Perspektiven der Online-Beweissicherung mit zentraler Sammelstelle

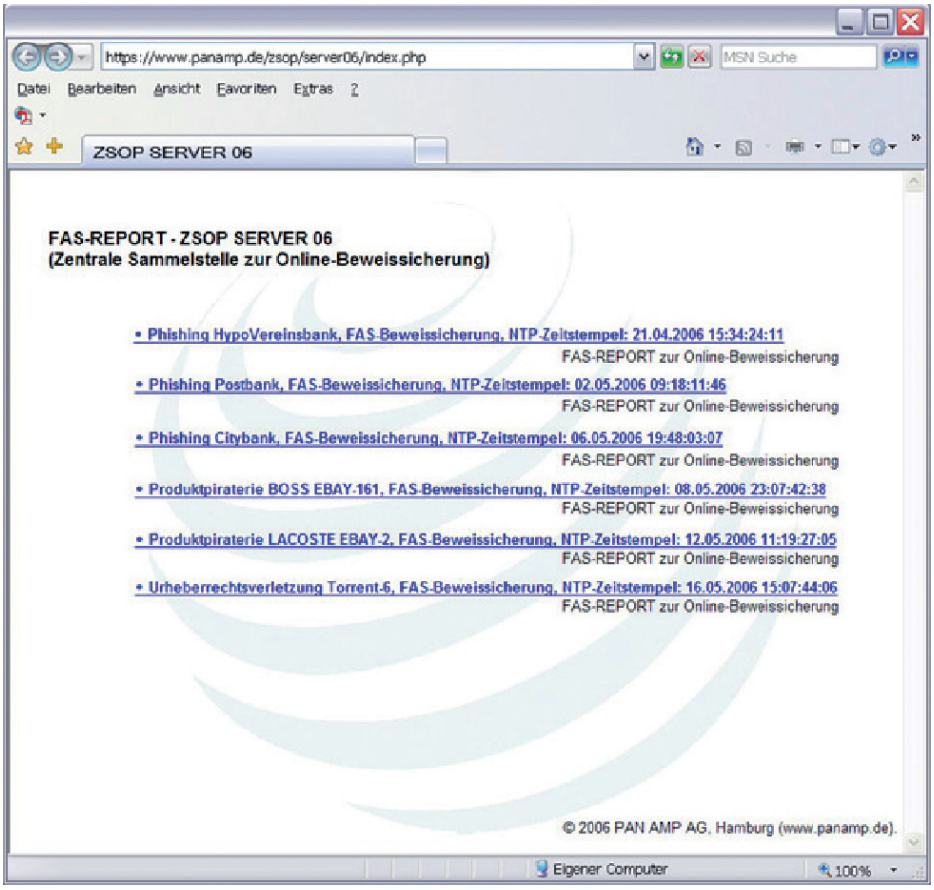
von Bert Weingarten,
Vorstand der PAN AMP AG, IT-Sicherheitsexperte und Erfinder der Online-Beweissicherung

Beflügelt durch eine umfassende Verfügbarkeit, immer schnellere Anbindungen und eine immer weitergehende Verbreitung des Internets erreicht die jederzeit für jedermann verfügbare Menge an Informationen und Daten ständig neue Dimensionen. Doch nicht nur legale Netzbetreiber, die lizenzierte und rechtlich einwandfreie Inhalte vertreiben, stellen immer größere Datenmengen in das Internet ein. Auch Kriminelle haben das Internet voll erschlossen; mit dem Effekt, dass in vielen staatlichen Einrichtungen bereits heute die Personalkapazitäten für die Verfolgung von Straftaten bis an die Grenze ausgeschöpft sind. Die noch immer verbreitete Recherche und Beweissicherung per Einzelplatz-PC mit Webbrowser und Screenshot (Abbild eines Programmfensters) wird der heutigen Anforderung bei weitem nicht mehr gerecht.

Immer neue Arbeitsweise in der Computerkriminalität – das Problem der „flüchtigen Beweise"

In – und Ausländische Strafverfolgungsbehörden stellten im vergangenen Jahr eine weitere Zunahme von Straftaten fest, die per Computer oder Rechenzentrum durchgeführt wurden. Das Spektrum der Straftaten reicht vom Betrug mit Dialern, Phishing, gefälschten Markenprodukten und Angaben über die Verbreitung von illegalem Material wie Kinder- oder Tierpornografie, bis zur Verbreitung von Computerviren und dem Einbruch in oder der Manipulation fremder Rechnersysteme.

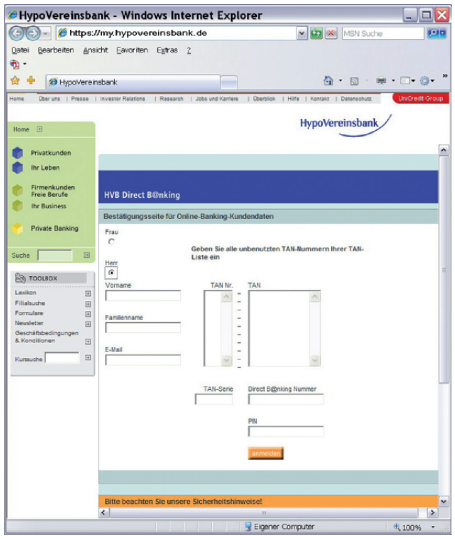
Bislang galt die goldene Regel, schnellstmöglich der zur Straftat verwendeten Computer habhaft zu werden, um einen technischen und kriminalistischen Prozess, den man als Digitale Forensik bezeichnet, durchzuführen. Doch wie sichert man „flüchtige Beweise", Beweise, von denen man erwarten muss, dass sie in kürzester Zeit nicht mehr verfügbar oder rekonstruierbar sein werden?



ZSOP – Zentrale Sammelstelle zur Online-Beweissicherung, PAN AMP AG, 12.05.2006

Bert Weingarten,
Vorstand der PAN AMP AG, IT-Sicherheitsexperte und Erfinder der Online-Beweissicherung

So ist es heutzutage Gang und Gebe, dass auf Servern die zu Betrugsdelikten eingesetzt werden, ein „cron job" eingerichtet ist, welcher in vorgegebenen Zeitabständen Spuren verwischt oder Daten zerstört, indem er diese mehrfach mit Datenmüll überschreibt. Bekommen die Forensik-Experten den Server nach der Aktivierung eines „cron jobs" zur Analyse, kann oftmals der Stecker gleich wieder aus dem Server gezogen werden.



FAS Online-Beweissicherung zum Phishing-Betrugsfall,HypoVereinsbank, 21.04.2006

Eine weitere ungelöste Problematik ist die Gegebenheit, dass die zur Straftat verwendeten Rechnersysteme oftmals ihren physikalischen Standort in einem anderen Bundesland oder im Ausland haben, oder es sicht gar um weltweit verteilte Rechnersysteme handelt. Eine Herausforderung, der bislang mit einem Ausdruck zur Akte begegnet wurde, da die Dokumentation Bestandteil der Beweismittelsicherung ist.

Diese Akte wurde bislang zu einem vor Gericht verwertbaren Gutachten aufbereitet, in dem die Forensik-Spezialisten technische Sachverhalte und Indizien so dokumentierten, dass auch für die in technischer Hinsicht unbedarften Prozessteilnehmer der Tatbestand und die Beweiskette augenfällig, also evident, werden. Allein die starke zeitliche Inanspruchnahme der Experten zur Herstellung des Gutachtens, die oftmals ein Mehrfaches der Zeit der Beweissicherung ausmacht, zeigt auf, dass dieses Prozedere ineffektiv und veraltet ist.

FAS Report zur Online-Beweissicherung zum Phishing-Betrugsfall, HypoVereinsbank, 21.04.2006

Der Weg zur Online-Beweissicherung – nur einen Mausklick entfernt

Wäre es nicht ausgezeichnet, wenn eine Technologie diese Arbeit erledigte?

Das dachten wir uns auch und stellten basierend auf der bereits entwickelten Sniffer-Technologie der PAN AMP AG umfassende Funktionen zur automatisierten Protokollierung plus Expertenanalyse her, die verdächtige Computer und Netzwerke mit fundiertem Know-How identifizieren, analysieren, Dossiers erstellen und die Online-Beweissicherung herstellen. Kurz: FAS-Report mit Online-Beweissicherung. (FAS = Filter Administrations System).

In Zeiten, in denen die Beweissicherung zur Straftat nur einen Mausklick entfernt ist, der Server, von dem die Straftat ausgeht, sich aber an jedem beliebigen Ort der Welt befinden kann, stellt die Online-Beweissicherung die vollumfängliche Ablösung der bislang händischen Bearbeitung da.

So stellt FAS-Report die vollständige Beweissicherung des Ausgangssystems über Datennetze her, ganz gleich ob Firewalls, SSL oder „Locked-Down"-Server eingesetzt werden. Somit ist es oftmals möglich, den kompletten Serverinhalt mit der vollen Funktionalität zu sichern.

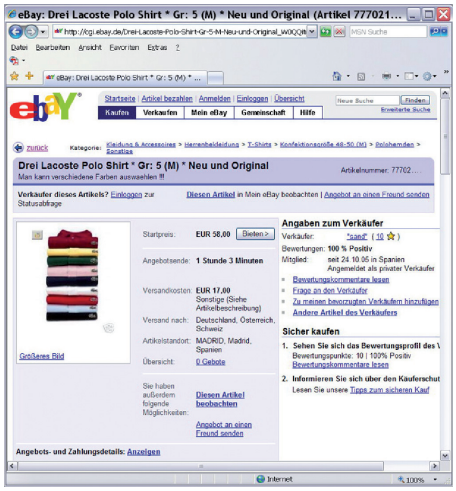
Nach der Sammlung und Sicherung aller Beweise kann die Analyse der Online-Beweissicherung beginnen. Automatische Auswertungen und Berichte können in kürzester Zeit zu vollständigen Dossiers verdichtet werden. Aus dem Dossier lassen sich etwa Zugangsberechtigungen und verschiedene Zeitstempel analysieren, die zu Antworten auf die Fragen führen, wann die letzte Veränderung statt fand und wer das System administriert hat. In nicht wenigen Fällen können weitere eindeutige Beweise über den verwendeten Onlinezugang des rechtlich Verantwortlichen sichergestellt werden.

Kommunikationsbeziehungs-analysen legen Identität der Straftäter offen

Mit Zuführung von weitergehenden Daten aus Firewall-Systemen, Routing- und Accounting- Daten, Datenbestände, die beim jeweiligen betroffenen Provider vorrätig sind, lassen sich vollständige Kommunikationsbeziehnungsanalysen (Forensic Accounting) herstellen, die die Identität der Straftäter offen legen.

In der ZSOP (Zentrale Sammelstelle zur Online-Beweissicherungen) erfolgen alle Speicherungen auf NTP-Basis (Network Time Protokoll). Der integrierte Zeitstempelserver, der sämtliche Online-Beweissicherungen und sonstige Ereignisse mit exakter Uhrzeit festhält, kann entweder die Referenzzeit über eine Funkuhr (DEC77/GPS) empfangen, oder per Server der Physikalish-Technischen Bundesanstalt in Braunschweig online synchronisiert werden.

Die in der ZSOP gespeicherten Online-Beweissicherungen sind somit manipulationssicher. Alle Zugriffe werden zusätzlich durch einem im „ZSOP" integrierten Log-Server festgehalten. Sowohl die Online-Beweissicherungen als auch die Dossiers werden auf optischen WORM-Laufwerken (Write Once Read Many) zusätzlich gespeichert. Somit besteht eine hundertprozentige Sicherheit vor Manipulationen.



FAS Online-Beweissicherung zur Markenpiraterie der Marke Lacoste, Ebay Deutschland, 12.05.2006

Zugriff der Sicherheitsbehörden über integrierte Schnittstellen

Durch integrierte Schnittstellen können weitere staatliche Stellen – nach jeweiliger Berechtigung und/oder Freigabe – auf Online-Beweissicherungen ohne jegliches Risiko eines unglücklichen Missgeschicks (Daten-Manipulation) zugreifen. Allein diese Position ist nicht zu unterschätzen, da so im Einsatzfall des ZSOP in Landeskriminalämtern die erste bundesweit nutzbare Datenschnittstelle entsteht, die zeitgleich für Internetfahnder zugänglich ist und plattformunabhängig per Webbrowser genutzt werden kann, ohne dass weitere Rechenlast auf lokalen Computern entsteht.

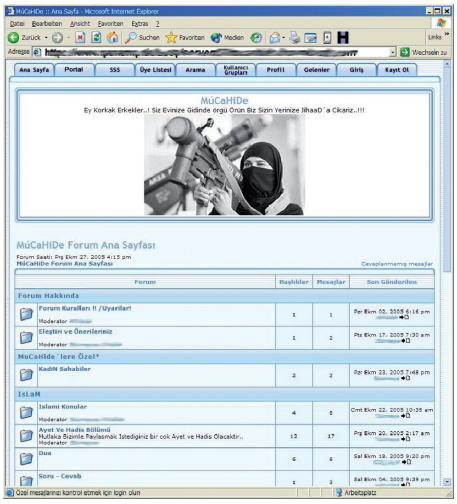
Zur vollständigen Beantwortung der juristischen Frage der so genannten „7-Goldenen-W" (wer? was? wann? wo? womit? wie? warum? reicht ein einziger Mausklick. Hierdurch werden die Online-Beweissicherung und das dazugehörige Dossier mit den erforderlichen Servernotwendigkeiten der Staatsanwaltschaft online zugestellt bzw. auf CD oder DVD zur Übergabe gespeichert. Vor Gericht kann die Straftat nicht nur angesehen, sondern durch die vorliegende Online-Beweissicherung nachgestellt werden.

Wie im Fall des Phishing-Betrugsfalls der HypoVereinsbank am 21.04.2006.

Hier ist aus dem Report der Standort, die verwendete Konfiguration und der vollständige betrügerische Auftritt ersichtlich (FAS Online-Beweissicherung HypoVereinsbank). Im Falle der Markenpiraterie wurde die Online-Beweissicherung bereits zur Überführung von Markenpiraten verwendet (FAS Online-Beweissicherung Ebay).

Automatisierten Analyse- und Reportingsystemen gehört die Zukunft der Internet-Beweissicherung

Automatisierten Analyse- und Reportingsystemen, die nicht gesetzeskonforme Inhalte im Internet aufspüren, entsprechende Analysen und Berichte erstellen, sowie die Online-Beweissicherung durchführen, gehören nicht nur die Zukunft. Sie sind bereits heute von erfolgs-



FAS Online-Beweissicherung zur Rekrutierungspraxis von Terror-Organisationen, Hürth bei Köln, 27.10.2005

entscheidender Bedeutung für die Abwehr von Gefahren und die Verfolgung von Straftaten. Die zusätzlichen Schnittstellen zur Ansicht, Analyse und zur Übergabe der Beweise beschleunigen die Strafverfolgung erheblich. Denn eines ist klar-die Internetstraftaten werden auch weiterhin ansteigen. Nur mit automatisierten Prozessen und Experten-Know-How kann die Durchsetzung bestehender Gesetzte auch zukünftig noch gewährleistet werden.

Aktuell befindet sich der Hersteller bereits mit zwei Landeskriminalämtern in konkreten Verhandlungen zur Integration der Online-Beweissicherung auf Landesebene. Die Inbetriebnahme ist hierbei noch für 2006 vorgesehen. Eine starke Einbindung der Datenschutzbeauftragten ist Bestandteil der Integration.

Kontakt:

PAN AMP AG
Ausschläger Elbdeich 2
D-20539 Hamburg
Tel.: +49 (40) 55 30 02-0
Fax :+49 (40) 55 30 02-100
E-Mail: info@panamp.de
Internet: www.panamp.de