende Daten abgesehen:

- Kundendaten
- Bank- / Finanzdaten des Unternehmens
- Patente / Produktinformationen / Konstruktionszeichnungen
- Preis- / Konditionsinformationen

Ungewollter Informationsabfluss wirkt sich sehr negativ auf Ihr Unternehmen aus. Folgen sind unter anderem ein immens hoher monetärer Schaden sowie Reputationsverlust. Gerade für klein- und mittelständische Unternehmen kann sich Datendiebstahl existenzbedrohend auswirken. Ein Vorfall sollte daher mit der nötigen Dringlichkeit behandelt werden.

Da Unternehmen vornehmlich externe Täter als Bedrohung ansehen, werden häufig zu wenig Schutz- und Präventionsmaßnahmen für die Sicherheit vertraulicher Daten durch Diebstahl interner Mitarbeiter durchgeführt. Beides ist gleich wichtig. Beachtet werden sollte daher das Unternehmen im ganzen wie Janotta und Partner rät.

Schaden für Unternehmen

Die Gesamtschadenssumme bei Datendiebstahl und Unterschlagung beträgt pro Unternehmen über 1,6 Millionen Euro.

Adresse Breslaustrasse 28
Ort 97424 Schweinfurt
Email info@janotta-partner.de

Wartezeit Nach Vereinbarung und Termin
Partner und Freundschaften Botfrei.de, FH AISEC, Berufsfachschule für Informationstechnik.

Ungenutzte Möglichkeiten

Die Möglichkeiten der Computer-Forensik werden heute besonders in Deutschland noch nicht ausreichend genutzt. Die Einsatzmöglichkeiten sind noch immer häufig unbekannt, besonders der Mobil IT-Forensik. Dieser Bereich wird üblicherweise nur im Zusammenhang mit Hacking und oder IT-Sicherheit gesehen, dabei hat die IT- und Kommunikationstechnik schon längst all unsere Lebensbereiche durchzogen, leider nicht nur zu unserem Nutzen. Computerforensische Analysen und -Auswertungen lassen sich demnach in verschiedensten Fällen sinnvoll einsetzen, wie z.B. Datenspionage, Computerbetrug, Unterschlagung, Wirtschaftskriminalität, bis hin zu allgemeinen Straftaten und familienrechtlichen Fragestellungen.

Jede Reduzierung eines Know-How Vorsprungs bringt meist finanzielle Verluste, vernichtet Arbeitsplätze und gefährdet die Existenz von Unternehmen. Viele Entscheidungsträger/Manager haben leider noch immer die Einstellung, das Wirtschafts- und Konkurrenzspionage sie oder ihr Unternehmen nicht berühre, da ihr Unternehmen ja noch nie betroffen gewesen wäre. Fakt ist jedoch, das über 80% der Wirtschaftsspionage- sowie Manipulationsaktivitäten im Verborgenen laufen und fast nie entdeckt werden bzw. an die Öffentlichkeit gelangen.

Deutsches Know-How ist sehr gefragt!

Ansprechpartner Adrian Janotta
Ort Bundesweit, Österreich und Schweiz
Telefon +49 (9721) 370 38 17
Zielgruppe Unternehmen aus Mittelstand und Konzern

Dauer der Tests Individuell
Kosten Tagespauschale je Tester 1442.62 EUR zuzügl. Mwst.