



Computer Forensik - Zum Schutz Ihres Unternehmens

Ohne funktionierende EDV ist das tägliche Geschäft für viele Unternehmen nicht mehr realisierbar. Aus wirtschaftlicher Sicht ist es unabdingbar unternehmenskritische Daten vor Angriffen zu schützen und für den Fall der Fälle mittels gerichtsfesten Beweisen vorzusorgen.

Systeme gefährdet

Kein Computersystem kann als hundertprozentig sicher vor Einbrüchen oder Manipulationen gelten. Die Gründe, die Anlass zu einer forensischen Betrachtung von Rechnersystemen und Netzwerken geben können, sind vielfältig. Datenspinage, -manipulation und -zerstörung sind leider traurige Realität und allzu häufig. Immer wieder entwenden und zerstören vor der Ent-

lassung stehende Mitarbeiter wichtige Daten.

Richtige Beweissicherung


Angesichts eines vermuteten straf- oder zivilrechtlichen Vorfalls ist es wichtig, vorhandene Beweise unverfälscht sicherzustellen zu werden. Übereifrige Anwender und Administratoren vernichten häufig in einer frühen Phase viele Beweise. Ein kleiner Fehler, wie allein das bloße Herunterfahren des kompromittierten Systems, macht es unter Umständen schon unmöglich, wichtige Beweise zu sichten und zu sichern.

Notfall- und Alarmplan

Es gilt ein paar Grundregeln zu beachten, wenn der Verdacht oder konkrete Hinweise bestehen, dass ein Computer oder

ein Netzwerk missbraucht oder angegriffen worden ist. Im Idealfall erstellt ein Unternehmen vor einem konkreten Fall einen allgemeinen Notfall- und Alarmierungsplan, der den zuständigen Mitarbeitern zugänglich ist.

Incident Response

Man bezeichnet die strukturierte Reaktion bei einem Verdachtsfall als Incident Response. Neben detaillierten Plänen für das Vorgehen im akuten Anlassfall sollten auch Massnahmen für die vorbeugende Sammlung von Beweisdaten im laufenden Systembetrieb geplant werden. Ein vorausschauendes Log Management bewährt sich in Krisensituationen und sorgt für eine rasche und effektive Beweissicherung. 

Seminarankündigung

Gemeinsam mit ARS veranstaltet FDS 2008 in Wien zwei Seminare zum Thema „E-Mail Security & Forensik - Die sichere Übermittlung und gerichts feste Speicherung elektronischer Post“.

Seite 4

Computer Forensik im Wirtschaftsalltag

Das Tagesgeschäft im Blickpunkt, „vergessen“ viele Klein- und Mittelbetriebe auf angemessene Schutzmaßnahmen vor Computerkriminalität. Wer trägt die Verantwortung für eine Untersu-



chung bei verdächtigen Vorfällen? Welche Daten werden für ein Gerichtsverfahren sichergestellt? Wie können Schadensansprüche vor Gericht glaubhaft und durchsetzbar gemacht werden?

Seite 3

IT-Missbrauch selbst aufklären

Bei Fällen von Computermisbrauch ist den betroffenen Unternehmen meist an eigenen Ermittlungen und größtmöglicher Diskretion gelegen.



Bei einem bestehenden Verdacht auf Computermisbrauch stellt sich für Unternehmen die Frage, ob eigene Ermittlungen durchgeführt oder amtliche Stellen herangezogen werden sollen. Befürchtete Image- und Vertrauensverluste in der Öffentlichkeit oder der häufig vorhandene Wunsch nach interner Klärung und Lösung des Vorfalls führen meist zu privaten Ermittlungen seitens des Unternehmens.

Private Ermittlung zulässig

Der Gesetzgeber erlaubt


private Ermittlungen, so lange sie auf rechtmässige Art und Weise erfolgen. Für die geplante Untersuchung kann das betroffene Unternehmen eigene Ressourcen heranziehen oder die Beweissicherung externen Spezialisten übertragen. Private Ermittler verfügen im Gegensatz zu amtlichen Ermittlungsbehörden nur über eingeschränkte Möglichkeiten zur Erlangung von Beweisen. Die Beschlagnahme eines Computers ist beispielsweise nicht möglich. Selbst der Eigentümer kann nur eine sofortige

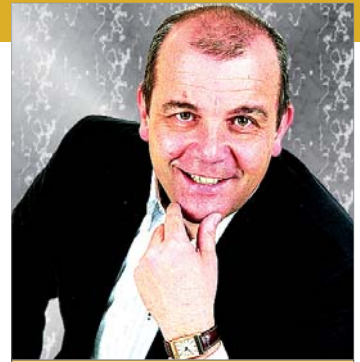
Herausgabe, seines im Besitz des Benutzers befindlichen Laptops, verlangen. Wird diese, beispielsweise mit dem Hinweis, dass sich private Daten auf dem System befinden, verweigert, ist dem Betroffenen die Möglichkeit zu geben, seine privaten Daten vom System zu löschen.

Datenschutz vorrangig

Daten dürfen nur ermittelt und verarbeitet werden, soweit Inhalt und Zweck der Datenverarbeitung in seinem berechtigten Zweck gedeckt sind und hiebei schutzwürdige Interessen des Betroffenen, insbesondere im Hinblick auf die Achtung seines Privat- und Familienlebens, nicht verletzt werden. Eine vorbeugende Überwachung durch Protokollierung der Computernutzung der Mitarbeiter zur Beweissicherung für den Eventualfall ist nicht zulässig.

Beratung empfehlenswert

Um sich bei privaten Ermittlungen nicht selbst ins Unrecht zu setzen, ist die möglichst frühe Beiziehung von Computer Forensik Experten empfehlenswert. Sie beraten bei der Ermittlungsplanung bzw. -durchführung und gerichtsfesten Aufbereitung der gefundenen Beweise. 



Die enorme Bedeutung betrieblicher Daten und Informationen erzeugt neue Formen der Kriminalität. Durch Computermisbrauch oder Datendiebstahl entstandene Schäden gehen in die Millionen und ruinieren Unternehmen. Schadensansprüche sind vor Gericht oder gegenüber Versicherungen nur bei zweifelsfreier Beweislage durchzusetzen. Welche Vorteile bietet Ihnen der Einsatz externer Spezialisten bei der Aufklärung? Zu einem erfolgreichen Verlauf der Untersuchungen ohne persönliche Beziehungen zu den Betroffenen, zum anderen gewährleisten wir Ihnen absolute Diskretion. Als Auftraggeber entscheiden Sie selbst, welche Erkenntnisse, wie weiterverwertet werden und beugen so etwaigen Image- und Vertrauensverlusten bei Bekanntwerden in der Öffentlichkeit aktiv vor.

Impressum

Ausgabe 01.2008.

Medieninhaber, Verleger und Herausgeber: FDS | Forensik Data Services - Ing. Mag. Horst Greifeneder. Linzer Straße 155b. A-4600 Wels. T 07242-77715. Mail office@fds.at.

Gestaltung: INFONOMICS Design, Wels.

Blattlinie: Wissenswertes in Zusammenhang mit der Erbringung von Forensik Data Services im Fachbereich Informationstechnik.

Recht und Informationstechnik im Internet

www.lexitec.at: Österreichische Fachzeitschrift für Recht und Informationstechnologie.

www.ars.at: Akademie für Recht & Steuern. Kooperationspartner von FDS | Forensik Data Services.

www.argedaten.at: Umfangreiche Informationen zu Informationsrecht, Datenschutz und Gesellschaft.

www.fds.at: Die Internet-Präsenz des Herausgebers.

Computer Forensik im Wirtschaftsalltag

Eine geschlossene Beweismittelkette, vollständige Dokumentation und die Gewährleistung absoluter Datenintegrität sind zentrale Qualitätsmerkmale für eine computerforensische Untersuchung.



Eine schlüssige und nachvollziehbare Vorgehensweise bei der Beweismittelsicherung ist das Um und Auf der Computer Forensik. Oberstes Gebot ist die absolute Integrität der sichergestellten Beweismittel.

Beweismittelquellen

Um die für Rechtsansprüche benötigten Beweise bei vermutetem Computermisbrauch zu sammeln, werden Daten von Systemen und Datenträgern sowie Protokolle des Netzverkehrs gesichert und analysiert.

Dokumentation

Eine geschlossene und vollständig dokumentierte Untersuchung ist zentrale Voraussetzung für eine gerichtsfeste Beweismittelgewinnung. Beweismittel und Dokumentation sind als Beweismittelkette so ins Verfahren einzubringen, dass keine Zweifel über Herkunft, Besitz und Integrität des Beweismittels auftauchen können.

Forensische Duplikate

In der Regel wird deshalb von den zu untersuchenden Datenträgern ein hundertprozentiges Duplikat (Image) erstellt. Zur Erstellung forensischer Kopien eignen sich sowohl Open Source Systemtools wie dd oder dcfldd als auch kommerzielle Forensik-Programme wie EnCase. Die genannten Programme stellen sicher, dass der Datenträgerinhalt vom Original Bit für Bit auf den Beweismittelträger kopiert wird. Mittels Hash-Zertifikaten (MD5 oder SHA-1) wird die Unverändertheit und Vollständigkeit der kopierten Daten gewährleistet.

Sichere Aufbewahrung

Nach der Fertigstellung und positiven Integrität-Check des Duplikats ist der Originaldatenträger unter Verschluss zu halten. Weitere Zugriffe auf das Original sind nach Möglichkeit zu vermeiden.

Zweitduplikat für Analyse

In der Praxis hat sich für die eigentliche Datenanalyse bewährt, vom Erstduplikat, eine weitere Kopien zu erstellen. Diese können von mehreren Analysten parallel untersucht werden und im Bedarfsfall können weitere Kopien vom Erstduplikat problemlos und schnell erstellt werden.

Analyse des Vorfalls

In der Folge werden die gesicherten Daten mit speziellen Analysemethoden untersucht. Durch Auswertung verschiedenster Datenquellen und Kombination der Informationen können

in der Regel für das Gericht oder dem Auftraggeber wichtige Fragen beantwortet werden: Was ist geschehen? Wann geschah der Vorfall? Welche Schäden sind genau entstanden? Die Antworten auf diese Fragen

Gesetzliche Lage

Nicht alles was technisch möglich ist, ist von rechts wegen auch erlaubt. Rechtliche Rahmenbedingungen wie Datenschutzgesetz, Persönlichkeitsrechte, Arbeitsrecht usw. sind zu beachten. Allzu schnell ist sonst die eigene Untersuchung selbst, Gegenstand von rechtlichen Ermittlungen. 🌀

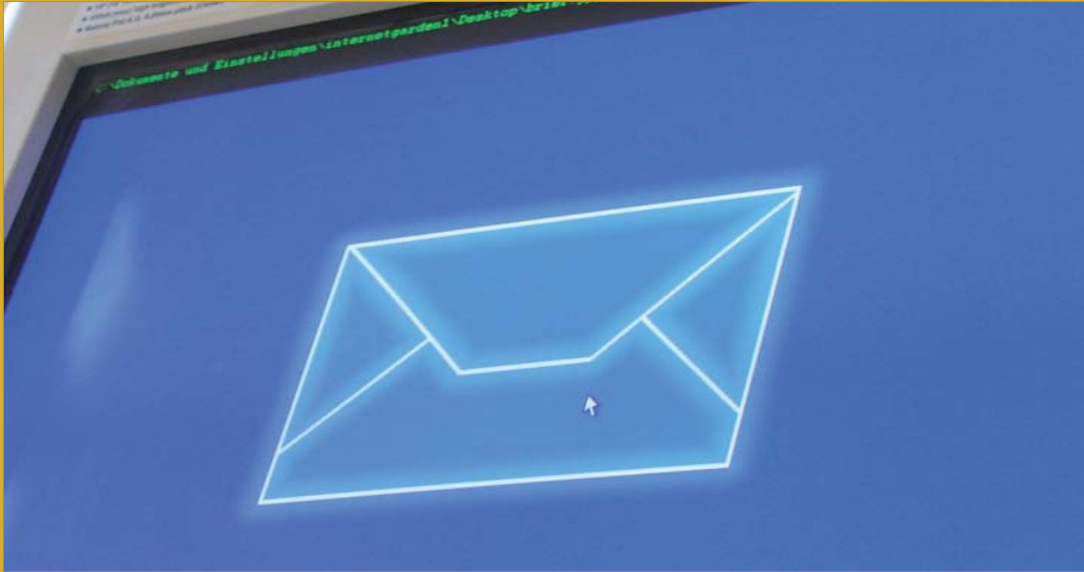
Computer Forensik Tools für Spezialisten

Helix - Knoppix-basierte Forensik Live-CD enthält eine Reihe von Open-Source-Tools für die Beweismittelsicherung und -analyse sowie Windows-Programme für eine sofortige Systemanalyse und Datenrettung. (www.e-fense.com).

EnCase Forensic - Windows-basiertes, kommerzielles Forensik-Standardprodukt für die Beweismittelsicherung mit umfangreichen Analyse-, Datenwiederherstellungs- sowie Reporting-funktionen. (www.encase.com).

E-Mails als Beweismittel vor Gericht

E-Mails sind leicht zu fälschen, haben kaum Beweiskraft und verfügen über keine verbindliche Sende- oder Empfangsbestätigung. Trotzdem spielen sie als Beweismittel eine wichtige Rolle vor Gericht.



Jeder halbwegs interessierte PC-Anwender kann elektronische Post auf einfachste Art und Weise verändern. Zudem sind der Versand und Empfang einer E-Mail in der Regel nicht zweifelsfrei nachweisbar, da die damit verbundenen Verkehrs- und Verbindungsdaten ebenfalls nahezu beliebig manipulierbar sind.

Aufbewahrung von E-Mails

Trotz der beschriebenen Problematik können E-Mails rechtsverbindliche Erklärungen enthalten und als Beweismittel vor Gericht von entscheidender Bedeutung sein. Abgesehen von gesetzlichen Aufbewahrungspflichten sollten deshalb Unternehmen alle E-Mails sicherstellen, die in einem Streitfall von Bedeutung sein könnten.

E-Mail vor Gericht

Normale E-Mails unterliegen in einem Prozess lediglich der freien Beweiswürdigung durch den Richter.

Er entscheidet letztendlich über die Glaubwürdigkeit des dargebotenen Inhalts und die Identität des angegebenen Absenders bzw. Empfängers.

Authentizität einer E-Mail

Nur bei einer nach dem Signaturgesetz signierten E-Mail kann davon ausgegangen werden, dass Inhalt und Absender der E-Mail authentisch sind. Entsprechende Zeitstempeldienste belegen zudem, dass die E-Mail zum einem bestimmten Zeitpunkt vorgelegt ist.

Vertraulichkeit gewährleisten

E-Mails werden auf dem Weg durch das Internet mittels zahlreicher Rechner weitergeleitet, bis sie bei ihrem eigentlichen Empfänger ankommen. Jeder, der Zugang zu diesen Netzwerkrechnern hat oder sich verschafft, kann diese E-Mails mitlesen. Um dies zu verhindern und etwaige datenschutzrechtliche Fall-

stricke zu entgehen, sollten E-Mails mit personenbezogenen Daten nur verschlüsselt gesendet werden.

Empfangsbestätigung

Bis heute fehlt bei der elektronischen Post ein Pendant zum eingeschriebenen, klassischen Brief. Damit ist der Nachweis, dass eine übermittelte Nachricht, den Empfänger auch erreicht hat, nicht zweifelsfrei möglich. Verschiedene technische Lösungsansätze wie die optionale Empfangsbestätigung und die Integration individueller Identifizierungselemente in versandte Nachrichten, versuchen zwar, entsprechende Empfangsbestätigungen zu generieren. Die endgültige Beweiskraft derartiger Verfahren vor Gericht ist in der Regel jedoch unbefriedigend. ☹️

Dieser Artikel ist eine gekürzte Version des Originals erschienen in der Fachzeitschrift für Recht und Informationstechnologie - lex:itec.

Seminarankündigung

Gemeinsam mit der Akademie für Recht, Steuern & Wirtschaft (ARS) veranstalten wir 2008 in Wien zwei Seminare zum Thema

E-Mail

Security & Forensik

Die sichere Übermittlung und gerichtsfeste Speicherung elektronischer Post.

Inhalte

Informieren Sie sich über Methoden und Verfahren zur sicheren Übermittlung, Sicherung der Integrität und Authentizität, Nachweisbarkeit der Zustellung von elektronischen Nachrichten und Möglichkeiten zur Wiederherstellung gelöschter E-Mails.

Zielgruppe

IT-Security-Verantwortliche, EDV-BeraterInnen, SystemadministratorInnen und VertreterInnen von Rechtsberufen.

Termine

10. April 2008, Wien, 09:00 - 17:00 Uhr, ARS Seminarzentrum.

7. November 2008, Wien, 09:00 - 17:00 Uhr, ARS Seminarzentrum.

Preis

Die Seminargebühr beträgt **€ 450,-** inkl Seminarunterlage, Begrüßungskaffee, Erfrischungsgetränke, Mittagessen und exkl. 20% USt.

Bei einer Buchung über FDS | Forensik Data Services erhalten Sie einen Referentenempfehlungs-Rabatt in der Höhe von 15% der Seminargebühr.

Weitere Informationen und persönliche Anmeldung auf www.fds.at.