Hakin9

HARD CORE IT SECURITY MAGAZINE

Hakin9 Ausgabe 12/2011 Dezember Monats-Online-Magazin

WELCHE SPEZIELLE HARDWARE VERWENDEN IT-FORENSIKER?

IT-Grundschutz

Web Security

Netzwerksicherheit

PLUS MYBIOS

LIEBE HAKIN9 LESER!

das Hauptthema der November Ausgabe ist IT-Forensik.

Kleine Fehler können Untersuchungsergebnisse unbrauchbar machen und ganze Verfahren ruinieren. Welche Punkte sind bei der Sicherung zu beachten? Welche Methoden sind üblich? Welche spezielle Hardware verwenden IT-Forensiker? Des Weiteren lesen Sie im Artikel Sicherung Digitaler Beweismittel. Das war das beliebteste Thema in unserer Umfrage und wir gehen Ihren Wünschen entgegen.

Zu weiteren Highlights der aktuellen Ausgabe gehören: Netzwerksicherheit - Spannungsverhältnis von Sicherheit, Komplexität und Produktivität, Web Security – Identifizieren und Beheben von Sicherheitslücken in Webanwendungen, Ein teilquantifizierter Risikobewertungsansatz mit einer Prise IT-Grundschutz, MYBIOS Lässt sich das BIOS infizieren?

Das ist die letzte Ausgabe in diesem Jahr, deswegen möchte ich Ihnen zur Weihnachtszeit Gesundheit, Glück und Zufriedenheit wünschen.

Wir danken Ihnen für das uns entgegen gebrachte Vertrauen und wünschen Ihnen auch einen guten Rutsch ins Neujahr.

Falls Sie Interesse an einer Kooperation hätten oder Themenvorschläge, wenden Sie sich bitte an unsere Redaktion.

Viel Spaß mit der Lektüre!
Karolina Sokołowska

hakin9

Sicherung Digitaler Beweismittel

Manuel Rundt, Martin Wundram, Alexander Sigel

Die Sicherung digitaler Beweismittel stellt hohe Anforderungen an eine absolut korrekte Arbeitsweise. Denn schon kleine Fehler können Untersuchungsergebnisse unbrauchbar machen und ganze Verfahren ruinieren. Welche Punkte sind bei dieser Sicherung zu beachten? Welche Methoden sind üblich? Wie kann sichergestellt werden, dass die Beweismittel später nicht manipuliert wurden, oder dass etwaige Manipulationen zumindest sicher aufgedeckt werden? Welche spezielle Hardware verwenden IT-Forensiker?

IN DIESEM ARTIKEL ERFAHREN SIE...

- welche Methodiken und Techniken bei einer forensischen Sicherung digitaler Beweismittel eingesetzt werden und was Sie von Anfang an vermeiden sollten. Zudem erfahren Sie, wie spätere Manipulationen von Beweisen ausgeschlossen werden oder zumindest zuverlässig aufgedeckt werden können.

WAS SIE VORHER WISSEN SOLLTEN...

welche verschiedenen Arten von Datenträgern potentiell wichtige Informationen enthalten können, um diese zunächst sicherzustellen. Um selbst forensische Sicherungen digitaler Beweismittel vorzunehmen, sollten Sie wissen, wie Änderungen an Datenträgern und Dateisystemen entstehen und vermieden werden können, sowie spezielle forensische Hardware verwendet und forensische Imaging-Software benutzt wird.

Zur Aufklärung von Hackerangriffen, aber auch von wirtschaftskriminellen Vorgängen, wird zunehmend häufiger auf die IT-forensische Analyse von digitalen Beweismitteln zurückgegriffen. Diese müssen zunächst gesichert werden, bevor Indizien und Beweise in den elektronischen Daten gefunden werden können. Dabei gibt es einige Fallstricke zu beachten. Wichtigstes Ziel bei einer Digitalen Beweismittelsicherung ist, die Vollständigkeit und die Unversehrtheit der Daten zu gewährleisten. Dies bedeutet, dass bei der Sicherung der Daten keine Veränderungen an den Datenträgern vorgenommen werden dürfen und dass auch bei der späteren Auswertung die Daten nicht verändert werden dürfen, da sonst Beweismittel unwiederbringlich vernichtet werden oder der Verdacht, die Beweise seien manipuliert, nur schwer zu widerlegen ist. Bei der Sicherung eingeschalteter Geräte, die verfahrensrelevante flüchtige Spuren enthalten können, z.B. hinsichtlich der Existenz von Rootkits, der Nutzung von Diensten im Internet oder in Clouds oder etwaiger Verschlüsselungen, kann die goldene Regel, keine Daten zu verändern, nicht eingehalten werden. Denn die Sicherung flüchtiger Spuren führt in der Regel zu Änderungen an den zu sichernden Daten. Hier ist eine Güterabwägung vorzunehmen. Erforderliche Änderungen sind auf ein Minimum zu beschränken und sorgfältig und beweissicher zu dokumentieren.

Wie sollte vorgegangen werden?

Eine sorgfältige Planung und Durchführung der digitalen Beweismittelsicherung ist entscheidend für den späteren Erfolg bei der Datenauswertung und der Nutzung der digitalen Beweismittel vor Gericht. Sofern im betroffenen Unternehmen keine ausgebildeten Computerforensik-Experten vorhanden sind, empfiehlt es sich, schon zu Beginn eines Vorfalls externe IT-Forensik-Experten hinzuzuziehen.

Die betroffenen Computer dürfen unter keinen Umständen eingeschaltet werden, bevor nicht alle Datenträger physisch gesichert wurden und die Beweismittelsicherung verifiziert ist. Auch eine unmittelbare Einsichtnahme („mal eben reinschauen“) in die aufgefundenen Datenträger ist unter allen Umständen zu vermeiden, da sich hierdurch nahezu immer für den Laien nicht sichtbare Spuren verändern, die später eine

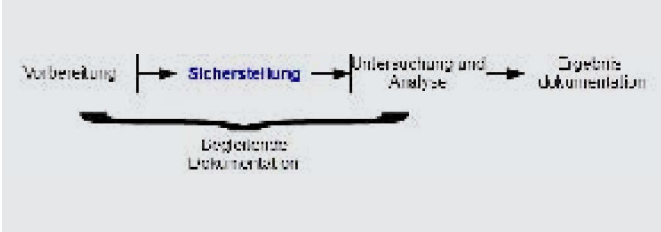

Abbildung 1. *Ablauf einer IT-forensischen Analyse*

verlässliche Zuordnung der aufgefundenen Beweise zu einem bestimmten Computerbenutzer unmöglich machen können.

Bei der physischen Sicherung ist zu unterscheiden, ob die Computer eingeschaltet oder ausgeschaltet sind:

Alle Computer, die **ausgeschaltet** sind, sollten an einen sicheren Ort verbracht werden, zu dem Verdächtige und deren mögliche Helfer keinen Zutritt haben. Dies gilt auch für andere relevante Datenträger wie externe Festplatten, DVDs, USB-Memory-Sticks, Speicherkarten, aber auch MP3-Player, PDAs, Smart- und Mobiltelefone, etc., die am Arbeitsplatz bzw. Tatort aufzufinden sind. Denn auch auf ihnen könnten sich digitale Beweise befinden.

Für **eingeschaltete** Computer und Mobilgeräte wurde vor einigen Jahren noch angeraten, diese durch Unterbrechen der Stromzufuhr „hart" abzuschalten (also Steckerziehen bzw. Batterie entfernen), um ein geordnetes Herunterfahren zu unterbinden, welches mögliche Beweise vernichten könnte. Auch durch dieses „harte" Abschalten gehen jedoch wichtige Informationen verloren, die je nach Fall entscheidend sein können. Zudem könnten Speichersysteme von Servern dadurch Schaden nehmen, wenn sie z.B. als RAID-Verbünde laufen und gepufferte Daten noch nicht auf die physischen Datenträger geschrieben wurden.

Deshalb wird heute empfohlen, laufende Computer so lange eingeschaltet zu lassen, bis von einem IT-Forensiker abgeklärt ist, wie weiter zu verfahren ist. Dies ist ohnehin angezeigt, wenn die Dienste auf dem System geschäftskritisch sind und eine Abschaltung möglicherweise grßeren Schaden verursacht als z.B. ein bislang nur vermuteter Sicherheitsvorfall anrichten könnte. Bis zum Eintreffen des Spezialisten sollte aber sichergestellt werden (z.B. durch Wechsel der Türschlsser oder persönliche Bewachung), dass kein Dritter physisch Zugang zu diesen Computern hat. Um zu verhindern, dass über Netzwerk Veränderungen an den Computern vorgenommen werden, sollten Netzwerkverbindungen (LAN-Kabel, WLAN-Verbindungen, ggf. auch UMTS- und ISDN- und Modem-Anbindungen) unterbrochen werden. Das genaue Vorgehen hängt jedoch vom Einzelfall ab. Ist das kompromittierte System ein Server, der für die Aufrechterhaltung des Geschäftsbetriebes notwendig ist, wird eine Trennung vom Netzwerk nur in Ausnahmefällen praktikabel sein. Ebenso kann es beispielsweise bei Hackerangriffen sinnvoll sein, den betroffenen Server vorläufig am Netz zu lassen, um den Angreifern zunächst verdeckt bei Ihrer Arbeit zuzuschauen und dadurch eventuell wichtige Erkenntnisse zu weiteren kompromittierten Systemen zu erhalten. Zudem könnten die Angreifer wichtige Beweise auf anderen Systemen Ischen, wenn sie zu früh bemerken, dass sie entdeckt wurden.

Digitale Beweismittelsicherungen

Ziel jeder digitalen Beweismittelsicherung und IT-forensischen Untersuchung ist die Erstellung von gerichtsverwertbaren, d.h. vor Gericht zulässigen digitalen Beweismitteln, um mögliche zivilrechtliche Ansprüche auch vor Gericht durchzusetzen oder um als Beweismittel in einem Strafverfahren zu dienen.

Dazu ist die Erstellung von exakten - sprich bitweise identischen - forensischen Kopien der originalen Datenträger nach den Grundsätzen der ordnungsgemäßen Beweiserhebung notwendig. Dabei hat sich allgemein durchgesetzt, dass stets **mindestens zwei** exakte Kopien der originalen Datenträger erstellt werden. Die erste Kopie dient als Beweiskopie und wird üblicherweise direkt nach Erstellung und erfolgreicher Verifikation manipulationssicher versiegelt und an einem sicheren Ort wie einem Tresor oder Bankschließfach verwahrt. Die weiteren Kopien dienen nach ihrer Verifikation als Grundlage für die anschließenden IT-forensischen Analysen.

Die originalen Daten und auch die erstellten Kopien dürfen weder während der digitalen Beweismittelsicherung noch zu einem späteren Zeitpunkt verändert werden. Hierzu wird zum einen geeignete Hardware eingesetzt, zum anderen kommen spezielle Prüfsummen, sog. Hashes, zum Einsatz, mit deren Hilfe die Unversehrtheit der Daten später nachgewiesen werden kann.

Vor der Erstellung der digitalen Beweismittelsicherungen und der computerforensischen Analysen muss jedoch die **Zulässigkeit** geklärt werden, denn bei schwerwiegenden oder fahrlässigen Verfahrensverstßen ist ein Beweisverwertungsverbot die zwingende Folge [1]. In jedem Fall sind jedoch die Vorschriften des Bundesdatenschutzgesetzes sowie weiterer einschlägiger Gesetze und Vorschriften sowie natürlich alle betriebsinternen Regelungen einzuhalten.

Die verfügbaren Datenquellen müssen vor der Beweissicherung hinsichtlich des Grades ihrer **Beständigkeit (Flüchtigkeit)** eingeordnet werden, um die richtige Reihenfolge für die Sicherung der Beweismittel festlegen zu können. Je flüchtiger (volatiler) ein Beweismittel ist, desto früher ist es zu sichern [2]. Flüchtige Spuren sind bereits nach kurzer Zeit bei normalem Betrieb des Computersystems oder nach dessen Abschalten für immer verloren. Hierzu zählen beispielsweise Daten in der CPU (Prozessorregister, CPU-Cache), im DNS-Cache oder im Hauptspeicher. Weniger flüchtige Informationen sind auch noch nach dem Abschalten des Computersystems auf den angeschlossenen Datenträgern aufzufinden und auswertbar.

Die Sicherung flüchtiger Daten

Vor jeglicher Analyse ist der Hauptspeicherinhalt vollständig zu sichern. Denn jede gezielte Abfrage flüchtiger Informationen aus dem Hauptspeicher (z.B. welche Prozesse sind aktiv? Welche Ports sind offen?) ändert den Hauptspeicherinhalt, wodurch wichtige Teile der flüchtigen Informationen verloren gehen können. Weil auch die Sicherung des gesamten Hauptspeichers typischerweise den Hauptspeicherinhalt ändert, darf man nur Werkzeuge einsetzen, welche die geringstmöglichen Veränderungen (minimal footprint) hervorrufen, d.h. minimal-invasiv sind [3]. Am wenigsten Veränderungen erzeugen Hauptspeichersicherungen mit spezieller Hardware oder besonderen Techniken (Firewire-Kabel oder „Cold boot"-Angriff), danach solche Sicherungsprogramme mit dem geringsten Hauptspeicherbedarf.

Bei der Sicherung über die Firewire-Schnittstelle können Geräte mit manipulierter Firmware eingesetzt werden [4] oder aber ein zweiter Computer, der, als Firewire-Gerät maskiert, an den Firewire-Port angeschlossen wird [5]. Mittels Direktzugriff auf den Hauptspeicher (via DMA) des zu sichernden Computers kann so der Hauptspeicher ausgelesen werden. Alternativ können bei einem „Cold boot"-Angriff die Speicherriegel des laufenden Computers mit Kühlmittel (z.B. Kältespray) gekühlt werden, sodass ihre Inhalte sich weniger schnell ändern. Danach werden die Speicherriegel mit einem speziellen Lesegerät oder über ein von einem externen Datenträger gebooteten Linux ausgelesen [6]. In der Praxis werden jedoch Hauptspeichersicherungen mit möglichst kleinen Kommandozeilen-Programmen bevorzugt, da sie praktischer sind.

Im Anschluss an die komplette Sicherung des Hauptspeichers können dann durch gezielte Abfragen weitere Informationen zum Computersystem und dessen Zustand gewonnen werden, wie beispielsweise Informationen zu den derzeit angemeldeten Benutzern, ausgeführten Prozessen und den bestehenden Netzwerkverbindungen. Im Zusammenhang mit den Netzwerkverbindungen sind auch die geffneten TCP- und UDP Ports, die Prozesse, welche diese Ports geffnet haben sowie die interne Routing-Tabelle von Bedeutung. Alternativ können diese Informationen meist auch nachträglich aus dem Abbild des Hauptspeichers ausgelesen werden. Das Tool der Wahl ist hierbei das bekannte Volatility Framework [7], das in der aktuellen Version 2.0 Hauptspeicherinhalte bis Windows 7 (allerdings nur 32bit) unterstützt.

Wichtig ist, dass für die Gewinnung der oben aufgeführten flüchtigen Informationen unter allen Umständen auf die bereits auf dem System verfügbaren Administrationswerkzeuge verzichtet wird, da nicht abgeschätzt werden kann, inwieweit diese möglicherweise absichtlich manipuliert wurden, um falsche Informationen zu liefern oder um weitere Schadfunktionen zu aktivieren. Daher sind nach Möglichkeit bei der Sicherung der flüchtigen Daten statisch kompilierte und aus vertrauenswürdiger Quelle stammende Administrationswerkzeuge zu verwenden, die von einer CD oder einem schreibgeschützten einem USB-Stick aufgerufen werden.

Als Tools kommen hierbei meist spezielle forensische Live-Distributionen zum Einsatz, wie beispielsweise Helix [8], F.I.R.E [9], Inside [10] oder grml [11] und Backtrack [12] mit der Forensic-Option. Oftmals dienen dabei zur Sicherung des Hauptspeichers und von Festplatten im laufenden Betrieb auf Windows portierte Open Source Tools, z.B. das dd aus der MoonSols Windows Memory Toolkit Community Edition [13]. Beliebt ist auch der frei verfügbare FTK Imager [14].

Sofern nicht geklärt ist, dass sämtliche Passworte eingebundener virtueller und verschlüsselter Laufwerke und Partitionen auch für die spätere Analyse zur Verfügung stehen, ist der Status der Verschlüsselung ebenfalls zu dokumentieren und müssen die die Daten aus den verschlüsselten Partitionen gesichert werden, bevor das System ausgeschaltet wird.

Die Sicherung weniger flüchtiger Daten

Klassisches Beispiel für eine digitale Beweissicherung von nicht-flüchtigen Daten ist die Erstellung von forensischen Kopien der Festplatten eines Computers. Hierbei wird eine bitweise Kopie des originalen Datenträgers erstellt, wobei jedes Bit der originalen Festplatte in gleicher Weise in die zu erstellende Kopie geschrieben wird. Bei Lesefehlern vom Originaldatenträger kann mit Werkzeugen wie dd_rescue versucht werden, noch möglichst viele Daten rund um den beschädigten Bereich herum zu retten.

Neben den erwähnten Beispielen zu nicht-flüchtigen Daten gibt es noch zahlreiche weitere Datenquellen. Dazu gehren zum Beispiel optische Medien wie CD und DVD, Flash-Speicher wie Solid State Disks, USB-Memory Sticks und Flash-Speicherkarten in diversen Formaten sowie Organizer wie MDAs, PDAs, XDAs und Palms. Auch MP3-Player, Smartphones, Blackberrys und Telefonanlagen können wichtige digitale Beweise enthalten.

Die zunehmend beliebteren Solid State-Disks (SSD) stellen eine besondere Herausforderung dar, weil selbst beim Einsatz von Hardware-Schreibschutz die Firmware bei der Nutzung und damit auch bei der Sicherung eine automatische Defragmentierung durchführen kann, welche Beweise vernichtet [15].

Als Werkzeuge kommen hierbei ebenfalls überwiegend spezielle forensische Live-CDs zum Ein-

satz, wie die bereits zuvor erwähnten Distributionen. Zudem liefern oftmals auch die Hersteller von computerforensischer Analyse-Software ihre eigenen Imaging Tools aus, so wie das von Guidance Software bereitgestellte LinEn, das zur Erstellung von Encase-Imagedateien verwendet werden kann, oder der zuvor erwähnte FTK Imager, der ebenfalls Encase-kompatible Images aber auch dd-kompatible Raw-Images erstellen kann. Als schnellste und effizienteste Kombination erweist sich in der Praxis meistens eine Linux-Live CD mit dem Kommandozeilen-Tool dd bzw. dessen forensischen Varianten wie dd_rescue und dcfldd. Letztere erlaubt auch die gleichzeitige Erstellung mehrerer Kopien und kann zudem auch gleich noch die notwendigen Hashwerte mit berechnen [16].

Um Änderungen an den originalen Datenträgern effektiv auszuschließen, wird spezielle Hardware eingesetzt, die jegliche Schreibzugriffe auf die Datenträger verhindert. Diese sogenannten Write-Blocker gibt es für nahezu alle möglichen Anschlusstechniken von Datenträgern und Bussystemen (IDE/PATA, SATA, USB, Firewire, SCSI, SAS, etc.). Darüber hinaus sind viele Linux-basierte forensische Live-Distributionen so ausgelegt, dass ein Schreiben auf die angeschlossenen Datenträger per Software Write-Block verhindert wird. Durch den Einsatz zertifizierter Hardware-Write-Blocker können Veränderungen an den originalen Datenträgern effektiv ausgeschlossen werden. Eine Liste zertifizierter Write-Blocker führt das US-amerikanische NIST (National Institute of Standards and Technology) [17]. Bekannte Hersteller von Hardware Write-Blockern sind Tableau [18] und WiebeTech [19]. Bei Einsatz von Software-Write-Blockern in Live-Distributionen ist ebenfalls darauf zu achten, ob ausreichend getestet wurde, dass diese wirklich keine Veränderungen an den Original-Datenträgern hervorrufen.

Die Verifizierung digitaler Beweismittel

Um sicherzustellen, dass die originalen Daten und die erstellten Kopien bitweise identisch sind, werden Prüfsummen des originalen Datenträgers und der erstellten Kopien berechnet. Hierzu werden kryptografische Hash-Funktionen eingesetzt, welche für einen eingelesenen Datenstrom eine eindeutige Prüfsumme berechnen. Mit geeigneten Hash-Funktionen lassen sich so selbst kleinste Unterschiede zwischen zwei Datenstrmen eindeutig nachweisen (etwa ein gekipptes Bit).

In der Praxis hat sich hier die Nutzung des SHA1 Hash-Algorithmus [20] durchgesetzt. Der früher verwendete MD5 Hash-Algorithmus [21] findet kaum noch Anwendung, da er mittlerweile als zu anfällig für Kollisionen gilt [22][23]. Um ganz sicher zu gehen, nutzen manche Computerforensik-Experten unterschiedliche Hash-Algorithmen gleichzeitig, zumal bekannte Sammlungen von Hashwerten z.T. noch auf MD5 basieren.

Durch die bei der Erstellung der Beweissicherungen erzeugten und dokumentierten Prüfsummen können später zufällige oder gezielte Manipulation von digitalen Beweisen in jedem Fall aufgedeckt werden. Auch wenn die kryptografische Stärke der in der Praxis verwendeten Hash-Algorithmen durch die allseits bekannten Kollisionsattacken geschwächt wurde (siehe Kasten), bedeutet dies noch lange nicht, dass diese Verfahren zur Aufdeckung von gezielten Manipulationen nicht mehr einsetzbar sind. Um beispielsweise eine digitale Beweismittelsicherung nachträglich zu manipulieren und gefälschte Beweise einzubringen oder vorhandene Beweise zu vernichten, müsste dazu eine neue Beweismittelkopie erzeugt werden, die wiederum exakt den bei der ursprünglichen Sicherung ermittelten Hash erzeugt. Hierzu ist eine sogenannte Pre-Image-Attacke notwendig (s. Kasten), bei der es bislang noch keine nennenswerten Fortschritte gibt.

Angriffe auf Hash-Funktionen am Beispiel von SHA1

Es gibt zwei Arten von Angriffen auf kryptografische Hashfunktionen. Die erste Angriffsart ist der sogenannte Pre-Image-Angriff, bei dem zu einer vorgegebenen Nachricht eine zweite Nachricht gefunden werden muss, die exakt den gleichen Hashwert liefert. Die zweite Angriffsart bezieht sich auf das Auffinden von zufälligen Kollisionen, d.h. von zwei zufälligen Nachrichten, die den gleichen Hashwert ergeben. Eine solche Attacke wird auch als „Kollisionsangriff" bezeichnet.

Während ein Pre-Image-Angriff auf den SHA1-Algorithmus mit einem 160 Bit-Hashwert theoretisch 2^{160} Hashwertberechnungen benötigt, benötigt das Auffinden zweier zufälliger Nachrichten, die eine Kollision der Hashwerte verursachen, aufgrund des Geburtstagsparadoxons nur 2^{80} Hashwertberechnungen.

Die von den chinesischen Forschern um Xiaoyun Wang berichteten Fortschritte bei der Errechnung von Kollisionen beim SHA1-Algorithmus beziehen sich ausschließlich auf den Kollisionsangriff. So konnten die Forscher den Aufwand zum Auffinden zweier zufälliger Kollisionen beispielsweise für den SHA1-Algorithmus von 2^{80} auf 2^{69} senken [25].

Doch auch die Senkung auf 2^{69} Hashwertberechnungen bedeutet in der Praxis, dass die Erzeugung von zufälligen Kollisionen selbst auf einem Computersystem, das theoretisch 1 Milliarde Hashwerte je Sekunde ausrechnen könnte, noch immer annähernd 20.000 Jahre dauern würde [26].

Um hingegen einen Pre-Image-Angriff durchzuführen, sind somit aktuell 2^{91} mal mehr Berechnungen notwendig, als bei einem Kollisionsangriff. Somit würde ein solcher Angriff auch mit aller weltweit verfügbaren Rechenkraft noch immer viele Millionen Jahre dauern.

Literatur

[1] Pressemitteilung Nr. 47/2005 vom 8. Juni 2005 zu Bundesverfassungsgericht 2 BvR 1027/02 vom 12. April 2005, *http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg05-047.html*

[2] Order of Volatility gemäß RFC 3227: „Guidelines for Evidence Collection and Archiving“ *http://www.ietf.org/rfc/rfc3227.txt*

[3] Windows Forensic Analysis – Incident Response and Cybercrime Investigation Secrets; Harlan Carvey, 2007, Syngress Verlag

[4] 0wned by an iPod; Maximillian Dornseif; Präsentation für die PacSec 2004 *http://pi1.informatik.uni-mannheim.de/filepool/presentations/0wned-by-an-ipod-hacking-by-firewire.pdf*

[5] pythonraw1394; Adam Boileau *http://www.storm.net.nz/projects/16*

[6] Lest We Remember: Cold Boot Attacks on Encryption Keys; Princeton University *http://citp.princeton.edu/research/memory/*

[7] The Volatility Framework *https://www.volatilesystems.com/default/volatility*

[8] Helix Live-CD *http://www.e-fense.com/helix/*

[9] F.I.R.E Live-CD *http://fire.dmzs.com/*

[10] Inside Live-CD *http://www.inside-security.de/*

[11] grml Live-DVD *http://grml.org*

[12] Backtrack Live-DVD *http://www.backtrack-linux.org/*

[13] Monsools Windows Memory Toolkit *http://www.moonsols.com/products/*

[14] Access Data FTK Imager / FTK Imager Lite *http://accessdata.com/*

[15] Graeme B. Bell & Richard Boddington: Solid State Drives: The Beginning of the End for Current Practice in Digital Forensic Recovery?, in: JDFSL – The Journal of Diigtal Forensics, Security and Law, 5(3), 2010 *http://www.jdfsl.org/subscriptions/JDFSL--V5N3-Bell.pdf*

[16] dcfldd *http://dcfldd.sourceforge.net/*

[17] NIST – Hardware Write Block reports *http://www.nist.gov/itl/ssd/cs/cftt/cftt-hardware-write-block.cfm*

[18] Tableau, Guidance Software Inc. *http://www.tableau.com/*

[19] Wiebetech, CRU Acquisitions Group, LLC *http://www.wiebetech.com/*

[20] RFC 3174 – US Secure Hash Algorithm 1 (SHA1); *http://www.ietf.org/rfc/rfc3174.txt*

[21] RFC 1321 – The MD5 Message-Digest Algorithm; R. Rivest, April 1992 *http://www.ietf.org/rfc/rfc1321.txt*

[22] Collisions for Hash Functions - MD4, MD5, HAVAL-128 and RIPEMD; Xiaoyun Wang, 2004 *http://eprint.iacr.org/2004/199.pdf*

[23] Schneier on Security: Cryptanalysis of SHA-1; Bruce Schneier, 2005 *http://www.schneier.com/blog/archives/2005/02/cryptanalysis_o.html*

[24] Moderne Elektroniktechnologie und Informationsbeschaffung im Zivilprozeß; Dr. Helmut Rüßmann, 1995

[25] Hash mich - Konsequenzen der erfolgreichen Angriffe auf SHA-1; Reinhard Wobst, Jürgen Schmidt, 2005 *http://www.heise.de/security/artikel/56555*

[26] Hashfunktion SHA-1 offenbar gebrochen - Digitale Signaturen in Gefahr; Gesellschaft für Informatik e.V., Fachgruppe für Angewandte Kryptologie, 2005

Somit können die gängigen Hash-Funktionen bislang noch als sicherer Schutz gegen Manipulationen angesehen werden.

Durch die gleichzeitige Verwendung mehrerer verschiedenartiger Hash-Algorithmen kann in der Praxis eine unentdeckte Manipulation an den Beweismitteln nahezu mit Sicherheit ausgeschlossen werden.

Zudem sollte das Vertrauen in die Unversehrtheit der Daten zusätzlich anhand einer lückenlosen Beweismittelkette („chain of custody“) nachgewiesen werden können [24]. Dazu müssen die Beweismittel sofort nach der -bergabe bzw. Erstellung sicher versiegelt und aufbewahrt werden. Dazu sollten manipulationssichere Beweismittelbeutel verwendet werden und die Beweismittel an einem zutrittsgeschützten und für die Lagerung digitaler Speichermedien geeigneten Ort aufbewahrt werden

Hierbei ist grundsätzlich zu überlegen, ob die Beweismittel überhaupt im eigenen Haus aufbewahrt werden sollten oder ob diese nicht lieber an einen unparteiischen Dritten wie den forensischen Dienstleister oder eine Anwaltskanzlei ausgehändigt werden sollten. So kann dem vor Gericht leicht geäußerten Verdacht, dass sowohl Interesse als auch Möglichkeit zur Manipulation der Beweismittel vorhanden waren, von vornherein effektiv ein Riegel vorgeschoben werden.

MANUEL RUNDT, MARTIN WUNDRAM, ALEXANDER SIGEL

Manuel Rundt, Dipl.-Kfm.
ist Geschäftsführer der IT Compliance Systeme GmbH. Er beschäftigt sich bereits seit mehr als 9 Jahren mit dem Thema Wirtschaftskriminalität insbesondere IT Forensik und Incident Response.
manuel.rundt@compliance-systeme.de

Martin Wundram
ist Geschäftsführer der TronicGuard GmbH. Er ist Sachverständiger für IT-Sicherheit und IT-Forensik und beschäftigt sich auch mit Anti-Forensik.
wundram@tronicguard.com

Alexander Sigel
Berät Ermittlungsbehörden und Unternehmen zu Fragen der IT-Forensik und Informationssicherheit. Er ist Sachverständiger für IT-Forensik und Geschäftsführer der DigiTrace GmbH.
sigel@digitrace.de